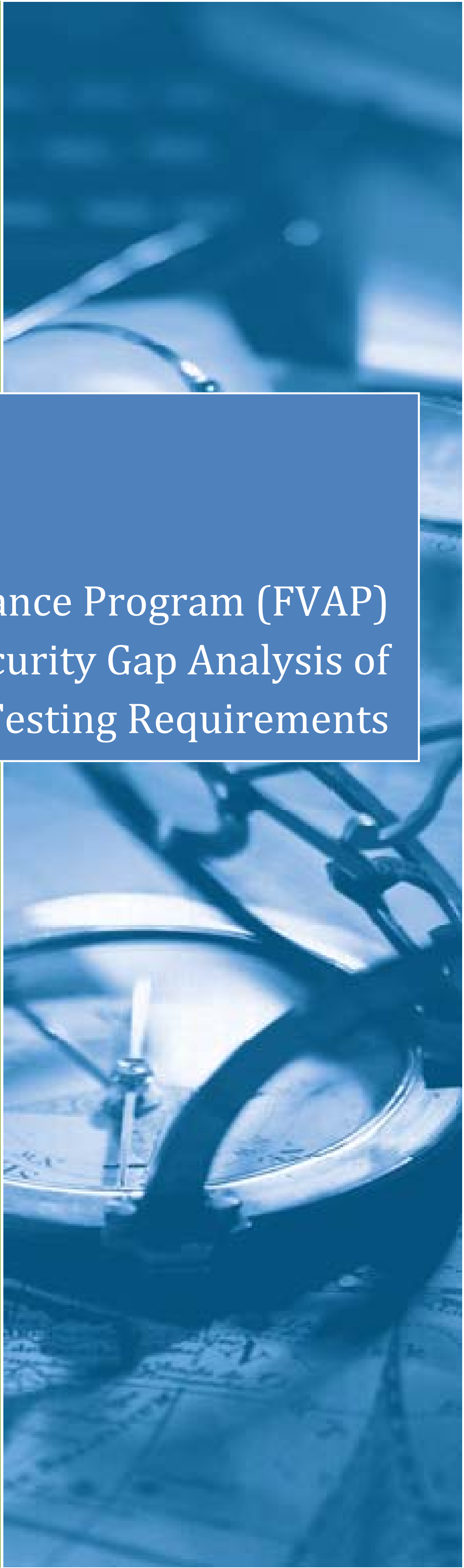
Appendix C



# Federal Voting Assistance Program (FVAP)
# Security Gap Analysis of
# UOCAVA Pilot Program Testing Requirements

*8 February 2011*

FVAP.GOV
FEDERAL VOTING ASSISTANCE PROGRAM

# Security Gap Analysis of UOCAVA Pilot Program Testing Requirements

***Delivery Order CT 80047-0037***

*Task 5.1.3*

*FINAL Report*

*February 8, 2011*

This report was prepared for the Federal Voting Assistance Program by CALIBRE Systems, Inc.

# Executive Summary

A complete Internet voting system could provide voter identification and authentication, voter registration, election administration, ballot delivery, voting, tabulation, and results reporting. However, any such electronic voting (eVoting) system must be able to insure privacy and security to the voting individual, as well as confirmation of their vote. However, there are many federal information systems that provide secure data transfer of privacy information and data of higher national security that are arguably far more sensitive than voting information that are currently in use and have met the requirements of the most stringent security guidance.

In December 2010, CALIBRE cyber security subject matter experts (SMEs) reached out to industry and federal agency contacts for additional insights on threats capable of launching a successful distributed denial of service (DDoS) attack or exploiting vulnerabilities associated with an eVoting system. A call for recommendations and insights was sent to senior cyber security experts and national security advisors. Additionally, CALIBRE contacted Carnegie Mellon University's Software Engineering Institute and Computer Emergency Response Team (CERT) for additional recommendations.

Simultaneously, CALIBRE began base-lining current UOCAVA testing requirements to determine if they meet current cyber threats. In total, 259 requirements were identified in the UOCAVA Pilot Program Test document from August 2008−2010. While many are functional requirements, all were evaluated for their security risk and potential exploit impacts. A security matrix was used to map the requirements to multiple industry and federal government security best practices and mandated requirements including: The National Institute of Standards and Technology (NIST), The International Standards Organization (ISO), Federal Information Security Management Act (FISMA), the Government Accountability Office (GAO), the Department of Defense (DoD), and Director of Central Intelligence Directive 6/3 Protecting Sensitive Compartmented Information within Information Systems (DCID 6/3).

Of the 259 requirements identified and evaluated, some only impact one of the three areas (confidentially, integrity and availability), but others could impact more than one. One hundred fifty requirements impacted confidentially, 246 impacted integrity, and 191 impacted availability. Of the 259 requirements, only 41 were categorized as having a low impact to security. However, 130 were considered to have a medium impact, and 88 were considered to have a high potential impact.

Of the 259 identified UOCAVA Pilot Program Testing Requirements, 186 meet specific federal guidance in the seven documents and are listed as "compliant" in the security requirements traceability matrix. Of the 259 requirements, 30 could not be traced directly to a federal requirement in the seven identified guidance documents. Therefore, it was unknown whether these requirements meet technical security requirements. Fifteen of the requirements are functional and do not have a security impact, and thereby, do not need to be reconciled. However, reconciliation with federal or international standards of 15 requirements was recommended. CALIBRE attempted to locate all documents listed as references within the UOCAVA Pilot Program Testing Requirements to match the 15 to possible requirements listed in those references. Not all of the references were located. However, of the un-reconciled 15 UOCAVA

Pilot Program Testing Requirements only 2 were found within the located references and were reconciled. Of the 13 requirements that were not found, they *do* follow best business practices.

Fifty-eight requirements were identified as functional (including the 15 mentioned above) and had no direct impact on security; they are only a functionality of the voting system. The most relevant finding is that NONE of the requirements that were traced were identified as NOT being compliant with the guidance, i.e., there are no notable gaps between UOCAVA Pilot Program Testing Requirements and the security guidance of the seven documents used in this analysis.

# Table of Contents

# Table of Tables

# 1 Background

The Federal Voting Assistance Program (FVAP) administers the federal responsibilities of the Presidential designee (Secretary of Defense) under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986. The Director, FVAP administers the Act on behalf of the Secretary of Defense.

The Act covers more than six million potential voters including the following:

- Active duty members of the uniformed services including the Coast Guard, commissioned corps of the Public Health Services, the Merchant Marine, and National Oceanic and Atmosphere Administration (NOAA);
- Their voting age dependents; and
- U.S. citizens residing outside the United States.

A complete electronic voting (eVoting) system would provide voter identification and authentication, voter registration, election administration, ballot delivery, voting, tabulation, and results reporting. However, any such eVoting system must be able to insure privacy and security to the voting individual, as well as confirmation of their vote.

# 2 Scope

The CALIBRE team, in support of FVAP efforts to develop the most secure remote voting capabilities, has been contracted to provide a technical gap analysis of testing procedures and related policies. In accordance with established guidance, [including NIST's research on security issues associated with remote electronic UOCAVA voting, and in coordination with the FVAP Office, the Wounded Warrior Care and Transition Policy (WWCTP) Office, and the Election Assistance Commission (EAC)] the CALIBRE team will conduct a variety of research, analysis, evaluation, and gap mitigation strategies to meet FVAP's strategic goals. The primary intent is to improve the policies, processes, and procedures for Wounded Warriors, disabled military members, military members, their dependents, and overseas civilian voters to register and vote successfully and securely with a minimum amount of effort.

# 3 Methodology

During the months of December 2010 and January 2011, a policy analysis team assembled relevant UOCAVA and FVAP materials and reviewed all known security-related concerns and policies relative to the UOCAVA Pilot Program Testing Requirements to understand these security issues. These efforts included, but were not limited, to the following:

- Identify all currently available UOCAVA, EAC, and FVAP mission and confidentiality policies.
- Identify mission assurance and confidentiality levels.
- Indentify most appropriate federal and industry best practices and guidance. Perform line-at-a-time comparison of UOCAVA Program Testing Requirements to all the chosen federally recognized and supported guidance standards.
- Produce a gap analysis and correlate identified security weaknesses with national vulnerability databases.
- Provide analysis of results.
- Identify mitigating methodologies and approaches when possible.

## *3.1 Identification of Mission and Data Classification*

### 3.1.1 The Mission of FVAP

FVAP's mission is to facilitate the absentee voting process for UOCAVA citizens living around the world. This includes: consulting with state and local election officials; prescribing the Federal Post Card Application (FPCA) for absentee registration/ballot requests, along with Federal Write-in Absentee Ballots (FWAB); and distributing descriptive material on state absentee registration and voting procedures. FVAP has three primary focus areas within its mission:

- Assist military and overseas voters in exercising their right to vote.
- Assist state and local election officials in complying with the requirements of federal law, and in providing equal voting opportunity for military and overseas voters.
- Advocate for military and overseas voting rights with federal, state and local governments.

### 3.1.2 Selection of MAC I and Confidentiality Level Sensitive

It is difficult to assign a DoD Mission Assurance Category (MAC) to the e-Voting system. However, in DoD Directive 8500.1 (Information Assurance) the DoD defines Mission Assurance Category I (MAC I) as the following: "Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures."[1]

While MAC I relates only to deployed forces outside the continental U.S. (OCONUS) and information that can affect their mission effectiveness, because the electoral process is considered to be an issue of national security, the e-Voting system would fall within this MAC level.

As for the confidentiality level (CL)[2] of the e-Voting system, the data stored in the system most closely matches the definition of sensitive data. For reasons of national security and for the highest level of confidentiality appropriate to the electoral process, we are evaluating the systems based on this level of classified.

Therefore, our analysis of the UOCAVA Pilot Program Testing Requirements in relation to the e-Voting system has been assigned the highest level Mission Assurance Category of I and confidentiality level of Classified, and will be evaluated against those Information Assurance (IA) controls.

**Table 1. Applicable IA Controls by MAC and CL Level**

| Mission Assurance Category and Confidentiality Level | Applicable IA Controls |
|---|---|
| MAC I, Classified | Encl. 4, Attachments A1 (Mission Assurance Category I Controls for Integrity and Availability) and A4 (Confidentiality Controls for DoD Information Systems Processing Classified Information) |
| MAC I, Sensitive | Encl. 4, Attachments A1 and A5 |
| MAC I, Public | Encl. 4, Attachments A1 and A6 |
| MAC II, Classified | Encl. 4, Attachments A2 and A4 |
| MAC II, Sensitive | Encl. 4, Attachments A2 and A5 |
| MAC II, Public | Encl. 4, Attachments A3 and A6 |
| MAC III, Classified | Encl. 4, Attachments A3 and A4 |
| MAC III, Sensitive | Encl. 4, Attachments A3 and A5 |
| MAC III, Public | Encl. 4, Attachments A3 and A6 |

### 3.1.3 Relevant Government Guidance

The UOCAVA Pilot Program Testing Requirements were derived from 120 references. These references range from a "Request for Proposal" and the Nevada Gaming Commission and State Gaming Control Board to IEEE standards[3]. While a few NIST special publications are listed, there are no references to current DIACAP guidance—which is needed for certification and accreditation if FVAP requires

[1] http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf

[2] http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf, Table E4.T3. Operating Environment Summary by Confidentiality Levels

[3] UOCAVA Pilot Program Testing Requirements, Appendix B.

certification and accreditation (C&A). Of the 259 identified requirements, 99 are security specific (only 32 percent). While UOCAVA made a significant effort to capture and define requirements based on 100-plus seemingly relevant guidance, we believe that fewer, more succinct references will benefit FVAP in the technical gap analysis.

Therefore, CALIBRE used seven prevailing IA documents for the Pilot Program Testing Requirements technical gap analysis. Within the Information Assurance industry there are multiple documents that provide guidance to civilian agencies, DoD and the intelligence community. For the civilian agencies, the dominant guiding documents are the NIST Special Publications; for DoD, there is the DIACAP guidance[4]; and for the intelligence community, there is the DCID 6/3. These three prevailing guidance documents are used to support this technical gap analysis for the following reasons. FVAP is a DoD entity, and therefore, falls under DIACAP processes. FVAP has a mission to support both DoD and civilian overseas personnel; falling under the NIST guidelines. However, because the electoral process is considered to be an issue of national security, the DCID 6/3 guidance must also be considered in the technical gap analysis.

In addition to this guidance, CALIBRE also referenced ISO 17799 (the International Standards Organization) due to the international requirements of FVAP, and ICD 503 (Intelligence Community Directive)—which was to replace DIACAP[1] in the analysis. FISMA guidance[5] and Government Accounting Office (GAO) FISCAM guidance[6] were also used because they are the mandating documents guiding all IA requirements within the U.S. Government.

### 3.1.4 Industry/Federal Data Call

In addition to the UOCAVA Pilot Testing Program gap analysis, CALIBRE has reached out to industry and federal agency contacts for additional insights on threats capable of launching a successful distributed denial of service (DDoS) attack on an election system. A data call for recommendations and insights were sent to 12 senior cyber security experts and national security advisors. Carnegie Mellon University's Software Engineering Institute and Computer Emergency Response Team (CERT) were contacted for additional guidance and recommendations. Aaron Bossert, a senior software exploit analyst for CERT has recommended that FVAP require vendors to apply the NIST SP-800-137 methodology and tools to the development and implementation of eVoting software. The recently developed NIST Software Assurance Metrics and Tool Evaluation (SAMATE) project defines software assurance as a "planned and systematic" set of activities that ensures that software processes and products conform to requirements, standards and procedures from the NASA Software Assurance Guidebook and Standard to better achieve the following:

- Trustworthiness—no exploitable vulnerabilities exist, either of malicious or unintentional origin (i.e., nothing is transmitted externally that will put the system at risk.)

[4] DIACAP guidance was intended to be replaced by Intelligence Community Directive (ICD503). However, this transition has not been widely adopted.

[5] The Federal Information Security Management Act of 2002.

[6] GAO Federal Information System Controls Audit Manual (FISCAM), 2009.

- Predictable Execution—justifiable confidence that software, when executed, functions as intended.

### 3.1.5 Internet Search

CALIBRE searched the following international vulnerability databases for technical vulnerabilities associated with the UOCAVA Pilot Program Testing Requirements:

- Microsoft Technical Databases
- NIST National Vulnerability Database
- National Checklist Program (automatable security configuration guidance in XCCDF & OVAL)
- SCAP (program and protocol that NVD supports)
- SCAP Compatible Tools
- SCAP Data Feeds (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
- Product Dictionary (CPE)
- Impact Metrics (CVSS)
- Common Weakness Enumeration (CWE)
- CVE Vulnerabilities–http://cve.mitre.org/
- Checklists–http://web.nvd.nist.gov/view/ncp/repository
- US-CERT Alerts–http://www.us-cert.gov/cas/techalerts/
- US-CERT Vuln Notes– http://www.kb.cert.org/ vuls/byupdate?open&start=1&count=10
- OVAL Queries–http://oval.mitre.org/
- Secunia–http://secunia.com/advisories/search/
- packetstorm– http://packetstormsecurity.org/files/tags/exploit/
- SANS Internet storm center– http://isc.incidents.org/
- OSVDB–http://osvdb.org/project_aims

# 4 Technical Gap Analysis

CALIBRE performed a technical gap analysis to compare existing UOCAVA internally published testing requirements with multiple federally supported and industry recognized information assurance guidance. The results were then compared to determine the current protection posture specific to e-Voting in order to better understand how effective those policies and requirements were in meeting security needs for eVoting as defined in the current government and industry standards.

This technical gap analysis identifies gaps in the current UOCAVA Pilot Program Testing Requirements (August 2008) based on guidance from multiple sources. The most widely referenced information assurance guidance comes from the following federally supported documents:

**Table 2. Referenced Guidance**

| Selected Guidance | Summary |
|---|---|
| The National Institute of Standards and Technology (NIST) Special Publications Series SP800-53A Rev2. | NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems. |
| The International Standards Organizations (ISO) and the International ElectroTechnical Commission (IEC) | ISO/IEC 17799:2005 is a code improved protection of practice for information security management.<br>The revised ISO/IEC 17799:2005 is the most important standard for managing information security that has been developed. |
| The Government Accounting Office (GAO) Federal Information System Control Audit Manual (FISCAM) | Provides security requirements for applicable controls specific to the applications they support. However, they generally involve ensuring that:<br>- data prepared for entry are complete, valid, and reliable;<br>- data are converted to an automated form and entered into the application accurately, completely, and on time;<br>- data are processed by the application completely and on time, and in accordance with established requirements; and<br>- output is protected from unauthorized modification or damage and distributed in accordance with prescribed policies. |

| Selected Guidance | Summary |
|---|---|
| The FIPS199/200 | Standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels.<br>Guidelines recommending the types of information and information systems to be included in each category.<br>Minimum information security requirements (i.e., management, operational, and technical controls) for information and information systems in each such category.<br>Standards for categorizing information and information systems collected or maintained by or on behalf of each federal agency based on the objective of providing appropriate levels of information security according to a range of risk levels.<br>Guidelines recommending the types of information and information systems to be included in each category.<br>Minimum information security requirements for information and information systems in each such category. |
| The Department of Defense 8500.2 | Implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks. |
| The Director Central Intelligence Directive 6/3 | Provides uniform policy guidance and requirements for ensuring adequate protection of certain categories of intelligence information;<br>Provides guidance to assist an Information System Security Manager (ISSM) or Information System Security Officer/Network Security Officer, (ISSO/NSO) in structuring and implementing the security protections for a system. |
| Intelligence Community Directive 503 (ICD 503) | ICD focuses on a holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop the use of common standards across the intelligence community. |

CALIBRE created a baseline of current UOCAVA Testing Requirements to determine if they meet current cyber threats. In total, 259 requirements were identified in the UOCAVA Pilot Program Test document from August 2008−2010. While many are functional requirements, all were evaluated for their security risk and potential exploit impacts. Using the NIST guidance, DIACAP guidance and DCID 6/3, the impacts were rated as low, medium and high relative to confidentially, integrity, and availability. The definition of the categories as stated by the three guidance methodologies is shown in the following tables.

**Table 3. Operating Environment Summary by Confidentiality Level According to NIST**

| Security Objective | Potential Impact | | |
|---|---|---|---|
| | Low | Medium | High |
| **Confidentiality**<br>Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. | The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |
| **Integrity**<br>Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity. | The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |
| **Availability**<br>Ensuring timely and reliable access to and use of information. Basic Testing: A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. | The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |

**Table 4. Operating Environment Summary by Confidentiality Level According to DIACAP**

| Confidentiality Level | Internal System Exposure | External System Exposure |
|---|---|---|
| High (Systems Processing Classified Information) | • Each user has a clearance for **all information** processed, stored or transmitted by the system.<br>• Each user has access approval for **all information** stored or transmitted by the system.<br>• Each user is granted access **only to information for which the user has a valid need-to-know**. | • System complies with DoDD C-5200.5 reference (aj) requirements for physical or cryptographic isolation.<br>• All Internet access is prohibited.<br>• All enclave interconnections with enclaves in the same security domain require boundary protection (e.g., firewalls, IDS, and a DMZ).<br>• All enclave interconnections with enclaves in a different security domain require a controlled interface.<br>• All interconnections undergo a security review and approval. |
| Medium (Systems Processing Sensitive Information) | • Each user has access approval for **all information** stored or transmitted by the system.<br>• Each user is granted access **only to information for which the user has a valid need-to-know**.<br>• Each IT user meets security criteria commensurate with the duties of the position. | • All non-DoD network access (e.g., Internet) is managed through a central access point with boundary protections (e.g., a DMZ).<br>• All enclave interconnections with enclaves in the same security domain require boundary protection (e.g., firewalls, IDS, and a DMZ).<br>• All remote user access is managed through a central access point.<br>• All interconnections undergo a security review and approval. |
| Basic (Systems Processing Public Information) | • Each user has access approval for **all information** stored or transmitted by the system.<br>• Each IT user meets security criteria commensurate with the duties of the position. | • N/A as the purpose of system is providing publicly released information to the public. |

**Table 5. Operating Environment Summary by Confidentiality Level According to DCID 6/3[7]**

| Level of Concern | Confidentiality Indicators (Chapter 4) | Integrity Indicators (Chapter 5) |
|---|---|---|
| Basic | Not applicable to this manual. | Reasonable degree of resistance required against unauthorized modification; or loss of integrity will have an adverse effect. |
| Medium | Not applicable to this manual. | High degree of resistance required against unauthorized modification; or bodily injury might result from loss of integrity; or loss of integrity will have an adverse effect on organizational-level interests. |
| High | All Information Protecting Intelligence Sources, Methods and Analytical Procedures.<br>All Sensitive Compartmented Information. | Very high degree of resistance required against unauthorized modification; or loss of life might result from loss of integrity; or loss of integrity will have an adverse effect on national-level interests; or loss of integrity will have an adverse effect on confidentiality. |

**Protection Levels  According to DCID 6/3**

| Lowest Clearance | Formal Access Approval | Need To Know | Protection Level |
|---|---|---|---|
| At Least Equal to Highest Data | All Users Have ALL | All Users Have ALL | 1<br>(paragraph 4.B.1) |
| At Least Equal to Highest Data | All Users Have ALL | NOT ALL Users Have ALL | 2<br>(paragraph 4.B.2) |
| At Least Equal to Highest Data | NOT ALL users have ALL | Not Contributing to Decision | 3<br>(paragraph 4.B.3) |
| Secret | Not Contributing to Decision | Not Contributing to Decision | 4<br>(paragraph 4.B.4) |
| Un-cleared | Not Contributing to Decision | Not Contributing to Decision | 5<br>(paragraph 4.B.5) |

There are no additional security requirements under the DCID 6/3 guidance, and the translation of the confidentiality, integrity and availability is directed at secure compartmented information (SCI) and the need to know. We've taken the high water mark of a High PL1 DCID 6/3 security profile for the UOCAVA Pilot Program Testing gap analysis.

A Pilot Program Testing Requirements Matrix[8] was created to map the requirements to multiple industry and federal government security best practices and mandated requirements as identified in Table 2.

We searched for security weaknesses and gaps by associating UOCAVA Pilot Program Testing Requirements with the seven guidance documents. Of the 259 requirements identified and evaluated, some only impact one of the three areas (confidentially, integrity and availability), but others could impact more than one; 150 requirements impacted confidentially, 246 impacted integrity, and 191

[7] Director Central Intelligence Directive 6/3, http://www.fas.org/irp/offdocs/DCID_6-3_20Manual.htm#Protection Levels

[8] See Appendix A: Security Requirements Traceability Matrix

impacted availability. Of the 259 requirements, only 41 were categorized as having a low impact to security. However, 130 were considered to have a medium impact, and 88 were considered to have a high potential impact.

Of the 259 identified UOCAVA Pilot Program Testing Requirements, 186 meet specific federal guidance in the seven documents and are listed as “compliant” in the security requirements traceability matrix. Of the 259 requirements, 30 could not be traced directly to a federal requirement in the seven identified guidance documents. Therefore, it was unknown whether these requirements meet technical security requirements. Fifteen of the requirements are functional and do not have a security impact, and thereby, do not need to be reconciled. However, reconciliation with federal or international standards of 15 requirements was recommended. CALIBRE attempted to locate all documents listed as references within the UOCAVA Pilot Program Testing Requirements to match the 15 to possible requirements listed in those references. Not all of the references were located. However, of the un-reconciled 15 UOCAVA Pilot Program Testing Requirements only 2 were found within the located references and were reconciled. Of the 13 requirements that were not found, they *do* follow best business practices.

Fifty-eight requirements were identified as functional (including the 15 mentioned above), and had no direct impact on security; they are only a functionality of the voting system. The most relevant finding is that NONE of the requirements that were traced were identified as NOT being compliant with the guidance, i.e., there are no notable gaps between UOCAVA Pilot Program Testing Requirements and the security guidance of the seven documents used in this analysis.

# 5 Recommendations

The industry assumption is that technology is a step behind the high level of encryption. This assumption, however, is continually challenged by advances in technology. For FVAP, the challenges are further complicated by the fact that the majority of sophisticated and well-funded threat information is held in a classified status and is not available for general disclosure.  Furthermore, in the computer world, information a month old is often outdated. The most recent publication, the *NIST Draft White Paper on Security Considerations for Remote Electronic UOCAVA Voting* (which is still out for comments), documents threats to UOCAVA voting systems using electronic technologies for overseas and military voting. However, by the time it is formally released, the cyber threat community may have ensured that the information is no longer viable.

Therefore, once the new security requirements have been identified and/or mitigated, they should be tracked over time to address changes in regulatory compliance, new attack vectors, threats and known vulnerabilities; the weighing of effort required to protect vulnerabilities will need to be assessed frequently as new technologies and exploit capabilities are developed or become known.

## 5.1 Recommendations to the UOCAVA Pilot Program Testing Requirements

CALIBRE recommends that FVAP address the following areas based on identified potential technical vulnerabilities and security weaknesses within the UOCAVA Pilot Program Testing Requirements. (See Table 6).

**Table 6. Recommendations to the UOCAVA Pilot Program Testing Requirements**

| Item | UOCAVA Req. No. | Recommendations |
|---|---|---|
| 1. | 2.2.3 | Recommend that the following guidance be referenced and followed. NIST SP800-52 provides guidance on protecting transmission integrity using TLS. Other NIST documents include SP800-81, 800-44, 800-45, 800-49, 800-57, 800-58, 800-66, 800-77 and 800-81. FIPS 198 also discusses transmission quality. |
| 2. | 2.3.1.1 | Recommend that all graphic file formats be tested for corruption from malformed packets. Known vulnerabilities exist with almost all graphic file formats. Appropriate patches to operating systems must be tested. |
| 3. | 2.3.1.2 | No recommendation. However, the requirement does not specify how this is to be accomplished. |
| 4. | 2.6.2.2 | See recommendation for 2.3.1.1. |
| 5. | 2.6.2.3 | See recommendation for 2.3.1.1. |
| 6. | 2.7.1.1 | Recommend that IDS/IPS system(s) SHALL be used that actively monitors, detects, and notifies system administrators of any potential malicious activity. |
| 7. | 4.9.1.3 | Recommend the use of application scanning tools such as Fortify 360, Nessus, |

| Item | UOCAVA Req. No. | Recommendations |
|---|---|---|
| | | Lumension etc. to identify source code vulnerabilities. |
| 8. | 4.9.1.4 | See recommendation for 4.9.1.3. |
| 9. | 5.1.1.1 | See recommendation for 4.9.1.3. |
| 10. | 5.1.1.2 | See recommendation for 4.9.1.3. |
| 11. | 5.2.1.1 | Recommend the use of three-factor authentication method to include biometric with a Cross over Error Rates (CER) and Equal Error Rates that meet minimum DoD requirements. |
| 12. | 5.2.1.3 | Recommend that passwords conform to DOD minimum requirements. |
| 13. | 5.2.1.12 | Recommend that authentication schema SHALL be commensurate with the highest level technically feasible, as this will constantly change as new schemas become available. |
| 14. | 5.3.1.2 | See recommendation for 5.2.1.12. |
| 15. | 9.5.1.9 | Recommend adoption of DoD guidance for erasable media. |

The following table is a list of UOCAVA Pilot Program Testing Requirements that were not found in any of the seven governmental guidance documents used for the technical gap analysis. The requirements on this list should be reconciled. (See Table 7).

**Table 7. UOCAVA Pilot Program Testing Requirements that are Not Reconciled with Guidances.**

| Item | UOCAVA Requirement Number | UOCAVA Requirement Title |
|---|---|---|
| 1. | 4.3.1.2 | Module Testability |
| 2. | 4.3.1.3 | Module Size and Identification |
| 3. | 4.7.2.7 | Nullify Freed Pointers |
| 4. | 4.7.2.8 | Do not disable error checks |
| 5. | 4.7.2.11 | Election Integrity Monitoring |
| 6. | 5.4.1.2 | Cast Vote Integrity Storage |
| 7. | 5.4.1.3 | Cast Vote Storage |
| 8. | 5.4.1.4 | Electronic Ballot Box Integrity |
| 9. | 6.2 | Components from Third Parties |
| 10. | 6.3 | Responsibilities for Tests |
| 11. | 7.5.2 | Function Configuration Audit (FCA) |
| 12. | 8.2.1 | TDP Implementation |
| 13. | 8.3.4.1 | Hardwired and Mechanical implementations of logic |
| 14. | 8.3.4.2 | Logic Specifications for PLD's, FPGA's and PIC's |
| 15. | 8.4.5.3 | Justify Coding Conventions |
| 16. | 8.4.6.1 | Application Logic Operating Environment |
| 17. | 8.4.7.1 | Hardware Environment and Constraints |
| 18. | 8.4.8.2 | Compilers and Assemblers |
| 19. | 8.4.8.3 | Interpreters |
| 20. | 8.4.9.1 | Application logic functional specification |
| 21. | 9.2.3.3 | Traceability of Procured Software |
| 22. | 9.4.5.1 | Ballot Count and Vote Total Auditing |
| 23. | 9.5.1.4 | Election Specific Software Identification |
| 24. | 9.5.1.7 | Compiler Installation Prohibited |

| Item | UOCAVA Requirement Number | UOCAVA Requirement Title |
|---|---|---|
| 25. | 9.5.1.8 | Procurement of System Software |
| 26. | 9.6.1.2 | Setup Inspection Record generation |
| 27. | 9.6.1.12 | Consumables quantity of vote capture device |
| 28. | 9.6.1.13 | Consumables Inspection Procedures |
| 29. | 9.6.1.14 | Calibration of vote capture devices components nominal range |
| 30. | 9.6.1.15 | Calibration of vote capture device components inspection procedure |

At this point, CALIBRE researched the UOCAVA Pilot Program Testing Requirements references to attempt to map the 30 un-reconciled requirements to other guidance. Of the 30 requirements to be reconciled, 15 were functional and did not have a security impact, and 2 were found in other related federal references. The remaining 13 requirements could not be mapped to specific federal regulatory guidance or requirements, but do support best business practices. (See Table 8.)

**Table. 8 UOCAVA Security Control Reconciliation**

| UOCAVA Requirement | Impact (C,I,A) | Risk | Comment |
|---|---|---|---|
| 4.7.2.7 Nullify Freed Pointers | I, A | Medium | A best coding practice. Recommend that coding follow CMMI level-3 methodologies at a minimum. |
| 6.3 Responsibility for tests | I, A | Medium | No specific regulatory requirement for manufactures to perform tests. Normally included within the RFP. |
| 8.3.4.1 Hardwired and mechanical implementation logic | C, I, A | High | Falls under border logic. This should be addressed within the System Security Plan. |
| 8.3.4.2 Logic specification for PLD's, FPGA's, and PIC's | C, I, A | High | Falls under border logic. This should be addressed within the System Security Plan. |
| 8.4.5.3 Justify coding conventions | C, I, A | Medium | No specific regulation identified. Can be addressed within the RFP. |
| 8.4.8.3 Interpreters | C, I, A | Low | No specific NIST or IEEE Requirements identified for COTS runtime code version. However, this should be documented within the System Security Plan. |
| 8.4.9.1 Application logic functional specifications | C, I, A | Low | No specific NIST or IEEE Requirements identified for COTS runtime code version. However, this should be documented within the System Security Plan. |
| 9.5.1.4 Election specific software identification | I | Medium | This is best security practice, but no specific federal regulatory reference could be identified. |
| 9.5.1.7 Compiler installation prohibited | C, I, A | Medium | This is best security practice, but no specific federal regulatory reference could be identified. |
| 9.6.1.2 Setup inspection record generation | C, I, A | Medium | Ref. in NIST SP800-100 speaks to security checklists. Should be addressed within the System Security Plan. |
| 9.6.1.12 Consumables quantity of vote capture device | A | Low | Not a significant risk. |
| 9.6.1.13 Consumables inspection | A | Low | No specific security risk. Mentioned in NIST H143 and media |

| UOCAVA Requirement | Impact (C,I,A) | Risk | Comment |
|---|---|---|---|
| procedures | | | storage. Should be addressed within the System Security Plan. |
| 9.6.1.14 Calibration of vote capture device components nominal range | I | Medium | This should fall under System Security Plan guidance. Should be addressed within the System Security Plan. |

*Note: for column 2, C=Confidentiality, I=Integrity, and A=Availability.*

## *5.2 Things to Consider*

### 5.2.1 Software Monitoring

Our data call research indicates that several automation specifications exist to support the continuous monitoring of software assurance, including the emerging Software Assurance Automation Protocol (SwAAP) that is being developed to measure and evaluate software weaknesses and assurance cases. SwAAP uses a variety of automation specifications such as the Common Weakness Enumeration (CWE), which is a dictionary of weaknesses that can lead to exploitable vulnerabilities, and the Common Weakness Scoring System (CWSS) for assigning risk scores to weaknesses. SwAAP also uses the Common Attack Pattern Enumeration & Classification (CAPEC)—which is a publicly available catalog of attack patterns with a comprehensive schema and classification taxonomy—to provide descriptions of common methods for exploiting software, and the Malware Attribute Enumeration & Characterization (MAEC), which provides a standardized language for encoding and communicating information about malware based upon attributes such as behaviors, artifacts, and attack patterns.

### 5.2.2 Other Secure Systems

There are many federal information systems that provide secure data transfer of privacy information and data of higher national security that are arguably far more sensitive than voting information and are currently in use and have met the requirements of the most stringent security guidance. For example, the EQIP[9] and JPAS[10] systems have been online for quite some time, and one can draw some very important parallels to an e-Voting system. They have to support the reality that a user may access it from any internet-connected computer system, and they must verify the relative security of that system. Another parallel is that the sensitivity is arguably equal to or greater than an e-Voting system.

Furthermore, the IRS uses the Electronic Federal Tax Payment System (EFTPS). Tax returns contain considerable privacy information including: name, address, rank, SSN, income, income sources, deductions, dependents, donations, and investments. However, since 1986, and with over 400 million

[9] EQIP is the Office of Personnel Managements background investigation tool. It has a diagnostic tool for evaluating the security of a PC to determine if it meets security requirements. This could also be used for remote voting via Internet.

[10] http://www.dss.mil/diss/jpas/jpas.html

returns, the IRS e-file system has never been compromised. According to the IRS website, the following facts and information are true.

> - *The IRS* **e-file** *System is not done over e-mail.*
> - *The IRS* **e-file** *System has many built-in security features.*
> - *The IRS* **e-file** *System employs multiple firewalls.*
> - *The IRS* **e-file** *System uses state of the art virus and worm detection.*
> - *The IRS* **e-file** *System meets or exceeds all government security standards.*
> - *The IRS* **e-file** *System is constantly tested for weaknesses by penetration testing.*
> - *The IRS* **e-file** *System has never had a security breach.*
> - *All Internet transmissions will use SSL (Secure Sockets Layer) encrypted security measures.*
>
> *IRS* **e-file** *transmissions are very secure because the IRS has been extremely diligent in the design, development, analysis and testing of the current infrastructure and system. IRS* **e-file** *meets or exceeds all government security standards and includes multiple firewalls***.**
>
> *Most e-filed online tax returns are transmitted over phone lines from the return preparer to a third-party transmitter. From there, the returns are forwarded over secured lines to the IRS. Intercepting telephone transmissions is quite difficult and requires access to phone company major transmission lines. Also, to transmit data like tax returns over telecommunications lines means that the information gets converted into digital format, which could not be easily read even if it were intercepted.*[11]

Because user confidence and demand is high, the IRS has recently designed and deployed a mobile application for use across inherently unsecured wireless connection (e.g., iPhone/Android apps).

In addition to these federally supported, secure online capabilities, financial institutions and stock trading companies (such as eTrade), as well as many healthcare institutions are heavily dependent upon transfer of privacy based data that supports extremely high system availability and data integrity. All of these systems must be compliant with federal guidance. If EQIP, JPAS and these others were certified and accredited and are in use today, then certainly a similar approach and technology could be taken when considering what risks are acceptable in an e-Voting system.

There is yet another consideration—even though there was a valiant effort made to document the risks associated with the current overseas voting system, and a hypothetical electronic system has been discussed, it is very important to make a direct comparison between the current threats to the existing system and the equivalent threats to a proposed electronic system, such as:

- The current paper-based system is susceptible to "man-in-the-middle" attacks with little or no mechanisms in place to detect or prevent them.
- Personal information (PII) can be stolen elsewhere and can be used to forge ballots.

[11] http://www.irs.gov/efile/article/0,,id=121477,00.html

- Physical signatures are less secure than properly implemented digital ones when it is considered that even though one can reliably verify that a physical signature is authentic, it is rarely done due to being prohibitively expensive to implement on this scale.
- This e-Voting system is no more, or less susceptible to DDoS or other types of attack than any other system; as such it could take advantage of the very well accepted countermeasures to these types of attacks. (Recently, DDoS attacks directed at WikiLeaks during the Cablegate scandal proved to be relatively ineffective, and WikiLeaks dealt with the attack quickly.)

While there are some serious security vulnerabilities that need to be addressed in terms of e-Voting, it is not impossible to implement a sufficiently secure e-Voting system, assuming that the cost of the countermeasures is acceptable.

# Appendix A Security Requirements Traceability Matrix

FVAP_UOCAVA_SRTM_v16.xls

Appendix A can be found on pg. 48 of this document

# Appendix B References

1. Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), (as modified by the National Defense Authorization Act for FY 2005). http://www.fvap.gov/resources/media/uocavalaw.pdf

2. 107th U.S. Congress (October 29, 2002). "Help America Vote Act of 2002 (Pub. L. 107-252)." U.S. Government Printing Office.

3. National Institute of Standards and Technology Interagency Report: 7551, *A Threat Analysis on UOCAVA Voting Systems*, December 2008.

4. Draft National Institute of Standards and Technology Interagency Report 7682, *Information System Security Best Practices for UOCAVA Supporting Systems*, April 2010.

5. U.S. Election Assistance Commission (March 24, 2010). UOCAVA Pilot Program Testing Requirements, March 24, 2010. Accessed May 10, 2010 at http://www.eac.gov/program-areas/voting-systems/docs/requirements-03-24-10-uocava-pilot-program

6. EAC (2010, April 26). Report to Congress on EAC's Efforts to Establish Guidelines for Remote Electronic Absentee Voting Systems. Accessed May 10, 2010 at http://www.eac.gov/program-areas/voting-systems/docs/04-26-10-move-act-report-to-congress-final-congress/

7. M. Volkamer and R. Vogt. Basic set of security requirements for Online Voting Products. Common Criteria Protection Profile BSI-CC-PP-0037, Bundesamt für Sicherheit in der Informationstechnik, Bonn, April 2008.

8. Council of Europe. Legal, Operational, and Technical Standards for E-Voting. Recommendation Rec (2004)11, September 2004.

9. Federal Voting Assistance Program. *Secure Electronic Registration and Voting Experiment. Threat Risk Assessment- Phase 3*. March 23, 2004.

10. McConnell, Steven (2004), Code Complete (Second Edition), Microsoft Press.

11. Georgia Tech Information Security Center (2008). *Emerging Cyber Threats Report for 2009.* Accessed May 15, 2010 at http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf

12. US-CERT (2008, May 16). *Technical Cyber Security Alert TA08-137A: Debian/Ubuntu OpenSSL Random Number Generator Vulnerability*. Accessed May 15, 2010 at http://www.us-cert.gov/cas/techalerts/TA08-137A.html

13. Symantec (2010, April). *Symantec Global Internet Security Threat Report: Tends for 2009*. Accessed May 15, 2010 at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

14. Dierks, T. and Rescorla, E., *The TLS Protocol Version 1.2*, Internet Engineering Task Force, Request for Comment 5246, August 2008, http://tools.ietf.org/html/rfc5246

15. Atsushi Fujioka, Tatsuaki Okamoto, and Kazui Ohta. A Practical Secret Voting Scheme for Large Scale Elections. In Jennifer Seberry and Yuliang Zheng, editors, *Advances in Cryptology - AUSCRYPT '92*, volume 718 of *Lecture Notes in Computer Science*, pages 244--251, Berlin, 1993. Springer-Verlag.

16. Rene Peralta. Issues, non-issues and cryptographic tools for Internet-based voting. In *Secure Electronic Voting* (Boston, 2003), Dimitris A. Gritzalis, editor. Kluwer Academic Publishers, pp. 153-164.

17. Lorrie Faith Cranor and Ron K. Cytron, Sensus: A Security-Conscious Electronic Polling System for the Internet. *Proceedings of the Hawai`i International Conference on System Sciences* , January 7-10, 1997, Wailea, Hawaii, USA.

18. J. Benaloh and D. Tuinstra. Receipt-Free Secret-Ballot Elections. *Proceedings of the 26th ACM Symposium on Theory of Computing*. Montreal, PQ. May 1994. (New York, USA: ACM 1994), pp. 544—553.

19. Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. *A secure and optimally efficient multi-authority election scheme*. European Transactions on Telecommunications, 8:481-489, 1997.

20. Premiere Election Solutions (2008, August 19). *Product Advisory Notice*. Accessed May 15, 2010 at http://www.sos.state.oh.us/sos/upload/news/20081001c.pdf

21. Fink, R.A.; Sherman, A.T.; Carback, R.; , "TPM Meets DRE: Reducing the Trust Base for Electronic Voting Using Trusted Platform Modules," *Information Forensics and Security, IEEE Transactions on* , vol.4, no.4, pp.628-637, Dec. 2009.

22. Ben Adida, Olivier de Marneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing a University President Using Open-Audit Voting: Analysis of Real-World Use of Helios, In D. Jefferson, J.L. Hall, T. Moran, editor(s), *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, Usenix, August 2009.

23. Nathanael Paul, Andrew S. Tanenbaum, "The Design of a Trustworthy Voting System," Computer Security Applications Conference, Annual, pp. 507-517, 2009 Annual Computer Security Applications Conference, 2009.

24. Common Criteria for Information Security Evaluation. Part 3: Security assurance components. Version 3.1, Rev. 3, July 2009.

25. Patrick Peterson, Henry Stern. "Botnets Gone Wild! Captured, Observed, Unraveled, Exterminated." Presented at RSA 2010, San Francisco, CA, March 1-5, 2010.

26. Testimony of Bob Carey, Director of FVAP. (2010) EAC Public Meeting, Dec. 3 2009. Accessed April 5, 2010 at http://www.eac.gov/public_meeting_12032010/

27. United States Postal Service (2007). *2007 Comprehensive Statement*. Accessed March 17, 2010 at http://www.usps.com/strategicplanning/cs07/chpt5_001.htm

28. Alvarez, R. Michael (2005, October 5). "Precinct Voting Denial of Service", *NIST Threats to Voting Systems Workshop*. Accessed March 17, 2010 at http://vote.nist.gov/threats/papers/precinct_dos.pdf

29. Davis, Joshua (2007, August 21). "Hackers Take Down the Most Wired Country in Europe" *Wired Magazine*. Accessed March 5, 2010 at http://www.wired.com/politics/security/magazine/15-09/ff_estonia

30. Markoff, John (2008, August 13). "Before the Gunfire, Cyberattacks" *The New York Times*. Accessed March 5, 2010 at http://www.nytimes.com/2008/08/13/technology/13cyber.html

31. Vixie, Paul, Sneeringer, Gerry, and Mark Schleifer (2002, November 24). Events of 21-Oct-2002." Accessed March 5, 2010 at http://d.root-servers.org/october21.txt

32. Internet Corporation for Assigned Names and Numbers. "Factsheet- Root server attack on 6 February 2007." Accessed March 5, 2010 at http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf

33. Worthham, Jenna, and Andrew E. Kramer (2009, August 7) "Professor Main Target of Assault on Twitter" *The New York Times*. Accessed March 5, 2010 at http://www.nytimes.com/2009/08/08/technology/internet/08twitter.html

34. D. J. Bernstein and Eric Schenk (1996). *SYN Cookies*. 1996. Accessed May 15, 2010 at http://cr.yp.to/syncookies.html

35. Mell, Peter and Tim Grance (2009, October 7), *The NIST Definition of Cloud Computing*. Accessed March 2, 2010 at http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

36. U.S. Election Assistance Commission (2006, December). *Election Crimes: An Initial Review and Recommendations for Future Study*. Accessed June 15, 2010 at http://www.eac.gov/assets/1/workflow_staging/Page/57.PDF

37. Gartner (2009, April 14). *Gartner Says Number of Phishing Attacks on U.S. Consumers Increased 40 Percent in 2008*. Accessed March 5, 2010 at http://www.gartner.com/it/page.jsp?id=936913

38. Cormac Herley and Dinei Florencio, A Profitless Endeavor: Phishing as Tragedy of the Commons, in *Proc. New Security Paradigms Workshop*, Association for Computing Machinery, Inc., September 2008.

39. Anti-Phishing Working Group (2009). *Phishing Activity Trends Report, 4th Quarter 2009*. Accessed March 5, 2010 at http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf

40. Office of Management and Budget (2006, June 23). *OMB Memo M06-16*. Accessed March 5, 2010 at http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-16.pdf

41. McAfee Labs (2009). *2010 Threat Predictions*. Accessed April 13, 2010 at http://www.mcafee.com/us/local_content/white_papers/7985rpt_labs_threat_predict_1209_v2.pdf

42. Department of Defense. *Common Access Card*. Accessed March 5, 2010 at http://www.cac.mil/

43. National Institute of Standards and Technology (2009). *About Personal Identity Verification (PIV) of Federal Employees and Contractors.* Accessed March 5, 2010 at http://csrc.nist.gov/groups/SNS/piv/

44. Estonian National Electoral Committee. *Internet voting in Estonia*. Accessed March 5, 2010 at http://www.vvk.ee/public/dok/Internet_Voting_in_Estonia.pdf

45. Mozilla Foundation (2006, November 14). *Firefox 2 Phishing Protection Effectiveness Testing.* Accessed April 5, 2010 at http://www.mozilla.org/security/phishing-test.html

46. S. Egelman, L. Cranor, and J. Hong. You've Been Warned: An Empirical Study on the Effectiveness of Web Browser Phishing Warnings. CHI '08: Proceedings of the SIGCHI conference on Human Factors in Computing Systems. April 2008.

47. National Institute of Standards and Technology (2008, August). *The 2008 NIST Speaker Recognition Evaluation Results.* Accessed May 5, 2010 at http://www.itl.nist.gov/iad/mig/tests/sre/2008/official_results/index.html

# Appendix C Glossary

This appendix provides definitions for security terminology used within or referenced in this document. The terms in the glossary are consistent with the terms used in the suite of FISMA-related security standards and guidelines developed by NIST. Unless otherwise stated, all terms used in this publication are also consistent with the definitions contained in the CNSS Instruction 4009, *National Information Assurance Glossary*.

**Activities**
An assessment object that includes specific protection related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic).

**Adequate Security**
**[OMB Circular A130, Appendix III]**
Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost effective management, personnel, operational, and technical controls.

**Advanced Persistent Threats**
An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information, and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future. Moreover the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.

**Agency**
See *Executive Agency*

**Allocation**
The process an organization employs to determine whether security controls are defined as system specific, hybrid, or common. The process an organization employs to assign security controls to specific information system components responsible for providing a particular security capability (e.g., router, server, remote sensor).

**Application**
A software program hosted by an information system.

**Assessment**
See *Security Control Assessment*.

**Assessment Findings**

Assessment results produced by the application of an assessment procedure to a security control or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a *satisfied* or *other than satisfied* condition.

**Assessment Method**

One of three types of actions (i.e., examine, interview, test) taken by assessors in obtaining evidence during an assessment.

**Assessment Object**

The item (i.e., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.

**Assessment Objective**

A set of determination statements that expresses the desired outcome for the assessment of a security control or control enhancement.

**Assessment Procedure**

A set of assessment objectives and an associated set of assessment methods and assessment objects.

**Assessor**

See *Security Control Assessor*.

**Assurance**

The grounds for confidence that the set of intended security controls in an information system are effective in their application.

**Assurance Case**
**[Software Engineering Institute, Carnegie Mellon University]**

A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute.

**Authentication [FIPS 200]**

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

**Authenticity**

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See Authentication.

**Authorization (to operate)**

The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed upon set of security controls.

**Authorization Boundary**
**[NIST SP 800-37]**

All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

**Authorize Processing** See *Authorization*.

**Authorizing Official (AO) [NIST SP 800-37]** A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

**Authorizing Official Designated Representative [NIST SP 800-37]** An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.

**Availability [44 U.S.C., Sec. 3542]** Ensuring timely and reliable access to and use of information.

**Basic Testing** A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as *Black Box Testing*.

**Black Box Testing** See *Basic Testing*.

**Categorization** The process of determining the security category (the restrictive label applied to classified or unclassified information to limit access) for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.

**Chief Information Officer (CIO) [PL 104-106, Sec. 5125(b)]** Agency official responsible for: 1) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; 2) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and 3) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

**Chief Information Security Officer** See Senior Agency Information Security Officer.

**Common Control [NIST SP 800-37]** A security control that is inherited by one or more organizational information systems. See Security Control Inheritance.

**Common Control Provider [NIST SP 800-37, Rev. 1]** An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems).

**Compensating Security Controls [NIST SP 800-53]**
The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.

**Comprehensive Testing**
A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as *White Box Testing*.

**Computer Incident Response Team (CIRT)**
Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability, or Cyber Incident Response Team).

**Confidentiality [44 U.S.C., Sec. 3542]**
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

**Configuration Control (or Configuration Control) [CNSSI 4009]**
Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.

**Continuous Monitoring**
Maintaining ongoing awareness to support organizational risk decisions. See *Information Security Continuous Monitoring*, *Risk Monitoring* and *Status Monitoring*.

**Controlled Interface**
A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems.

**Controlled Unclassified Information**
A categorical designation that refers to unclassified information that does not meet the standards for National Security classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces *Sensitive But Unclassified (SBU)*.

**Countermeasures [CNSSI 4009]**
Actions, devices, procedures, techniques, or other measures that

reduce the vulnerability of an information system. Synonymous with security controls and safeguards.

**Cross Domain Solution** A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains.

**Coverage** An attribute associated with an assessment method that addresses the scope or breadth of the assessment objects included in the assessment (e.g., types of objects to be assessed and the number of objects to be assessed by type). The values for the coverage attribute, hierarchically from less coverage to more coverage, are basic, focused, and comprehensive.

**Data Loss** The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.

**Depth** An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method. The values for the depth attribute, hierarchically from less depth to more depth, are basic, focused, and comprehensive.

**Domain [CNSSI 4009]** An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See *Security Domain*.

**Dynamic Subsystem** A subsystem that is not continually present during the execution phase of an information system. Service oriented architectures and cloud computing architectures are examples of architectures that employ dynamic subsystems.

**Environment of Operation [NIST SP 800-37]** The physical surroundings in which an information system processes, stores, and transmits information.

**Examine** A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time.

**Executive Agency [41 U.S.C., Sec. 403]** An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

**External Information System** An information system or component of an information system

**(or Component)** that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

**External Information System Service** An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

**External Information System Service Provider** A provider of external information system services to an organization through a variety of consumer producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain arrangements.

**Federal Agency** See *Executive Agency*.

**Federal Information System [40 U.S.C., Sec. 11331]** An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

**Federal Enterprise Architecture [FEA Program Management Office]** A business-based framework for government-wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen centered, results-oriented, and market-based.

**Focused Testing** A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. Also known as *Gray Box Testing.*

**Gray Box Testing** See *Focused Testing*.

**High-Impact System [FIPS 200]** An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.

**Hybrid Security Control [NIST SP 800-53]** A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See *Common Control* and *System-Specific Security Control*.

**Individuals** An assessment object that includes people applying specifications, mechanisms, or activities.

**Industrial Control System**

An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.

**Information [FIPS 199]**

An instance of an information type.

**Information Owner**
**[CNSSI 4009]**

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

**Information Resources**
**[44 U.S.C., Sec. 3502]**

Information and related resources, such as personnel, equipment, funds, and information technology.

**Information Security**
**[44 U.S.C., Sec. 3542]**

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

**Information Security Risk**

The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and /or information systems.

**Information Security Architect**

Individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization’s core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes.

**Information Security Continuous Monitoring**

Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

**Information Security Policy**
**[CNSSI 4009]**

Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

**Information Security Program Plan**
**[NIST SP 800-53]**

Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.

**Information Steward**

Individual or group that helps to ensure the careful and responsible management of federal information belonging to the nation as a whole, regardless of the entity or source that may have originated, created, or compiled the information. Information stewards provide maximum access to federal information to elements of the federal government and its customers, balanced by the obligation to protect the information in accordance with the provisions of FISMA and any associated security- related federal policies, directives, regulations, standards, and guidance.

**Information System [44 U.S.C., Sec. 3502]**

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

**Information System Boundary**

See *Authorization Boundary*.

**Information System Owner (or Program Manager)**

Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

**Information System Security Engineer**

Individual assigned responsibility for conducting information system security engineering activities.

**Information System Security Engineering**

Process that captures and refines information security requirements and ensures their integration into information technology component products and information systems through purposeful security design or configuration.

**Information System related Security Risks**

Information system-related security risks are those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the nation. See *Risk*.

**Information System Security Officer (ISSO) [CNSSI 4009]**

Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.

**Information Technology [40 U.S.C., Sec. 1401]**

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

**Information Type [FIPS 199]** A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

**Integrity [44 U.S.C., Sec. 3542]** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

**Interview** A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control effectiveness over time.

**Intrusion Detection and Prevention System (IDPS)** Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

**Joint Authorization** Security authorization involving multiple authorizing officials.

**Low-Impact System [FIPS 200]** An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.

**Malware** A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

**Management Controls [FIPS 200]** The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

**Measures** All the output produced by automated tools (e.g., IDS/IPS, vulnerability scanners, audit record management tools, configuration management tools, asset management tools) as well as various information security program-related data (e.g., training and awareness data, information system authorization data, contingency planning and testing data, incident response data). Measures also include security assessment evidence from both automated and manual collection methods.

**Mechanisms**

An assessment object that includes specific protection-related items (e.g., hardware, software, or firmware) employed within or at the boundary of an information system.

**Metrics**

Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance- related data.

**Moderate- Impact System [FIPS 200]**

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate, and no security objective is assigned a FIPS 199 potential impact value of high.

**National Security Information**

Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

**National Security System [44 U.S.C., Sec. 3542]**

Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

**Net-Centric Architecture**

A complex system of systems composed of subsystems and services that are part of a continuously evolving, complex community of people, devices, information and services interconnected by a network that enhances information sharing and collaboration. Subsystems and services may or may not be developed or owned by the same entity, and, in general, will not be continually present during the full life cycle of the system of systems. Examples of this architecture include service- oriented architectures and cloud computing architectures.

**Operational Controls [FIPS 200]** The security controls (i.e., safeguards or countermeasures) for an Information system that are primarily implemented and executed by people (as opposed to systems).

**Organization [FIPS 200, Adapted]** An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency, or, as appropriate, any of its operational elements).

**Organizational Information Security Continuous Monitoring** Ongoing monitoring sufficient to ensure and assure effectiveness of security controls related to systems, networks, and cyberspace, by assessing security control implementation and organizational security status in accordance with organizational risk tolerance – and within a reporting structure designed to make real time, data driven risk management decisions.

**Patch Management** The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

**Penetration Testing** A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.

**Plan of Action & Milestones (POA&M) [OMB Memorandum 02-01]** A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

**Potential Impact [FIPS 199]** The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.

**Reciprocity** Mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.

**Records** The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

**Risk [FIPS 200, Adapted]**

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.[12]

**Risk Assessment**

The process of identifying risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

**Risk Executive (Function) [NIST SP 800-37]**

An individual or group within an organization that helps to ensure that: (i) security risk- related considerations for individual information systems, to include the authorization decisions, are viewed from an organization- wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing information system- related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with organizational risks affecting mission/business success.

**Risk Management**

The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk- related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

**Risk Monitoring**

Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.

**Risk Response**

Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or

[12] Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation. Adverse impacts to the nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.

reputation), organizational assets, individuals, other organizations, and the Nation.

**Risk Tolerance**
The level of risk an entity is willing to assume in order to achieve a potential desired result.

**Safeguards [CNSSI 4009]**
Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with *Security Controls and Countermeasures*.

**Security Authorization**
See *Authorization*.

**Security Categorization**
The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.

**Security Controls [FIPS 199]**
The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

**Security Control Assessment**
The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

**Security Control Assessor**
The individual, group, or organization responsible for conducting a security control assessment.

**Security Control Baseline [FIPS 200, Adapted]**
One of the sets of minimum security controls defined for federal information systems in NIST Special Publication 800-53 and CNSS Instruction 1253.

**Security Control Effectiveness**
The measure of correctness of implementation (i.e., how consistently the control implementation complies with the security plan) and by how well the security plan meets organizational needs in accordance with current risk tolerance.

**Security Control Enhancements**
Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.

**Security Control Inheritance**
A situation in which an information system or application receives protection from security controls (or portions of security

controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See *Common Control*.

**Security Domain [CNSSI 4009]**
A domain that implements a security policy and is administered by a single authority.

**Security Impact Analysis**
The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

**Security Management Dashboard [NIST SP 800-128]**
A tool that consolidates and communicates information relevant to the organizational security posture in near-real time to security management stakeholders.

**Security Objective [FIPS 199]**
Confidentiality, integrity, or availability.

**Security Plan**
Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See *System Security Plan* or *Information Security Program Plan*.

**Security Policy [CNSSI 4009]**
A set of criteria for the provision of security services.

**Security Posture**
The security status of an enterprise's networks, information, and systems based on IA resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

**Security Requirements [FIPS 200]**
Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

**Senior (Agency) Information Security Officer (SISO) [44 U.S.C., Sec. 3544]**
Official responsible for carrying out the Chief Information Officer responsibilities under the Federal Information Security Management Act (FISMA) and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. Note: Organizations subordinate to federal agencies may use the term *Senior Information Security Officer* or *Chief Information Security Officer* to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.

**Senior Information Security Officer** See *Senior Agency Information Security Officer*.

**Specification** An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system.

**Status Monitoring** Monitoring the information security metrics defined by the organization in the information security continuous monitoring strategy.

**Subsystem** A major subdivision of an information system consisting of information, information technology, and personnel that performs one or more specific functions.

**Supplementation (Assessment Procedures)** The process of adding assessment procedures or assessment details to assessment procedures in order to adequately meet the organization's risk management needs.

**Supplementation (Security Controls)** The process of adding security controls or control enhancements to a security control baseline from NIST Special Publication 800-53 or CNSS Instruction 1253 in order to adequately meet the organization's risk management needs.

**System** See *Information System*.

**System Security Plan [NIST SP 800-18]** Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

**System-Specific Security Control [NIST SP 800-37]** A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.

**System Development Life Cycle (SDLC)** The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

**Tailored Security Control Baseline** A set of security controls resulting from the application of tailoring guidance to the security control baseline. See *Tailoring*.

**Tailoring [NIST SP 800-53, CNSSI 4009]** The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization defined parameters in the security controls via explicit assignment and selection statements.

**Tailoring (Assessment Procedures)** The process by which assessment procedures defined in Special Publication 800-53A are adjusted, or scoped, to match the characteristics of the information system under assessment, providing organizations with the flexibility needed to meet specific organizational requirements and to avoid overly constrained assessment approaches.

**Technical Controls [FIPS 200]** The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

**Test** A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time.

**Threat [CNSSI 4009, Adapted]** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

**Threat Assessment [CNSSI 4009]** Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

**Threat Information** Information about types of attacks rather than specific threat actors.

**Threat Source [FIPS 200]** The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with Threat Agent.

**Vulnerability [CNSSI 4009]** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

**Vulnerability Assessment [CNSSI 4009]** Formal description and evaluation of the vulnerabilities in an information system.

**White Box Testing** See *Comprehensive Testing*.

# Appendix A  Security Requirements Traceability Matrix

**FVAP Security Requirement Traceability Matrix**

| | | |
|---|---|---|
| | **Pilot Program Testing Requirements Security Gap Analysis** | |
| **POC Name:** | **Michael Teribury (CALIBRE)** | **Jim Martin (CALIBRE)** |
| **POC Phone:** | **(703) 588-8104** | **(703) 588-1179** |
| **POC E-Mail:** | michael.teribury.ctr@fvap.gov | James.Martin@calibresys.com |
| **Last Update: Jan. 31, 2011** | | |

| **UOCAVA REQ. No.**<br>**(1)** | **UOCAVA TEST REQ.**<br>**(2)** | **TEST METHOD**<br>**(3)** | **TEST ENTITY**<br>**(4)** | **POTENTIAL IMPACT**<br>**(5)** |
|---|---|---|---|---|
| UOCAVA REQ.  Number from "UOCAVA Pilot Program Test Requirements" | UOCAVA Req. from "UOCAVA Pilot Program Test Requirements" | UOCAVA Req. Test Method: Functional or Inspection | Test Entity: EAC, Manufacturer, or VSTL | NIST SP800-30: The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability.<br>• System mission (e.g., the processes performed by the IT system)<br>• System and data criticality (e.g., the system's value or importance to an organization)<br>• System and data sensitivity.<br>**Rated on a Low, Midium or High Impact**<br>The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:<br>**Loss of Integrity.** System and data integrity refers to the requirement that information be protected from improper modification.<br>**Loss of Availability.** If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected.<br>**Loss of Confidentiality.** System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. |

LEGEND: TEST METHOD

A=ANALYSIS

D=DEMONSTRATION

I=INSPECTION

T=TEST

# FVAP SRTM DEFINITIONS & EXPLANATIONS

| | | | | | | | | | | Risk | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **VERIFICATION METHOD (6)** | **NIST Control No. (7)** | **IA Control Name (8)** | **ISO / IEC 17799 (9)** | **NIST SP800-26 (10)** | **GAO FISCAM (11)** | **DOD 8500.2 (12)** | **DCID 6/3 (13)** | **Related Control Guidance and References (14)** | **Mitagating IA Control (15)** | **Confidentiality** | **Integrity** |
| The method for determining if the requirement that is being satisfactorally met. Includes Demonstration, Inspection or Test | NIST Special Publications IA Control Family | NIST Special Publications IA Control Family Name | International Standard Organization and International Electrotechnical Commission Reference Number | NIST SP800-26 Security Self-Assessment Guide Reference | Government Accounting Office Federal Information System Control Audit Manual | Depart of Defense 8500.1/2 IA guidance | Director of Central Intelligence Directive 6/3 | Other federal, industy or international IA guidance applicable to this UOCAVA Pilot Program Testing Requirement | FVAP internal/external compensating control | See tab 3 CIA Triad | See tab 3 CIA Triad |

## Gap Risk Analysis

| | | Impact Rating | | | Compliant | | | |
|---|---|---|---|---|---|---|---|---|
| **Availability** | **Mitigated** | **Low** | **Medium** | **High** | **Yes** | **No** | **No available reference** | **Functional Requirement** |
| See tab 3 CIA Triad | This UOCAVA Pilot Program Testing Requirement has been mitigated through another security control | See tab 3 CIA Triad | See tab 3 CIA Triad | See tab 3 CIA Triad | UOCAVA Pilot Program Testing Requirement meets guidance | UOCAVA Pilot Program Testing Requirement does NOT meet guidance | None of the seven guidance documents has a direct reference to this UOCAVA test requirement | This is a UOCAVA test requirement that is functional and does not have a security related component |

FVAP

**FVAP Security Requirement Traceability Matrix**

**Pilot Program Testing Requirements Security Gap Analysis**

**Last Update: Jan. 31, 2011**

LEGEND: TEST METHOD

A=ANALYSIS

D=DEMONSTRATION

I=INSPECTION

T=TEST

## FVAP SRTM DEFINITIONS & EXPLANATIONS

**Gap Risk Analysis**

| | | | | | | | | | | | | | | Risk | | | | Impact Rating | | | Compliant | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| UOCAVA REQ. No. (1) | UOCAVA TEST REQ. (2) | TEST METHOD (3) | TEST ENTITY (4) | POTENTIAL IMPACT (5) | VERIFICATION METHOD (6) | NIST Control No. (7) | IA Control Name (8) | ISO / IEC 17799 (9) | NIST SP800-26 (10) | GAO FISCAM (11) | DOD 8500.2 (12) | DCID 6/3 (13) | Related Control Guidance and References (14) | Mitagating IA Control (15) | Confidentiality | Integrity | Availability | Mitigated | Low | Medium | High | Yes | No | No available reference | Functional Requirement | Reconciled in other documentation (Yes or No) | Identified Reference Documentation |
| 4.3.1.2 Module testability | Each module SHALL have a specific function that can be tested and verified independently from the remainder of the code. | Inspection | Manufacturer | Relates to software integrity | I=INSPECTION | None | None | None | None | None | None | None | None | No reference documentation identified. | | 1 | | | | 1 | | | | | 1 | Yes | Found in Voting Systems Standards produced by the EAC. Other references relate to cryptographic modules within NIST Guidance and FIPS |
| 4.3.1.3 Module size and identification | Modules SHALL be small and easily identifiable. | Inspection | Manufacturer | Relates to software integrity | I=INSPECTION | None | None | None | None | None | None | None | Nonme | N/A | | 1 | | | | 1 | | | | 1 | 1 | Yes | Good coding practices woud dictate that modules be easily identified. The IEEE Software Engineering Body of Knowledge (SWEBOK) provides exception guidance and best practice knowledge that has been vetted by hundreds of industry experts. However, none of the additional reference documents speak to size of the modules. |
| 4.7.2.7 Nullify freed pointers | If pointers are used, any pointer variables that remain within scope after the memory they point to is deallocated SHALL be set to null or marked as invalid (pursuant to the idiom of the programming language used) after the memory they point to is deallocated. | Inspection | Manufacturer | Integrity and Availability: Relates to software quality and best programming practices. No specific security control. | I=INSPECTION | None | None | None | None | None | None | None | None | None | | 1 | 1 | | | 1 | | | | 1 | | No | Good coding practices woud dictate that all Null Pointers are reset. Additionally, there are specific requirements that agencies must follow when implementing cookies. See OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, available at: http://www.whitehouse.gov/omb/memoranda/m03-22.html. |
| 4.7.2.11 Election integrity monitoring | The voting system SHALL proactively detect or prevent basic violations of election integrity (e.g., stuffing of the ballot box or the accumulation of negative votes) and alert an election official or administrator if such violations they occur. | Inspection | Manufacturer | N/A to IT Security capability | I=INSPECTION | None | None | None | None | None | None | None | None Identified | N/A | | 1 | | | | 1 | | | | 1 | 1 | Yes | A requirement of 4.1.4 of The Voting Over the Internet Pilot Project 2001. |
| 5.4.1.2 Cast vote integrity; storage | The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage. | Functional | VSTL | Functional Requirement. Loss of Integrity. | T=TEST | None | None | None | None | None | None | None | Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006. | N/A | | 1 | | | | | 1 | 1 | | 1 | | Yes | Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006. |
| 5.4.1.3 Cast vote storage | Cast vote data SHALL NOT be permanently stored on the vote capture device. | Functional | VSTL | Functional Requirement. Loss of Integrity. | T=TEST | None | None | None | None | None | None | None | Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006. | N/A | | 1 | | | | | 1 | | | 1 | 1 | Yes | Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006. |
| 5.4.1.4 Electronic ballot box integrity | The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature. | Functional | VSTL | Functional Requirement. Loss of Integrity and/or Confidentiality. | T=TEST | None | None | None | None | None | None | None | Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006. | N/A | | 1 | | | | | 1 | | | 1 | 1 | Yes | Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006. |
| 6.2 Components from Third Parties | A manufacturer who does not manufacture all the components of its voting system, but instead procures components as standard commercial items for assembly and integration into a voting system, SHALL verify that the supplier manufacturers follow documented quality assurance procedures that are at least as stringent as those used internally by the voting system manufacturer. | Inspection | Manufacturer | loss of Integrity, availability and/or Confidentiality | I=INSPECTION | None | None | None | None | None | None | None | Nothing found in referencfed documentation. However, this may be referenced within another publication involving acquisitions. | N/A | 1 | 1 | 1 | | | 1 | | | | 1 | | Yes | The June 2010 Accessibility and Usability Consideration of Remote Voting Systems DRAFT Whitepaper prepared by NIST discusses 3rd party components. It specifically recommends that "design and test voting system components against standards and guidelines for interoperability and test all likely configurations." |
| 6.3 Responsibility for Tests | Manufacturer SHALL be responsible for performing all quality assurance tests, acquiring and documenting test data, and providing test reports for examination by the VSTL as part of the national certification process. These reports SHALL also be provided to the purchaser upon request. | Inspection | Manufacturer | loss of Integrity or availability | I=INSPECTION | None | None | None | None | None | None | None | Nothing found in referencfed documentation. However, this may be referenced within another publication involving acquisitions. | N/A | | 1 | 1 | | | 1 | | | | 1 | | No | No reference materials define responsibility for manufacturer to test systems. |
| 7.5.2 Functional Configuration Audit (FCA) | The Functional Configuration Audit is conducted by the VSTL to verify that the voting system performs all the functions described in the system documentation. Manufacturers SHALL: a. Completely describe its procedures and related conventions used to support this audit for all voting system components; and b. Provide the following information to support this audit: c. Copies of all procedures used for module or unit testing, integration testing, and system testing; d. Copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for system tests; and e. Records of all tests performed by the procedures listed above, including error corrections and retests. | Functional / Inspection | VSTL | Configuration/Testing | I=INSPECTION | None | None | None | None | None | None | None | | N/A | 1 | 1 | 1 | | | 1 | | | | 1 | | Yes | Technical Guidelines Development Committee to the Election Assistance Commission: A reference was located in Chapter 4: Documentation and Design Reviews (Inspection) under section 4.1-A Applies to Voting Systems: An accredited test lab SHALL verify that the documentation submitted by the manufacturer in the TDP meets all the requirements applicable to the TDP, is sufficient to enable the inspections specified in this chapter, and is sufficient to enable tests specified. |
| 8.2.1 TDP Implementation Statement | The TDP SHALL include an implementation statement. | Inspection | Manufacturer | Documentation | I=INSPECTION | None | None | None | None | None | None | None | None | N/A | | | 1 | | 1 | | | | | 1 | 1 | Yes | This requirement is only mentioned in the VVSG Recommendations to the EAC in Chapter 2-10. |
| 8.3.4.1 Hardwired and mechanical implementations of logic | For each non-COTS hardware component (e.g., an application-specific integrated circuit or a manufacturer-specific integration of smaller components), manufacturers SHALL provide complete design and logic specifications, such as Computer Aided Design and Hardware Description Language files. | Inspection | Manufacturer | Industrial controll logic could impact Confidentiality, Integrity and/or Availability. | I=INSPECTION | None | None | None | None | None | None | None | NIST SP800-53 Reference: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes. | Full Documentation of boarder logic and identification of all devices. Border logic should be minimized. | 1 | 1 | 1 | | | | 1 | | | 1 | | No | This falls under "border Logic" within the definition found in Appendix A of VVSG-0807. This does represent a significant threat to integrity and confidentiality. |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8.3.4.2 Logic specifications for PLDs, FPGAs and PICs | For each Programmable Logic Device (PLD), Field-Programmable Gate Array (FPGA), or Peripheral Interface Controller (PIC) that is programmed with non- COTS logic, manufacturers SHALL provide complete logic specifications, such as Hardware Description Language files or source code. | Inspection | Manufacturer | Industrial controll logic could impact Confidentiality, Integrity and/or Availability. | I=INSPECTION | None | None | None | None | None | None | None | NIST SP800-53 Reference: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes. | Full Documentation of boarder logic and identification of all devices. Border logic should be minimized. | 1 | 1 | 1 | | | | 1 | | | 1 | | No | This falls under "border Logic" within the definition found in Appendix A of VVSG-0807. This does represent a significant threat to integrity and confidentiality. |
| 8.4.5.3 Justify coding conventions | Manufacturers SHALL furnish evidence that the selected coding conventions are "published" and "credible" as specified in section 4.3.1. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan under "robustness". Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | None | None | None | None | None | None | None | NIST SP800-137 References coding practices. DCID 6/3: 1.H.1 In the following pages, the term "good engineering practice" refers to the state of the engineering art for commercial systems that have equivalent problems and solutions; a good engineering practice by definition meets commercial requirements. These practices are usually part of the normal installation and operating procedures for systems. When placing security reliance on items that implement good engineering practice (such as commercial off-the shelf [COTS] software), the DAAs or their designees shall verify that the item(s) are set up properly and are operating as | Full Documentation of boarder logic and identification of all devices, manufacturer and design. | 1 | 1 | 1 | | | 1 | | | | 1 | | No | There is a discussion DRAFT posted on Dec. 1, 2006 regarding coding convention and logic verification that was prepared by NIST for the TGDC. This paper outlines specific requirements and guidance for coding best practices. |
| 8.4.6.1 Application logic operating environment | Manufacturers SHALL describe or make reference to all operating environment factors that influence the design of application logic. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan under "robustness". Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | None | None | None | None | None | None | None | None | PE-1 through PE-19 define environmental controls and related requirrements. | 1 | 1 | 1 | | | 1 | | | | 1 | | Yes | NIST SP800-18 provides guidance for operating environements. |
| 8.4.7.1 Hardware environment and constraints | Manufacturers SHALL identify and describe the hardware characteristics that influence the design of the application logic, such as: a. Logic and arithmetic capability of the processor; b. Memory read-write characteristics; c. External memory device characteristics; d. Peripheral device interface hardware; e. Data input/output device protocols; and f. Operator controls, indicators, and displays. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan under "robustness". Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | None | None | None | None | None | None | None | None | PE-1 through PE-19 define environmental controls and related requirrements. | 1 | 1 | 1 | | 1 | | | | | 1 | | Yes | NIST SP800-18 provides guidance for operating environements. |
| 8.4.8.2 Compilers and assemblers | For systems containing compiled or assembled application logic, manufacturers SHALL identify the COTS compilers or assemblers used in the generation of executable code, and the specific versions thereof. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | None | None | None | None | None | None | None | None. Only references backups should provide for the protection of compilers. | None. Only references backups should provide for the protection of compilers. | 1 | 1 | 1 | | 1 | | | | | 1 | | Yes | The TGDC Recommendations from August, 2007 specify requirements. There are numerous IEEE standards and requirements defined that relate to compilers and assemblers. |
| 8.4.8.3 Interpreters | For systems containing interpreted application logic, manufacturers SHALL specify the COTS runtime interpreter that SHALL be used to run this code, and the specific version thereof. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | None | None | None | None | None | None | None | None. Only references backups should provide for the protection of compilers. | None. Only references backups should provide for the protection of compilers. | 1 | 1 | 1 | | 1 | | | | | 1 | | No | No specific NIST or IEEE requirement located. |
| 8.4.9.1 Application logic functional specification | Manufacturers SHALL provide a description of the operating modes of the system and of application logic capabilities to perform specific functions. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | None | None | None | None | None | None | None | None | None | 1 | 1 | 1 | | 1 | | | | | 1 | | No | No specific NIST or IEEE requirement located. |
| 9.2.3.3 Traceability of procured software | The system description SHALL include a declaration that procured software items were obtained directly from the manufacturer or from a licensed dealer or distributor. | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | None | None | None | None | None | None | None | | | 1 | 1 | 1 | | | 1 | | | | 1 | | Yes | The DOE has a specific requirement for traceability of procured software. |
| 9.4.5.1 Ballot count and vote total auditing | The system's user documentation SHALL fully specify a secure, transparent, workable and accurate process for producing all records necessary to verify the accuracy of the electronic tabulation result. | Inspection | Manufacturer | Loss of data Integrity | I=INSPECTION | None | None | None | None | None | None | None | None | None | 1 | 1 | 1 | | | | 1 | | | 1 | | Yes | IEEE P1583 speaks to voting system standards for election accuracy, and auditable results. |
| 9.5.1.4 Election specific software identification | Manufacturers SHALL identify election specific software in the user documentation. | Inspection | Manufacturer | No securiyt impact | I=INSPECTION | None | None | None | None | None | None | None | None | Special denotation within the supplied documentation | | 1 | | | | 1 | | | | 1 | | No | This requirement is not clear as to its meaning. Now references available. However, this is a good security practice and should be followed. |
| 9.5.1.7 Compiler installation prohibited | The software installation procedures used to install software on programmed devices of the system SHALL specify that no compilers SHALL be installed on the programmed device. | Inspection | Manufacturer | No direct security implication of this addition to the documentation. However, installation of compilers could impact confidentiality, availablity and integrity. | I=INSPECTION | None | None | None | None | None | None | None | End user software is prohibited. However, no specific guidance on compilers within the referenced documetation. | None | 1 | 1 | 1 | | | 1 | | | | 1 | | No | Now references available. However, this is a good security practice and should be followed. |
| 9.6.1.2 Setup inspection record generation | The setup inspection process SHALL describe the records that result from performing the setup inspection process. | Inspection | Manufacturer | This requirement could impact Confidentiality and/or integrity and availability. | I=INSPECTION | None | None | None | None | None | None | None | NIST SP800-100 States: In addition, developing a security requirements checklist based on the security requirements specified for the system during the conceptual, design, and implementation phases of the SDLC can be used to provide a 360-degree inspection of the system. | None | 1 | 1 | 1 | | | 1 | | | | 1 | | No | No specific reference documentation for this requirement. |
| 9.6.1.12 Consumables quantity of vote capture device | Manufacturers SHALL provide a list of consumables associated with the vote capture device, including estimated number of usages per quantity of consumable. | Inspection | Manufacturer | No known security risk. | I=INSPECTION | None | None | None | None | None | None | None | No specific IA Control referenced. | None | | | 1 | | 1 | | | | | 1 | | No | This is specific to the voting system. NIST H143 makes a brief reference to consumables. However, this is a reasponable requirement. Media storage is a requirement of NIST guidance for DIACAP, and while it is not specifically mentioned, it would be reasonable to assume that it would fall under this guidance. |
| 9.6.1.13 Consumable inspection procedure | Manufacturers SHALL provide the procedures to inspect the remaining amount of each consumable of the vote capture device. | Inspection | Manufacturer | No known security risk. | I=INSPECTION | None | None | None | None | None | None | None | No specific IA Control referenced. | None | | | 1 | | 1 | | | | | 1 | | No | This is specific to the voting system. NIST H143 makes a brief reference to consumables. However, this is a reasponable requirement. Media storage is a requirement of NIST guidance for DIACAP, and while it is not specifically mentioned, it would be reasonable to assume that it would fall under this guidance. |
| 9.6.1.14 Calibration of vote capture device components nominal range | Manufacturers SHALL provide a list of components associated with the vote capture devices that require calibration and the nominal operating ranges for each component. | Inspection | Manufacturer | No known security risk. | I=INSPECTION | None | None | None | None | None | None | None | No specific IA Control referenced. | None | | 1 | | | | 1 | | | | 1 | | No | This should fall under the SSP guidance. However, this is election specific, and no other reference documentation was located. |
| 9.6.1.15 Calibration of vote capture device components inspection procedure | Manufacturers SHALL provide the procedures to inspect the calibration of each component. | Inspection | Manufacturer | No known security risk. | I=INSPECTION | None | None | None | None | None | None | None | No specific IA Control referenced. | None | | 1 | | | | 1 | | | | 1 | | Yes | This is a HAVA requirement under Quality Assurance and Configuration Management. |

FVAP Security Requirement Traceability Matrix

UOCAVA Pilot Program Testing Requirements Security Gap Analysis

| | | |
|---|---|---|
| POC Name: | | |
| POC Phone: | | |
| POC E-Mail: | | |

Last Update: Jan.31, 2011

LEGEND: TEST METH

A=ANALYSIS

D=DEMONSTRATION

I=INSPECTION

T=TEST

| | | | | | | | | | | | | | | Gap Risk Analysis | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | Risk | | | | Impact Rating | | | Compliant | | | | Recommended Technical or UOCAVA Requirement Change<br>N/C = No Change |
| UOCAVA REQ. No. (1) | UOCAVA TEST REQ. (2) | TEST METHOD (3) | TEST ENTITY (4) | POTENTIAL IMPACT (5) | VERIFICATION METHOD (6) | NIST Control No. (7) | IA Control Name (8) | ISO / IEC 17799 (9) | NIST SP800-26 (10) | GAO FISCAM (11) | DOD 8500.2 (12) | DCID 6/3 (13) | Related Control Guidance and References (14) | Mitagating IA Control (15) | Confidentiality | Integrity | Availability | Mitigated | Low | Medium | High | Yes | No | No available reference | Functional Requirement | |
| 2.1.1.1 Component accuracy | Memory hardware, such as semiconductor devices and magnetic storage media, SHALL be accurate. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST & Demonstration | MP-1 | Media Protection Policy and Procedures | 10.1.1<br>10.7<br>15.1.1<br>15.1.3 | 8.2 | --- | PESP-1<br>DCAR-1 | DCID: B.2.a Manual: 2.B.6.c(7) 8.B.2 | | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 2.1.1.2 Equipment design | The design of equipment in all voting systems SHALL provide for protection against mechanical, thermal, and electromagnetic stresses that impact voting system accuracy. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST & Demonstration | MP-2 | Media Access | 10.7.3 | 8.2.1; 8.2.2; 8.2.3; 8.2.6; 8.2.7 | --- | PEDI-1; PEPF-1 | 2.B.9.b(4); 4.B.1.a(1); 4.B.1.a(7) | | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 2.1.1.3 Voting system accuracy | To ensure vote accuracy, all voting systems SHALL: a. Record the election contests, candidates, and issues exactly as defined by election officials; b. Record the appropriate options for casting and recording votes; c. Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast; d. Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the voting system has been designed for accuracy; and e. Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST & Demonstration | SI-10 | Information Accuracy, Completeness, Validity, and Authenticity | 10.7.3; 12.2.1; 12.2.2 | --- | --- | --- | 7.B.2.h; 2.B.4.d | | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 2.1.2 Environmental Range | All voting systems SHALL meet the accuracy requirements over manufacturer specified operating conditions and after storage under non-operating conditions. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST & Demonstration | None | None | None | None | None | None | None | FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-100. Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family. Related security controls: MP-4, MP-5. | The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy. | 1 | 1 | 1 | | | | 1 | | | | 1 | N/C |
| 2.1.3.1 Election management system accuracy | Voting systems SHALL accurately record all election management data entered by the user, including election officials or their designees. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST & Demonstration | PL-3 | System Security Plan Update | 6.1 | 3.2.10; 5.2.1 | SP-2.1 | 5.7.5 | 2.B.7.c(5) | | Significant changes are defined in advance by the organization and identified in the configuration management process. NIST Special Publication 800-18 provides guidance on security plan updates. | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 2.1.3.2 Recording accuracy | For recording accuracy, all voting systems SHALL: a. Record every entry made by the user except where it violates voter privacy; b. Accurately interpret voter selection(s) and record them correctly to memory; c. Verify the correctness of detection of the user selections and the addition of the selections correctly to memory; d. Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory; and e. Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST & Demonstration | SI-10 | Information Accuracy, Completeness, Validity, and Authenticity | 10.7.3; 12.2.1; 12.2.2 | --- | --- | --- | 7.B.2.h; 2.B.4.d | | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 2.1.4 Telecommunications Accuracy | The telecommunications components of all voting systems SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST & Demonstration | None | None | None | None | None | None | None | | | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 2.1.5.1 Simulators | If a simulator is used, it SHALL be verified independently of the voting system in order to produce ballots as specified for the accuracy testing. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. Inaccurate testing with potential false validation of results. | A=ANALYSIS | None | None | None | None | None | None | None | | | 1 | 1 | 1 | | | | 1 | | | | 1 | N/C |
| 2.1.5.2 Ballots | Ballots used for accuracy testing SHALL include all the supported types (i.e., rotation, alternative languages) of contests and election types (primary, general). | Functional | VSTL | Functional requirement with no direct security impact. | T=TEST & Demonstration | None | None | None | None | None | None | None | | | | 1 | | | | 1 | | | | | 1 | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2.1.6 Reporting Accuracy | Processing accuracy is defined as the ability of the voting system to process stored voting data. Processing includes all operations to consolidate voting data after the voting period has ended. The voting systems SHALL produce reports that are consistent, with no discrepancy among reports of voting data. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST & Demonstration | SI-7 | Software and Information Integrity | 12.2.1; 12.2.2; 12.2.4 | 11.2.1; 11.2.4 | --- | ECSD-2 | 4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6) | ECAT-2 Audit Trail, Monitoring, Analysis and Reporting;<br>ECTP-1 Audit Trail Protection<br>SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY | N/A | | 1 | | | | | 1 | 1 | | | | N/C |
| 2.2.1 Maximum Capacities | The manufacturer SHALL specify at least the following maximum operating capacities for the voting system (i.e. server, vote capture device, tabulation device, and communications links): Throughput, Memory, Transaction processing speed, and Election constraints: Number of jurisdictions Number of ballot styles per jurisdiction Number of contests per ballot style Number of candidates per contest Number of voted ballots | Functional | VSTL | No direct security impact | T=TEST & Demonstration | None | None | None | None | None | None | None | | N/A | | | | | 1 | | | | | | 1 | N/C |
| 2.2.1.1 Capacity testing | The voting system SHALL achieve the maximum operating capacities stated by the manufacturer in section 2.2.1. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST & Demonstration | None | None | None | None | None | None | None | | | 1 | 1 | 1 | | | | 1 | | | | 1 | N/C |
| 2.2.2 Operating Capacity notification | The voting system SHALL provide notice when any operating capacity is approaching its limit. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST & Demonstration | None | None | None | None | None | None | None | | | 1 | 1 | 1 | | | | 1 | | | | 1 | N/C |
| 2.2.3 Simultaneous Transmissions | The voting system SHALL protect against the loss of votes due to simultaneous transmissions. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST & Demonstration | SC-8 | Transmission Integrity | 10.6.1; 10.8.1; 10.9.1 | 11.2.1; 11.2.4; 11.2.9; 16.2.14 | AC-3.2 | ECTM-1 Transmission Integrity Controls ECTM-2 Transmission Integrity Controls | 5.B.3.a(11) | NIST Special Publication 800-52 provides guidance on protecting transmission integrity using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission integrity using IPsec. NIST Special Publication 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. Others include: FIPS 198; NIST Special Publications 800-44, 800-45, 800-49, 800-52, 800-57, 800-54, 800-58, 800-66, 800-77, 800-81, 800-95, 800-97 | N/A | | 1 | | | | | 1 | 1 | | | | N/C |
| 2.3.1.1 Import the election definition | The voting system SHALL: a. Keep all data logically separated by, and accessible only to, the appropriate state and local jurisdictions; b. Provide the capability to import or manually enter ballot content, ballot instructions and election rules, including all required alternative language translations from each jurisdiction; c. Provide the capability for the each jurisdiction to verify that their election definition was imported accurately and completely; d. Support image files (e.g., jpg or gif) and/or a handwritten signature image on the ballot so that state seals, official signatures and other graphical ballot elements may be properly displayed; and e. Support multiple ballot styles per each local jurisdiction. | Inspection / Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST & Demonstration | PE-2<br>AC-5<br>SEPARATION OF DUTIES | Physical Access Authorizations | 9.1.2; 9.1.6; 10.1.3; 10.6.1; 10.10.1 | 7.1.1; 7.1.2; 6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5 | AC-3.1; AC-3.2; SD-1.2 | PECF-1<br>DCPA-1 Partitioning the Application<br>ECCD-2 Changes to Data<br>PRAS-2 Access to Information<br>ECLP-1 | 4.B.1.a(1); 8.E; 2.A.1; 4.B.3.a(18) | The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions. | Discretionary Access Control (DAC). A means of restricting access to an object (e.g., files, data entities) based on the identity and need-to-know of a subject (e.g., user, process) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) to any other subject (unless restrained by a mandatory access control). | 1 | 1 | 1 | | | 1 | | 1 | | | | Graphic formats are subject to corruption and remote code execution when malformed. Graphic file formats should be evaluated for potential risks and vulnerabilities. Appropriate Microsoft security bulletins and patches should be updated prior to elections. |
| 2.3.1.2 Protect the election definition | The voting system SHALL provide a method to protect the election definition from unauthorized modification. | Functional | VSTL | A loss of integrity is the unauthorized modification or destruction of information.Information, the loss, misuse, or unauthorized access to or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code, | T=TEST & Demonstration | SI-7 | Software and Information Integrity | 12.2.1; 12.2.2; 12.2.4 | 11.2.1; 11.2.4 | --- | ECSD-2 | 4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6) | | Information Security [44 U.S.C., Sec. 3542] The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.Integrity [44 U.S.C., Sec. 3542] Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. | 1 | 1 | | | | | 1 | 1 | | | | Does not specify how this is to be accomplished. No recommendation |
| 2.3.2.1 Voting system test mode | The voting system SHALL provide a test mode to verify that the voting system is correctly installed, properly configured, and all functions are operating to support pre-election readiness testing for each jurisdiction. | Functional | VSTL | A system self test. NIST has SP800-126 Rev. 1 DRAFT Technical Specifications for the Security Content Automation Protocol (SCAP) that may relate testing requirements and specifications for security software flaws. | T=TEST & Demonstration | None | None | None | None | None | None | None | | No specific findings for diagnostics or test mode analysis. Howvever, remote diagnostic is mentioned. | 1 | 1 | 1 | | | | 1 | | | | 1 | N/C |
| 2.3.2.2 Test data segregation | The voting system SHALL provide the capability to zero-out or otherwise segregate test data from actual voting data. | Functional | VSTL | Functional test. | T=TEST & Demonstration | None | None | None | None | None | None | None | | | 1 | 1 | 1 | | | 1 | | | | | 1 | N/C |
| 2.4.1.1 Accessing the ballot | The voting system SHALL: a. Present the correct ballot style to each voter; b. Allow the voting session to be canceled; and c. Prevent a voter from casting more than one ballot in the same election. | Functional | VSTL | Functional test. | T=TEST & Demonstration | None | None | None | None | None | None | None | | | 1 | 1 | 1 | | | | 1 | | | | 1 | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2.4.2.1 Record voter selections | The voting system SHALL: a. Record the selection and non-selection of individual vote choices; b. Record the voter's selection of candidates whose names do not appear on the ballot, if permitted under state law, and record as many write-ins as the number of candidates the voter is allowed to select; c. Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources); d. Allow the voter to change a vote within a contest before advancing to the next contest; e. Provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance; f. Indicate to the voter when no selection, or an insufficient number of selections, has been made for a contest (e.g., undervotes); g. Provide the voter the opportunity to correct the ballot for an undervote before the ballot is cast; h. Allow the voter, at the voter's choice, to submit an undervoted ballot without correction. i. Prevent the voter from making more than the allowable number of selections for any contest (e.g., overvotes); and j. In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume voting once the voting system has reverted to back-up power. | Functional | VSTL | Functional test. | D=DEMONSTRATION | None | None | None | None | None | None | None | | | 1 | 1 | 1 | | | | 1 | | | | 1 | N/C |
| 2.4.2.2 Verify voter selections | The voting system SHALL: a. Produce a paper record each time the confirmation screen is displayed; b. Generate a paper record identifier. This SHALL be a random identifier that uniquely links the paper record with the cast vote record; c. Allow the voter to either cast the ballot or return to the vote selection process to make changes after reviewing the confirmation screen and paper record; and d. Prompt the voter to confirm his choices before casting the ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm his intention to cast the ballot. | Functional | VSTL | Functional test. | D=DEMONSTRATION | None | None | None | None | None | None | None | | | 1 | 1 | 1 | | | | 1 | | | | 1 | N/C |
| 2.4.2.3 Cast ballot | The voting system SHALL: a. Store all cast ballots in a random order; logically separated by, and only accessible to, the appropriate state/local jurisdictions; b. Notify the voter after the vote has been stored persistently that the ballot has been cast; c. Notify the voter that the ballot has not been cast successfully if it is not stored successfully, and provide clear instruction as to steps the voter should take to cast his ballot should this event occur; and d. Prohibit access to voted ballots until such time as state law allows for processing of absentee ballots. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | PE-2<br>AC-5<br>SEPARATION OF DUTIES | Physical Access Authorizations | 9.1.2; 9.1.6; 10.1.3; 10.6.1; 10.10.1 | 7.1.1; 7.1.2; 6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5 | AC-3.1; AC-3.2; SD-1.2 | PECF-1<br>DCPA-1<br>Partitioning the Application<br>ECCD-2<br>Changes to Data<br>PRAS-2<br>Access to Information<br>ECLP-1 | 4.B.1.a(1); 8.E; 2.A.1; 4.B.3.a(18) | The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions. | Discretionary Access Control (DAC). A means of restricting access to an object (e.g., files, data entities) based on the identity and need-to-know of a subject (e.g., user, process) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) to any other subject (unless restrained by a mandatory access control). | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 2.4.2.4.1 Absentee model | The cast ballot SHALL be linked to the voter's identity without violating the privacy of the voter. | Functional | VSTL | Privacy requirements and Audit Trail Requirements | D=DEMONSTRATION | None | None | None | None | None | None | None | | National Institute of Standards and Technology Federal Information Processing Standards Publication 201-1, Personal Identity Verification of Federal Employees and Contractors, March 2006. | 1 | 1 | | | | | 1 | | | | 1 | N/C |
| 2.4.2.4.2 Early voting model | The cast ballot SHALL NOT be linked to the voter's identity. | Inspection | VSTL | Privacy requirements and Audit Trail Requirements | D=DEMONSTR | None | None | None | None | None | None | None | | | 1 | | | | | | 1 | | | | 1 | N/C |
| 2.4.3.1 Link to voter | The voting system SHALL be capable of producing a cast vote record that does not contain any information that would link the record to the voter. | Functional | VSTL | Integrity: Privacy requirements and Audit Trail Requirements | D=DEMONSTR | None | None | None | None | None | None | None | | | 1 | | | | | | 1 | | | | 1 | N/C |
| 2.4.3.2 Voting session records | The voting system SHALL NOT store any information related to the actions performed by the voter during the voting session. | Functional | VSTL | Integrity: Privacy requirements and Audit Trail Requirements | T=TEST & Demonstration | None | None | None | None | None | None | None | | | 1 | 1 | | | | | 1 | | | | 1 | N/C |
| 2.5.1.1 Seal and sign the electronic ballot box | The voting system SHALL seal and sign each jurisdiction's electronic ballot box, by means of a digital signature, to protect the integrity of its contents. | Functional | VSTL | Integrity: Privacy requirements and Audit Trail Requirements | T=TEST & Demonstration | None | None | None | None | None | None | None | NIST FIPS 140-2 validated cryptography (e.g., DoD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards should be applied as they become available. | National Institute of Standards and Technology Federal Information Processing Standards Publication 186-2, Digital Signature Standard (DSS), January 2000. National Institute of Standards and Technology Federal Information Processing Standards Publication 186-3 (Draft), Digital Signature Standard (DSS), March 2006. National Institute of Standards and Technology Special Publication 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications November 2006. | | 1 | | | | | 1 | | | | 1 | N/C |
| 2.5.1.2 Electronic ballot box retrieval | The voting system SHALL allow each jurisdiction to retrieve its electronic ballot box. | Functional | VSTL | Functional Requirement | T=TEST & Demonstration | None | None | None | None | None | None | None | | | 1 | 1 | 1 | | | | 1 | | | | 1 | N/C |
| 2.5.1.3 Electronic ballot box integrity check | The voting system SHALL perform an integrity check on the electronic ballot box verifying that it has not been tampered with or modified before opening. | Functional | VSTL | Functional Requirement | T=TEST & Demonstration | None | Physical Access Control | None | None | None | None | None | | | 1 | 1 | 1 | | | | 1 | | | | 1 | N/C |
| 2.5.2.1 Tabulation device connectivity | The tabulation device SHALL be physically, electrically, and electromagnetically isolated from any other computer network. | Inspection | VSTL | Functional Requirement related to a loss of integrity | T=TEST & Demonstration | None | None | None | None | None | DCSP-1<br>EBBD-2 | None | DCSP-1 Security Support Structure Partitioning: The security support structure is isolated by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions. The security support structure maintains separate execution domains (e.g., address spaces) for each executing process. EBBD-2 Boundary Defense Boundary: defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, at layered or internal enclave boundaries and at key points in the network, as required. All Internet access is proxied through Internet access points that are under the management and control of the enclave and are isolated from other DoD information systems by physical or technical means. | Control: The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk. | 1 | 1 | 1 | | | 1 | | | | | 1 | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2.5.2.2 Open ballot box | The tabulation device SHALL allow only an authorized entity to open the ballot box. | Functional | VSTL | Functional Requirement related to a loss of confidentiality due to physical access | T=TEST & Demonstration | PE-1<br>PE-2<br>PE-3<br>PE-6 | Physical and Environmental Protection Policy and Procedures | 15.1.1 | 7 | PETN-1; DCAR-1 | DCID: B.2.a; Manual: 2.B.4.e(5) | 8.D | PECF-2 Access to Computing Facilities Only authorized personnel with appropriate clearances are granted physical access to computing facilities that process classified information.PECF-1 Access to Computing Facilities Only authorized personnel with a need-to-know are granted physical access to computing facilities that process sensitive information or unclassified information that has not been cleared for release. PEPF-1 Physical Protection of Facilities Every physical access point to facilities housing workstations that process or display sensitive information or unclassified information that has not been cleared for release is controlled during working hours and guarded or locked during non-work hours. | Control: The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials [Assignment: organization-defined frequency, at least annually]. | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 2.5.2.3.1 Adjudication | The tabulation device SHALL allow the designation of electronic ballots as "accepted" or "not accepted" by an authorized entity. | Functional | VSTL | Functional Requirement related to Operations and Integrity. No specific security control identified. | T=TEST & Demonstration | None | None | None | None | None | None | None | | | | 1 | | | | | 1 | | | | 1 | N/C |
| 2.5.2.4 Ballot decryption | The tabulation device decryption process SHALL remove all layers of encryption and breaking all correlation between the voter and the ballot, producing a record that is in clear text. | Functional | VSTL | Functional Requirement related to Operations and Confidentiality. No specific security control identified. | T=TEST & Demonstration | None | None | None | None | None | None | None | | | 1 | 1 | | | | | 1 | | | | 1 | N/C |
| 2.5.2.5 Tabulation report format | The tabulation device SHALL have the capability to generate a tabulation report of voting results in an open and non-proprietary format. | Functional | VSTL | Functional Requirement related to Operations. No specific security control identified. | T=TEST & Demonstration | None | None | None | None | None | None | None | | | 1 | 1 | | | | | 1 | | | | 1 | N/C |
| 2.6.2.1 All records capable of being exported | The voting system SHALL provide the capability to export its electronic records in an open format, such as XML, or include a utility to export log data into a publicly documented format. | Functional | VSTL | Functional Requirement related to Operations. No specific security control identified. | T=TEST & Demonstration | None | None | None | None | None | None | None | | | 1 | 1 | | | | 1 | | | | | 1 | N/C |
| 2.6.2.2 Ballot images | The voting system SHALL have the capability to generate ballot images in a human readable format. | Functional | VSTL | Functional Requirement related to Operations. No specific security control identified. | T=TEST & Demonstration | None | None | None | None | None | None | None | | | 1 | | | | | 1 | | | | | 1 | Ballot Image format should meet security requirements in 2.3.1.1 |
| 2.6.2.3 Ballot image content | The voting system SHALL be capable of producing a ballot image that includes: a. Election title and date of election; b. Jurisdiction identifier; c. Ballot style; d. Paper record identifier; and e. For each contest and ballot question: i. The choice recorded, including write-ins; and ii. Information about each write-in. | Functional | VSTL | Functional Requirement related to Operations. No specific security control identified. | T=TEST & Demonstration | None | None | None | None | None | None | None | | | 1 | 1 | | | | | 1 | | | | 1 | Ballot Image format should meet security requirements in 2.3.1.1 |
| 2.6.2.4 All records capable of being printed | The tabulation device SHALL provide the ability to produce printed forms of its electronic records. The printed forms SHALL retain all required information as specified for each record type other than digital signatures. | Functional | VSTL | Functional Requirement related to Operations. No specific security control identified. | T=TEST & Demonstration | None | None | None | None | None | None | None | | | 1 | 1 | | | | | 1 | | | | 1 | N/C |
| 2.6.2.5 Summary count record | The voting system SHALL produce a summary count record including the following: a. Time and date of summary record; and b. The following, both in total and broken down by ballot style and voting location: i. Number of received ballots ii. Number of counted ballots iii. Number of rejected electronic CVRs iv. Number of write-in votes v. Number of undervotes. | Functional | VSTL | Functional Requirement related to Operations. No specific security control identified. | T=TEST & Demonstration | None | None | None | None | None | None | None | None Identified | N/A | | 1 | | | | | 1 | | | | 1 | N/C |
| 2.6.3.1 Paper record creation | Each vote capture device SHALL print a human readable paper record. | Functional | VSTL | Functional Requirement related to Operations. No specific security control identified. | T=TEST & Demonstration | None | None | None | None | None | None | None | None Identified | N/A | | 1 | | | | 1 | | | | | 1 | N/C |
| 2.6.3.2 Paper record contents | Each paper record SHALL contain at least: a. Election title and date of election; b. Voting location; c. Jurisdiction identifier; d. Ballot style; e. Paper record identifier; and f. For each contest and ballot question: i. The recorded choice, including write-ins; and ii. Information about each write-in. | Inspection | VSTL | Functional Requirement related to Operations. No specific security control identified. | T=TEST & Demonstration | None | None | None | None | None | None | None | None Identified | N/A | | 1 | | | | 1 | | | | | 1 | N/C |
| 2.6.3.3 Privacy | The vote capture device SHALL be capable of producing a paper record that does not contain any information that could link the record to the voter. | Inspection | VSTL | Functional Requirement related to Operations and Confidentiality. No specific security control identified. | T=TEST & Demonstration | None | None | None | None | None | None | None | None Identified | N/A | 1 | 1 | | | | | 1 | | | | 1 | N/C |
| 2.6.3.4 Multiple pages | When a single paper record spans multiple pages, each page SHALL include the voting location, ballot style, date of election, and page number and total number of the pages (e.g., page 1 of 4). | Functional | VSTL | Functional Requirement related to Operations. No specific security control identified. | T=TEST & Demonstration | None | None | None | None | None | None | None | None Identified | N/A | | 1 | | | | 1 | | | | | 1 | N/C |
| 2.6.3.5 Machine-readable part contains same information as humanreadable part | If a non-human-readable encoding is used on the paper record, it SHALL contain the entirety of the human-readable information on the record. | Inspection | VSTL | Functional Requirement related to Operations and loosly to encryption. No specific security control identified. | T=TEST & Demonstration | None | None | None | None | None | None | None | None Identified | N/A | 1 | 1 | | | | 1 | | | | | 1 | N/C |
| 2.6.3.6 Format for paper record non-human-readable data | Any non-human-readable information on the paper record SHALL be presented in a non-proprietary format. | Inspection | VSTL | Functional Requirement related to Operations and loosly to encryption. No specific security control identified. | T=TEST & Demonstration | None | None | None | None | None | None | None | None Identified | N/A | 1 | 1 | 1 | | | 1 | | | | | 1 | N/C |
| 2.6.3.7 Linking the electronic CVR to the paper record | The paper record SHALL: a. Contain the paper record identifier; and b. Identify whether the paper record represents the ballot that was cast. | Inspection | VSTL | Functional Requirement related to Operations. No specific security control identified. | T=TEST & Demonstration | None | None | None | None | None | None | None | None Identified | N/A | | 1 | | | | 1 | | | | | 1 | N/C |
| 2.7.1.1 Network monitoring | The system server SHALL provide for system and network monitoring during the voting period. | Functional | VSTL | Functional Requirement related to Network Monitoring and Audit capability. | D=DEMONSTRATION | SI-4 | Information System Monitoring Tools and Techniques | 10.6.2; 10.10.1; 10.10.2; 10.10.4 | 11.2.5; 11.2.6 | --- | EBBD-1; EBVC-1; ECID-1 | 4.B.2.a(5)(b); 4.B.3.a(8)(b); 6.B.3.a(8) | Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities.Control Enhancements:<br>(1) The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.<br>(2) The organization employs automated tools to support near-real-time analysis of events.<br>(3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.<br>(4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. | Control: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system. | 1 | 1 | 1 | | | 1 | | 1 | | | | IDS/IPS systems SHALL be used that actively monitors, detects, and notifies administrators of any potential malicious activity. |
| 2.7.1.2 Tool access | The system and network monitoring functionality SHALL only be accessible to authorized personnel from restricted consoles. | Functional | VSTL | Functional and Technical security requirement related to access controls and Roles and Responsibilities. | D=DEMONSTRATION | SI-4 | PS-6 | Access Agreements | 6.1.5; 8.1.3 | 6.1.5; 6.2.2 | SP-4.1 | PRRB-1 | E2.1.44. Privileged User. An authorized user who has access to system control, monitoring, or administration functions.PRRB-1 - Security Rules of Behavior or Acceptable Use Policy<br>A set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 2.7.1.3 Tool privacy | System and network monitoring functionality SHALL NOT have the capability to compromise voter privacy or election integrity. | Functional | VSTL | Functional Requirement related to voter privacy and Integrity. | D=DEMONSTRATION | None | None | None | None | None | None | None | | No reference documentation identified. | 1 | 1 | | | | | 1 | | | | 1 | N/C |
| 4.1.1 Acceptable Programming Language Constructs | Application logic SHALL be produced in a high-level programming language that has all of the following control constructs: a. Sequence; b. Loop with exit condition (e.g., for, while, and/or do-loops); c. If/Then/Else conditional; d. Case conditional; and e. Block-structured exception handling (e.g., try/throw/catch). | Inspection | Manufacturer | Integrity: Error Handling and system logic could jeopardize confidentiality, integrity and/or availability of the voting system. | I=INSPECTION | SI-11<br>SI-10 | Error Handling Information Accuracy, Completeness, Validity, and Authenticity | 12.2.1; 12.2.2; 12.2.3; 12.2.4; 10.7.3; 12.2.1; 12.2.2 | --- | --- | --- | 2.B.4.d 7.B.2.h; 2.B.4.d | ERROR HANDLING: Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.<br>NIST Special Publications 800-44, 800-57 | N/A | | 1 | | | | 1 | | 1 | | | | N/C |
| 4.2.1 Acceptable Coding Conventions | Application logic SHALL adhere to (or be based on) a published, credible set of coding rules, conventions or standards (herein simply called "coding conventions") that enhance the workmanship, security, integrity, testability, and maintainability of applications. | Inspection | Manufacturer | Integrity: Relates to software integrity | I=INSPECTION | None | None | None | None | None | DCSQ-1 Software Quality | None | DCSQ-1 Software Quality: Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives. | N/A | | 1 | | | | | 1 | | | | 1 | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4.2.1.1 Published | Coding conventions SHALL be considered published if they appear in publicly available media. | Inspection | Manufacturer | Integrity: Relates to software integrity | I=INSPECTION | None | None | None | None | None | DCSQ-1 Software Quality | None | DCSQ-1 Software Quality: Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives. | N/A | | 1 | | | | | 1 | | | | 1 | N/C |
| 4.2.1.2 Credible | Coding conventions SHALL be considered credible if at least two different organizations independently decided to adopt them and made active use of them at some time within the three years before conformity assessment was first sought. | Inspection | Manufacturer | Relates to software integrity | I=INSPECTION | None | None | None | None | None | DCSQ-1 Software Quality | None | DCSQ-1 Software Quality: Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives. | N/A | 1 | 1 | 1 | | | | 1 | | | | 1 | N/C |
| 4.3.1.2 Module testability | Each module SHALL have a specific function that can be tested and verified independently from the remainder of the code. | Inspection | Manufacturer | Relates to software integrity | I=INSPECTION | None | None | None | None | None | None | None | None | No reference documentation identified. | | 1 | | | | 1 | | | | 1 | 1 | N/C |
| 4.3.1.3 Module size and identification | Modules SHALL be small and easily identifiable. | Inspection | Manufacturer | Relates to software integrity | I=INSPECTION | None | None | None | None | None | None | None | Nonme | N/A | | 1 | | | | 1 | | | | 1 | 1 | N/C |
| 4.4.1.1 Exception handling | Application logic SHALL handle exceptions using block-structured exception handling constructs. | Inspection | Manufacturer | Relates to software integrity and quality | I=INSPECTION | SI-11<br>SI-10 | Error Handling Information Accuracy, Completeness, Validity, and Authenticity | 12.2.1; 12.2.2; 12.2.3; 12.2.4; 10.7.3; 12.2.1; 12.2.2 | --- | --- | --- | 2.B.4.d<br>7.B.2.h;<br>2.B.4.d | ERROR HANDLING: Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.<br>NIST Special Publications 800-44, 800-57 | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.4.1.2 Legacy library units must be wrapped | If application logic makes use of any COTS or third-party logic callable units that do not throw exceptions when exceptional conditions occur, those callable units SHALL be wrapped in callable units that check for the relevant error conditions and translate them into exceptions, and the remainder of application logic SHALL use only the wrapped version. | Inspection | Manufacturer | Relates to software integrity, quality and error handling of third party software | I=INSPECTION | SI-7<br>SI-10 | Software and Information Integrity | 12.2.1; 12.2.2; 12.2.4 | 11.2.1; 11.2.4 | --- | ECSD-2 | 4.B.1.c(2);<br>5.B.1.a(3);<br>5.B.2.a(6) | SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY<br>Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.4.2 Unstructured Control Flow is Prohibited | Application logic SHALL contain no unstructured control constructs. | Inspection | Manufacturer | Relates to software integrity and quality | I=INSPECTION | SI-11<br>SI-10 | Error Handling Information Accuracy, Completeness, Validity, and Authenticity | 12.2.1; 12.2.2; 12.2.3; 12.2.4; 10.7.3; 12.2.1; 12.2.2 | --- | --- | --- | 2.B.4.d<br>7.B.2.h;<br>2.B.4.d | ERROR HANDLING: Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.<br>NIST Special Publications 800-44, 800-57 | N/A | | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 4.4.2.1 Branching | Arbitrary branches (a.k.a. GoTos) SHALL NOT be allowed. | Inspection | Manufacturer | Relates to software integrity, quality and error handling of third party software | I=INSPECTION | SI-7<br>SI-10 | Software and Information Integrity | 12.2.1; 12.2.2; 12.2.4 | 11.2.1; 11.2.4 | --- | ECSD-2 | 4.B.1.c(2);<br>5.B.1.a(3);<br>5.B.2.a(6) | SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY<br>Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.4.2.2 Intentional exceptions | Exceptions SHALL only be used for abnormal conditions. Exceptions SHALL NOT be used to redirect the flow of control in normal ("non-exceptional") conditions. | Inspection | Manufacturer | Relates to software integrity, quality and error handling of third party software | I=INSPECTION | SI-7<br>SI-10 | Software and Information Integrity | 12.2.1; 12.2.2; 12.2.4 | 11.2.1; 11.2.4 | --- | ECSD-2 | 4.B.1.c(2);<br>5.B.1.a(3);<br>5.B.2.a(6) | SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY<br>Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.4.2.3 Unstructured exception handling | Unstructured exception handling (e.g., On Error GoTo, setjmp/longjmp) SHALL NOT be allowed. | Inspection | Manufacturer | Relates to software integrity, quality and error handling of third party software | I=INSPECTION | SI-7<br>SI-10 | Software and Information Integrity | 12.2.1; 12.2.2; 12.2.4 | 11.2.1; 11.2.4 | --- | ECSD-2 | 4.B.1.c(2);<br>5.B.1.a(3);<br>5.B.2.a(6) | SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY<br>Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.4.2.4 Separation of code and data | Application logic SHALL NOT compile or interpret configuration data or other input data as a programming language. | Inspection | Manufacturer | Relates to software integrity and quality | I=INSPECTION | SI-9 | Information Input Restrictions | 12.2.1; 12.2.2 | --- | SD-1 | --- | 2.B.9.b(11) | SI-9 INFORMATION INPUT RESTRICTIONS<br>Control: The organization restricts the capability to input information to the information system to authorized personnel.<br>Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.5.1 Header Comments | Application logic modules SHALL include header comments that provide at least the following information for each callable unit (e.g., function, method, operation, subroutine, procedure.): a. The purpose of the unit and how it works (if not obvious); b. A description of input parameters, outputs and return values, exceptions thrown, and side-effects; and c. Any protocols that must be observed (e.g., unit calling sequences). | Inspection | Manufacturer | Relates to software integrity and quality | I=INSPECTION | None | None | None | None | None | None | None | SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY<br>Control: The information system checks information for accuracy, completeness, validity, and authenticity.<br>Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements. | N/A | | 1 | 1 | | | 1 | | 1 | | | 1 | N/C |
| 4.6.1 Code Coherency | Application logic SHALL conform to the following sub-requirements: a. Self-modifying code SHALL NOT be allowed; b. Application logic SHALL be free of race conditions, deadlocks, livelocks, and resource starvation; c. If compiled code is used, it SHALL only be compiled using a COTS compiler; and d. If interpreted code is used, it SHALL only be run under a specific, identified version of a COTS runtime interpreter. | Inspection | Manufacturer | Relates to mobile code and best coding practices to prevent error that could impact system availability, integrity and confidentiality. This also implies that code support IA robustness requirements. | I=INSPECTION | SI-7 | Software and Information Integrity | 12.2.1; 12.2.2; 12.2.4 | 11.2.1; 11.2.4 | --- | ECSD-2 | 4.B.1.c(2);<br>5.B.1.a(3);<br>5.B.2.a(6) | SI-7: SOFTWARE AND INFORMATION INTEGRITY<br>Control: The information system detects and protects against unauthorized changes to software and information.<br>Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.6.2 Prevent Tampering With Code | Programmed devices SHALL defend against replacement or modification of executable or interpreted code. | Inspection | Manufacturer | Relates to mobile code and best coding practices to prevent error that could impact system availability, integrity and confidentiality. This also implies that code support IA robustness requirements. | I=INSPECTION | SI-7 | Software and Information Integrity | 12.2.1; 12.2.2; 12.2.4 | 11.2.1; 11.2.4 | --- | ECSD-2 | 4.B.1.c(2);<br>5.B.1.a(3);<br>5.B.2.a(6) | SI-7: SOFTWARE AND INFORMATION INTEGRITY<br>Control: The information system detects and protects against unauthorized changes to software and information.<br>Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.<br>NIST Special Publication 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. | N/A | 1 | 1 | | | | 1 | | 1 | | | | N/C |
| 4.6.3 Prevent Tampering With Data | The voting system SHALL prevent access to or manipulation of configuration data, vote data, or audit records. | Inspection | Manufacturer | Relates to audit capabilities and configuration management and data integrity. | I=INSPECTION | AU-1 | Audit and Accountability Policy and Procedures | 10.10; 15.1.1 | 17 | --- | ECAT-1; ECTB-1; DCAR-1 | DCID: B.2.d;<br>Manual:;<br>2.B.4.e(5);<br>4.B.2.a(4) | | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4.7.1.1 Validity check | Programmed devices SHALL check information inputs for completeness and validity. | Inspection | Manufacturer | Relates to the accuracy of information and integrity of data. | I=INSPECTION | SI-10 | Information Accuracy, Completeness, Validity, and Authenticity | 10.7.3; 12.2.1; 12.2.2 | --- | --- | --- | 7.B.2.h; 2.B.4.d | | N/A | | 1 | | | | | 1 | 1 | | | | N/C |
| 4.7.1.2 Defend against garbage input | Programmed devices SHALL ensure that incomplete or invalid inputs do not lead to irreversible error. | Inspection | Manufacturer | Functional requirement and Error handling | I=INSPECTION | SI-11 | Error Handling | 12.2.1; 12.2.2; 12.2.3; 12.2.4 | --- | --- | --- | 2.B.4.d | SI-11: ERROR HANDLING<br>Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.<br>Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.7.2.1 Error checking | Application logic that is vulnerable to the following types of errors SHALL check for these errors at run time and respond defensively (as specified by Requirement 4.7.2.8) when they occur: Out-of-bounds accesses of arrays or strings (includes buffers used to move data); Stack overflow errors; CPU-level exceptions such as address and bus errors, dividing by zero, and the like; Variables that are not appropriately handled when out of expected boundaries; Numeric overflows; and Known programming language specific vulnerabilities. | Inspection | Manufacturer | Relates to the accuracy of information and integrity of data. | I=INSPECTION | SI-11 | Error Handling | 12.2.1; 12.2.2; 12.2.3; 12.2.4 | --- | --- | --- | 2.B.4.d | SI-11: ERROR HANDLING<br>Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.<br>Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.7.2.2 Range checking of indices | If the application logic uses arrays, vectors, character sequences, strings or any analogous data structures, and the programming language does not provide automatic run-time range checking of the indices, the indices SHALL be rangedchecked on every access. | Inspection | Manufacturer | Relates to the accuracy of information and integrity of data. | I=INSPECTION | SI-11 | Error Handling | 12.2.1; 12.2.2; 12.2.3; 12.2.4 | --- | --- | --- | 2.B.4.d | SI-11: ERROR HANDLING<br>Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.<br>Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. | N/A | | 1 | | | | | 1 | 1 | | | | N/C |
| 4.7.2.3 Stack overflows | If stack overflow does not automatically result in an exception, the application logic SHALL explicitly check for and prevent stack overflow. | Inspection | Manufacturer | Relates to the accuracy of information and integrity of data. | I=INSPECTION | SI-11 | Error Handling | 12.2.1; 12.2.2; 12.2.3; 12.2.4 | --- | --- | --- | 2.B.4.d | SI-11: ERROR HANDLING<br>Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.<br>Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. | N/A | | 1 | | | | | 1 | 1 | | | | N/C |
| 4.7.2.4 CPU traps | The application logic SHALL implement such handlers as are needed to detect and respond to CPU-level exceptions including address and bus errors and dividing by zero. | Inspection | Manufacturer | Relates to the accuracy of information and integrity of data. | I=INSPECTION | SI-11 | Error Handling | 12.2.1; 12.2.2; 12.2.3; 12.2.4 | --- | --- | --- | 2.B.4.d | SI-11: ERROR HANDLING<br>Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.<br>Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.7.2.5 Garbage input parameters | All scalar or enumerated type parameters whose valid ranges as used in a callable unit (e.g., function, method, operation, subroutine, procedure.) do not cover the entire ranges of their declared data types SHALL be range-checked on entry to the unit. | Inspection | Manufacturer | Relates to error handling and data range values. | I=INSPECTION | SI-10 | Information Accuracy, Completeness, Validity, and Authenticity | 10.7.3; 12.2.1; 12.2.2 | --- | --- | --- | 7.B.2.h; 2.B.4.d | SI-10: INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY<br>Control: The information system checks information for accuracy, completeness, validity, and authenticity.<br>Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements. | N/A | | 1 | | | | 1 | | 1 | | | | N/C |
| 4.7.2.6 Numeric overflows | If the programming language does not provide automatic run-time detection of numeric overflow, all arithmetic operations that could potentially overflow the relevant data type SHALL be checked for overflow. | Inspection | Manufacturer | Integrity: Relates to error handling and data range values. | I=INSPECTION | SI-10 | Information Accuracy, Completeness, Validity, and Authenticity | 10.7.3; 12.2.1; 12.2.2 | --- | --- | --- | 7.B.2.h; 2.B.4.d | SI-10: INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY<br>Control: The information system checks information for accuracy, completeness, validity, and authenticity.<br>Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements. | N/A | | 1 | | | | 1 | | 1 | | | | N/C |
| 4.7.2.7 Nullify freed pointers | If pointers are used, any pointer variables that remain within scope after the memory they point to is deallocated SHALL be set to null or marked as invalid (pursuant to the idiom of the programming language used) after the memory they point to is deallocated. | Inspection | Manufacturer | Integrity and Availability: Relates to software quality and best programming practices. No specific security control. | I=INSPECTION | None | None | None | None | None | None | None | None | None | | 1 | 1 | | | 1 | | | | 1 | | N/C |
| 4.7.2.8 React to errors detected | The detection of any of the errors enumerated in Requirement 4.7.2.1 SHALL be treated as a complete failure of the callable unit in which the error was detected. An appropriate exception SHALL be thrown and control SHALL pass out of the unit forthwith. | Inspection | Manufacturer | Integrity and Availability: Relates to software quality and best programming practices. No specific security control. | I=INSPECTION | SI-11 | Error Handling | 12.2.1; 12.2.2; 12.2.3; 12.2.4 | --- | --- | --- | 2.B.4.d | None | N/A | | 1 | 1 | | | 1 | | | | | 1 | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4.7.2.9 Do not disable error checks | Error checks detailed in Requirement 4.7.2.1 SHALL remain active in production code. | Inspection | Manufacturer | Integrity and Availability: Relates to error handling and data range values. | I=INSPECTION | SI-10 | Information Accuracy, Completeness, Validity, and Authenticity | 10.7.3; 12.2.1; 12.2.2 | --- | --- | --- | 7.B.2.h; 2.B.4.d | SI-10: INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY<br>Control: The information system checks information for accuracy, completeness, validity, and authenticity.<br>Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.7.2.10 Roles authorized to respond to errors | Exceptions resulting from failed error checks or CPU-level exceptions SHALL require intervention by an election official or administrator before voting can continue. | Inspection | Manufacturer | Integrity: Relates to error handling and data range values. | I=INSPECTION | SI-11<br>SI-10 | Error Handling | 12.2.1; 12.2.2; 12.2.3; 12.2.4 | --- | --- | --- | 2.B.4.d | | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.7.2.11 Election integrity monitoring | The voting system SHALL proactively detect or prevent basic violations of election integrity (e.g., stuffing of the ballot box or the accumulation of negative votes) and alert an election official or administrator if such violations they occur. | Inspection | Manufacturer | N/A to IT Security capability | I=INSPECTION | None | None | None | None | None | None | None | None Identified | N/A | | 1 | | | | 1 | | | | 1 | 1 | N/C |
| 4.8.1.1 Resuming normal operations | All voting systems SHALL be capable of resuming normal operations following the correction of a failure in any device. | Functional | Manufacturer | Integrity: Relates to system error handling and recovery of operations. | I=INSPECTION | CP-10 | Information System Recovery and Reconstitution | 14.1.4 | 9.2.8 | SC-2.1 | COTR-1; ECND-1 | 4.B.1.a(4); 6.B.1.a(1); 6.B.2.a(3)(d) | CP-10: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION<br>Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.<br>Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested. | N/A | | 1 | | | | | 1 | 1 | | | | N/C |
| 4.8.1.2 Failures not compromise voting or audit data | Exceptions and system recovery SHALL be handled in a manner that protects the integrity of all recorded votes and audit log information. | Functional | Manufacturer | Integrity: Relates to error handling and data range values. | I=INSPECTION | SI-11<br>SI-10 | Error Handling | 12.2.1; 12.2.2; 12.2.3; 12.2.4 | --- | --- | --- | 2.B.4.d | | N/A | | 1 | | | | 1 | | 1 | | | | N/C |
| 4.8.1.3 Device survive component failure | All vote capture device SHALL be capable of resuming normal operation following the correction of a failure in any component (e.g., memory, CPU, printer) provided that catastrophic electrical or mechanical damage has not occurred. | Functional | Manufacturer | Integrity: Relates to system error handling and recovery of operations. | I=INSPECTION | SI-11<br>SI-10 | Error Handling | 12.2.1; 12.2.2; 12.2.3; 12.2.4 | --- | --- | --- | 2.B.4.d | CP-10: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION<br>Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.<br>Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.8.2 Controlled Recovery | Error conditions SHALL be corrected in a controlled fashion so that voting system status may be restored to the initial state existing before the error occurred. | Functional | Manufacturer | Integrity: Relates to system error handling and recovery of operations. | I=INSPECTION | SI-11<br>SI-10 | Error Handling | 12.2.1; 12.2.2; 12.2.3; 12.2.4 | --- | --- | --- | 2.B.4.d | CP-10: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION<br>Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.<br>Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.8.2.1 Nested error conditions | Nested error conditions that are corrected without reset, restart, reboot, or shutdown of the vote capture device SHALL be corrected in a controlled sequence so that voting system status may be restored to the initial state existing before the first error occurred. | Functional | Manufacturer | Integrity: Relates to system error handling and recovery of operations. | I=INSPECTION | SI-11<br>SI-10 | Error Handling | 12.2.1; 12.2.2; 12.2.3; 12.2.4 | --- | --- | --- | 2.B.4.d | CP-10: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION<br>Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.<br>Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.8.2.2 Reset CPU error states | CPU-level exceptions that are corrected without reset, restart, reboot, or shutdown of the vote capture device SHALL be handled in a manner that restores the CPU to a normal state and allows the voting system to log the event and recover as with a software-level exception. | Functional | Manufacturer | Integrity and Availability: Relates to system error handling and recovery of operations. | D=DEMONSTRATION | SI-11 | Error Handling | 12.2.1; 12.2.2; 12.2.3; 12.2.4 | --- | --- | --- | 2.B.4.d | SI-11<br>ERROR HANDLING<br>Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. | N/A | | 1 | 1 | | | 1 | | 1 | | | | |
| 4.8.3 Restore Device to Checkpoints | When recovering from non-catastrophic failure or from any error or malfunction that is within the operator's ability to correct, the voting system SHALL restore the device to the operating condition existing immediately prior to the error or failure, without loss or corruption of voting data previously stored in the device. | Functional | Manufacturer | Integrity: Relates to system error handling and recovery of operations. | I=INSPECTION | SI-11<br>SI-10 | Error Handling | 12.2.1; 12.2.2; 12.2.3; 12.2.4 | --- | --- | --- | 2.B.4.d | CP-10: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION<br>Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.<br>Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested. | N/A | | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 4.9.1.1 Review source versus manufacturer specifications | The test lab SHALL assess the extent to which the application logic adheres to the specifications made in its design documentation. | Inspection | VSTL | Functional and ST&E Requirement defined ins Appendix F of the NIST SP800-53A Rev.2 | I=INSPECTION | SI-9 | Information Input Restrictions | 12.2.1; 12.2.2 | --- | SD-1 | --- | 2.B.9.b(11) | SI-9 INFORMATION INPUT RESTRICTIONS<br>Control: The organization restricts the capability to input information to the information system to authorized personnel.<br>Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.9.1.2 Review source versus coding conventions | The test lab SHALL assess the extent to which the application logic adheres to the published, credible coding conventions chosen by the manufacturer. | Inspection | VSTL | Integrity and Availability: Application programming best practices. | I=INSPECTION | SI-9 | Information Input Restrictions | 12.2.1; 12.2.2 | --- | SD-1 | --- | 2.B.9.b(11) | SI-9 INFORMATION INPUT RESTRICTIONS<br>Control: The organization restricts the capability to input information to the information system to authorized personnel.<br>Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 4.9.1.3 Review source versus workmanship requirements | The test lab SHALL assess the extent to which the application logic adheres to the requirements of Section 4 Software. | Inspection | VSTL | Application programming best practices. | I=INSPECTION | SI-9 | Information Input Restrictions | 12.2.1; 12.2.2 | --- | SD-1 | --- | 2.B.9.b(11) | SI-9 INFORMATION INPUT RESTRICTIONS<br>Control: The organization restricts the capability to input information to the information system to authorized personnel.<br>Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities. | N/A | | 1 | 1 | | | 1 | | 1 | | | | Recommend the use of application scvanning tools such as Lumension, Nessus or Fortify for source code analysis. |
| 4.9.1.4 Efficacy of built-in self-tests | The test lab SHALL verify the efficacy of built-in measurement, self-test, and diagnostic capabilities. | Inspection | VSTL | Relates to Self test and diagnostic capability. Impacts Confedentiality, Integrity and Availability | I=INSPECTION | SI-6 | Security Functionality Verification | --- | 11.2.1; 11.2.2 | SS-2.2 | DCSS-1 | 4.B.1.c(2); 5.B.2.b(2) | SI-6: SECURITY FUNCTIONALITY VERIFICATION<br>Control: The information system verifies the correct operation of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered.<br>Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required. | N/A | | 1 | 1 | | | 1 | | 1 | | | | Recommend the use of application scvanning tools such as Lumension, Nessus or Fortify for source code analysis. |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4.9.2.1 Security control source code review | The test lab SHALL analyze the source code of the security controls to assess whether they function correctly and cannot be bypassed. | Inspection | VSTL | Loss of Integrity, availability and/or Confidentiality | I=INSPECTION | RA-5 | Vulnerability Scanning | 12.6.1 | 10.3.2; 14.2.1 | --- | ECMT-1; VIVM-1 | 4.B.3.a(8)(b) ; 4.B.3.b(6)(b) ; 9.B.4.e | RA-5: VULNERABILITY SCANNING<br>Control: The organization scans for vulnerabilities in the information system [Assignment: organization-defined frequency] or when significant new vulnerabilities potentially affecting the system are identified and reported.<br>Supplemental Guidance: Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code). NIST Special Publication 800-42 provides guidance on network security testing. NIST Special Publication 800-40 (Version 2) provides guidance on patch and vulnerability management. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | Recommend the use of application scvanning tools such as Lumension, Nessus or Fortify for source code analysis. |
| 5.1.1.1 Definition of roles | The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system. | Functional | VSTL | Relates to the separation of duties, least priviledge and account management. Roles and Responsibilities are discussed in many different sections. Impacts include: Loss of Confidentiality, Availability and Integrity. This is an operating system functional requirement to meet the above. | D=DEMONSTRATION | AC-2 | Account Management | 6.2.2; 6.2.3; 8.3.3; 11.2.1; 11.2.2; 11.2.4; 11.7.2 | 6.1.8; 15.1.1; 15.1.4; 15.1.5; 15.1.8; 15.2.2; 16.1.3; 16.1.5; 16.2.12 | AC-2.1; AC-2.2; AC-3.2; SP-4.1 | IAAC-1 | 4.B.2.a(3) | ECLP-1 Least Privilege<br>Access procedures enforce the principles of separation of duties and "least privilege." Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | Recommend the use of application scvanning tools such as Lumension, Nessus or Fortify for source code analysis. |
| 5.1.1.2 Access to election data | The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data. | Functional | VSTL | Relates to the separation of duties, least priviledge and account management. Roles and Responsibilities are discussed in many different sections. Impacts include: Loss of Confidentiality, Availability and Integrity. This is an operating system functional requirement to meet the above. | D=DEMONSTRATION | AC-2 | Account Management | 6.2.2; 6.2.3; 8.3.3; 11.2.1; 11.2.2; 11.2.4; 11.7.2 | 6.1.8; 15.1.1; 15.1.4; 15.1.5; 15.1.8; 15.2.2; 16.1.3; 16.1.5; 16.2.12 | AC-2.1; AC-2.2; AC-3.2; SP-4.1 | IAAC-1 | 4.B.2.a(3) | | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | Recommend the use of application scvanning tools such as Lumension, Nessus or Fortify for source code analysis. |
| 5.1.1.3 Separation of duties | The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process. | Functional | VSTL | Integrity & Confidentiality: Procedual requirement to prevent collusion | D=DEMONSTRATION | AC-4 | Information Flow Enforcement | 10.6.2; 11.4.5; 11.4.6; 11.4.7 | --- | --- | EBBD-1; EBBD-2 | 4.B.3.a(3); 7.B.3.g | AC-5<br>SEPARATION OF DUTIES<br>Control: The information system enforces separation of duties through assigned access authorizations.<br>Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 5.1.2.1 Identity verification | The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | AC-7 | Unsuccessful Login Attempts | 11.5.1 | 15.1.14 | AC-3.2 | ECLO-1 | 4.B.2.a(17)(c)-(d) | | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.1.2.2 Access control configuration | The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | AC-5 | Separation of Duties | 10.1.3; 10.6.1; 10.10.1 | 6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5 | AC-3.2; SD-1.2 | ECLP-1 | 2.A.1; 4.B.3.a(18) | AC-5<br>SEPARATION OF DUTIES<br>Control: The information system enforces separation of duties through assigned access authorizations.<br>Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.1.2.3 Default access control configuration | The voting system’s default access control permissions SHALL implement the least privileged role or group needed. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | AC-5 | Separation of Duties | 10.1.3; 10.6.1; 10.10.1 | 6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5 | AC-3.2; SD-1.2 | ECLP-1 | 2.A.1; 4.B.3.a(18) | AC-5<br>SEPARATION OF DUTIES<br>Control: The information system enforces separation of duties through assigned access authorizations.<br>Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 5.1.2.4 Escalation prevention | The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | AC-5 | Separation of Duties | 10.1.3; 10.6.1; 10.10.1 | 6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5 | AC-3.2; SD-1.2 | ECLP-1 | 2.A.1; 4.B.3.a(18) | SC-3<br>SECURITY FUNCTION ISOLATION<br>Control: The information system isolates security functions from nonsecurity functions.<br>Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5.1.2.5 Operating system privileged account restriction | The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | AC-5 | Separation of Duties | 10.1.3; 10.6.1; 10.10.1 | 6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5 | AC-3.2; SD-1.2 | ECLP-1 | 2.A.1; 4.B.3.a(18) | AC-5<br>SEPARATION OF DUTIES<br>Control: The information system enforces separation of duties through assigned access authorizations.<br>Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.1.2.6 Logging of account | The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log. | Functional | VSTL | Forensic auditing abilities. Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | AU-2 | Auditable Events | 10.10.1 | 17.1.1; 17.1.2; 17.1.4 | --- | ECAR-3 | 4.B.2.a(4)(d) | ECAR-3 Audit Record Content<br>Audit records include:<br>- User ID.<br>- Successful and unsuccessful attempts to access security files<br>- Date and time of the event.<br>- Type of event.<br>- Success or failure of event.<br>- Successful and unsuccessful logons.<br>- Denial of access resulting from excessive number of logon attempts.<br>- Blocking or blacklisting a user ID, terminal or access port, and the reason for the action.<br>- Activities that might modify, bypass, or negate safeguards controlled by the system.<br>- Data required to audit the possible use of covert channel mechanisms.<br>- Privileged activities and other system-level access.<br>- Starting and ending time for access to the system.<br>- Security relevant actions associated with periods processing or the changing of security labels or categories of information. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | |
| 5.1.2.7 Monitoring voting system access | The voting system SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs. | Functional | VSTL | Forensic auditing abilities. Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | AU-2 | Auditable Events | 10.10.1 | 17.1.1; 17.1.2; 17.1.4 | --- | ECAR-3 | 4.B.2.a(4)(d) | ECAR-3 Audit Record Content<br>Audit records include:<br>- User ID.<br>- Successful and unsuccessful attempts to access security files<br>- Date and time of the event.<br>- Type of event.<br>- Success or failure of event.<br>- Successful and unsuccessful logons.<br>- Denial of access resulting from excessive number of logon attempts.<br>- Blocking or blacklisting a user ID, terminal or access port, and the reason for the action.<br>- Activities that might modify, bypass, or negate safeguards controlled by the system.<br>- Data required to audit the possible use of covert channel mechanisms.<br>- Privileged activities and other system-level access.<br>- Starting and ending time for access to the system.<br>- Security relevant actions associated with periods processing or the changing of security labels or categories of information. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.1.2.8 Login failures | The vote capture devices at the kiosk locations and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures. a. The lockout threshold SHALL be configurable by appropriate administrators/operators. b. The voting system SHALL log the event. c. The voting system SHALL immediately send a notification to appropriate administrators/operators of the event. d. The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation. | Functional | VSTL | Forensic auditing abilities. Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | AU-2 | Auditable Events | 10.10.1 | 17.1.1; 17.1.2; 17.1.4 | --- | ECAR-3 | 4.B.2.a(4)(d) | ECAR-3 Audit Record Content<br>Audit records include:<br>- User ID.<br>- Successful and unsuccessful attempts to access security files<br>- Date and time of the event.<br>- Type of event.<br>- Success or failure of event.<br>- Successful and unsuccessful logons.<br>- Denial of access resulting from excessive number of logon attempts.<br>- Blocking or blacklisting a user ID, terminal or access port, and the reason for the action.<br>- Activities that might modify, bypass, or negate safeguards controlled by the system.<br>- Data required to audit the possible use of covert channel mechanisms.<br>- Privileged activities and other system-level access.<br>- Starting and ending time for access to the system.<br>- Security relevant actions associated with periods processing or the changing of security labels or categories of information. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 5.1.2.9 Account lockout logging | The voting system SHALL log a notification when any account has been locked out. | Functional | VSTL | Forensic auditing abilities. Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | AU-2 | Auditable Events | 10.10.1 | 17.1.1; 17.1.2; 17.1.4 | --- | ECAR-3 | 4.B.2.a(4)(d) | ECAR-3 Audit Record Content<br>Audit records include:<br>- User ID.<br>- Successful and unsuccessful attempts to access security files<br>- Date and time of the event.<br>- Type of event.<br>- Success or failure of event.<br>- Successful and unsuccessful logons.<br>- Denial of access resulting from excessive number of logon attempts.<br>- Blocking or blacklisting a user ID, terminal or access port, and the reason for the action.<br>- Activities that might modify, bypass, or negate safeguards controlled by the system.<br>- Data required to audit the possible use of covert channel mechanisms.<br>- Privileged activities and other system-level access.<br>- Starting and ending time for access to the system.<br>- Security relevant actions associated with periods processing or the changing of security labels or categories of information. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 5.1.2.10 Session time-out | Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices. | Functional | VSTL | Forensic auditing abilities. Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | AU-2 | Auditable Events | 10.10.1 | 17.1.1; 17.1.2; 17.1.4 | --- | ECAR-3 | 4.B.2.a(4)(d) | ECAR-3 Audit Record Content<br>Audit records include:<br>- User ID.<br>- Successful and unsuccessful attempts to access security files<br>- Date and time of the event.<br>- Type of event.<br>- Success or failure of event.<br>- Successful and unsuccessful logons.<br>- Denial of access resulting from excessive number of logon attempts.<br>- Blocking or blacklisting a user ID, terminal or access port, and the reason for the action.<br>- Activities that might modify, bypass, or negate safeguards controlled by the system.<br>- Data required to audit the possible use of covert channel mechanisms.<br>- Privileged activities and other system-level access.<br>- Starting and ending time for access to the system.<br>- Security relevant actions associated with periods processing or the changing of security labels or categories of information. | N/A | 1 | | | | | 1 | | 1 | | | | N/C |
| 5.1.2.11 Screen lock | Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked. | Functional | VSTL | Access control and session lock: Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | AC-11 | Session Lock | 11.3.2 | 16.1.4 | AC-3.2 | PESL-1 | 4.B.1.a(5) | SESSION LOCK<br>Control: The information system prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.<br>Supplemental Guidance: Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the information system. Organization-defined time periods of inactivity comply with federal policy; for example, in accordance with OMB Memorandum 06-16, the organization-defined time period is no greater than thirty minutes for remote access and portable devices. | N/A | | 1 | 1 | | | 1 | | 1 | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5.2.1.1 Strength of authentication | Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | IA-2 | User Identification and Authentication | 11.2.3; 11.4.2; 11.5.2 | 15.1 | --- | IAIA-1 | 4.B.2.a(7) | USER IDENTIFICATION AND AUTHENTICATION<br>Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).<br>Supplemental Guidance: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST Special Publication 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | Recommendation: The use of three factor authentication method to include biometric. Cross-over error rates (CER) and Equal Error Rates should be known. |
| 5.2.1.2 Minimum authentication methods | The voting system SHALL authenticate users per the minimum authentication methods outlined below. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | IA-2 | User Identification and Authentication | 11.2.3; 11.4.2; 11.5.2 | 15.1 | --- | IAIA-1 | 4.B.2.a(7) | IA-2<br>USER IDENTIFICATION AND AUTHENTICATION<br>Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).<br>Supplemental Guidance: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 5.2.1.3 Multiple authentication mechanisms | The voting system SHALL provide multiple authentication methods to support multi-factor authentication. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | IA-2 | User Identification and Authentication | 11.2.3; 11.4.2; 11.5.2 | 15.1 | --- | IAIA-1 | 4.B.2.a(7) | IA-2<br>USER IDENTIFICATION AND AUTHENTICATION<br>Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).<br>Supplemental Guidance: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.2.1.4 Secure storage of authentication data | When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | IA-5 | Authenticator Management | 11.5.2; 11.5.3 | 15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3 | AC-3.2 | IAKM-1; IATS-1; IAIA-2 | 4.B.2.a(7); 4.B.3.a(11) | IA-5<br>AUTHENTICATOR MANAGEMENT<br>Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.<br>Supplemental Guidance: Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. | N/A | 1 | 1 | | | | 1 | | 1 | | | | N/C |
| 5.2.1.5 Password reset | The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy. | Functional | VSTL | Passwords, tokens, or other devices are used to identify and authenticate users. Loss of Integrity, Availability and Confidentiality | D=DEMONSTRATION | IA-5 | Authenticator Management | 11.5.2; 11.5.3 | 15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3 | AC-3.2 | IAKM-1; IATS-1 | 4.B.2.a(7); 4.B.3.a(11) | Related security controls: AC-14, AC-17 | N/A | 1 | 1 | | | | 1 | | 1 | | | | N/C |
| 5.2.1.6 Password strength configuration | The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800 63 Electronic Authentication Guideline Standards. | Functional | VSTL | Medium Impact. Administrave roles and responsibilities | D=DEMONSTRATION | IA-5 | Authenticator Management | 11.5.2; 11.5.3 | 15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3 | AC-3.2 | IAKM-1; IATS-1 | 4.B.2.a(7); 4.B.3.a(11) | IA-5<br>AUTHENTICATOR MANAGEMENT<br>Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically. | N/A | 1 | 1 | | | | 1 | | 1 | | | | N/C |
| 5.2.1.7 Password history configuration | The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system. 1 NIST Special Publication 800-57 | Functional | VSTL | Medium: Impacts Integrity. | D=DEMONSTRATION | IA-5 | Authenticator Management | 11.5.2; 11.5.3 | 15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3 | AC-3.2 | IAKM-1; IATS-1 | 4.B.2.a(7); 4.B.3.a(11) | IA-5<br>AUTHENTICATOR MANAGEMENT<br>Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically. | N/A | 1 | 1 | | | | 1 | | 1 | | | | N/C |
| 5.2.1.8 Account information password restriction | The voting system SHALL ensure that the user name is not used in the password. | Functional | VSTL | Medium: Impacts Integrity. | D=DEMONSTRATION | IA-5 | Authenticator Management | 11.5.2; 11.5.3 | 15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3 | AC-3.2 | IAKM-1; IATS-1 | 4.B.2.a(7); 4.B.3.a(11) | IA-5<br>AUTHENTICATOR MANAGEMENT<br>Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically. | N/A | 1 | 1 | | | | 1 | | 1 | | | | N/C |
| 5.2.1.9 Automated password expiration | The voting system SHALL provide a means to automatically expire passwords. | Functional | VSTL | Medium: Impacts Integrity. | D=DEMONSTRATION | IA-5 | Authenticator Management | 11.5.2; 11.5.3 | 15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3 | AC-3.2 | IAKM-1; IATS-1 | 4.B.2.a(7); 4.B.3.a(11) | IA-5<br>AUTHENTICATOR MANAGEMENT<br>Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically. | N/A | 1 | 1 | | | | 1 | | 1 | | | | Passwords SHALL conform to DoD DIACAP minimum standards. |
| 5.2.1.10 Device authentication | The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security. | Functional | VSTL | Medium: Impacts Integrity. | D=DEMONSTRATION | CA-3 | Information System Connections | 10.6.2; 10.9.1; 11.4.5; 11.4.6; 11.4.7 | 1.1.1; 3.2.9; 4.1.8; 12.2.3 | CC-2.1 | DCID-1; EBCR-1; EBRU-1; EBPW-1; ECIC-1 | 9.B.3; 9.D.3.c | CA-3<br>INFORMATION SYSTEM CONNECTIONS<br>Control: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis. | N/A | 1 | 1 | | | | | 1 | 1 | | | | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5.2.1.11 Network authentication | Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | AC-17 | Remote Access | 11.4.2; 11.4.3; 11.4.4 | 16.2.4; 16.2.8 | AC-3.2 | EBRP-1; EBRU-1 | 4.B.1.a(1)(b); 4.B.3.a(11); 7.D.2.e | FISCAM Requirement<br>FIPS 200 Requirements<br>AC-17<br>REMOTE ACCESS<br>Control: The organization authorizes, monitors, and controls all methods of remote access to the information system.<br>Supplemental Guidance: Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.2.1.12 Message authentication | Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security. | Functional | VSTL | Loss of Integrity. | D=DEMONSTRATION | SC-23 | Session Authenticity | --- | --- | --- | --- | --- | SC-23<br>SESSION AUTHENTICITY<br>Control: The information system provides mechanisms to protect the authenticity of communications sessions.<br>Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to implement session-level protection where needed (e.g., in service-oriented architectures providing web-based services). NIST Special Publication 800-52 provides guidance on the use of transport layer security (TLS) mechanisms. NIST Special Publication 800-77 provides guidance on the deployment of IPsec virtual private networks (VPNs) and other methods of protecting communications sessions. NIST Special Publication 800-95 provides guidance on secure web services. | N/A | | 1 | | | | 1 | | 1 | | | | Recommend that authentication schema SHALL be commensurate with the highest level technically feasable. This requirement will constantly change as new schema's become available. |
| 5.2.1.13 Message authentication mechanisms | IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | D=DEMONSTRATION | AC-17 | Remote Access | 11.4.2; 11.4.3; 11.4.4 | 16.2.4; 16.2.8 | AC-3.2 | EBRP-1; EBRU-1 | 4.B.1.a(1)(b); 4.B.3.a(11); 7.D.2.e | AC-17<br>REMOTE ACCESS<br>Control: The organization authorizes, monitors, and controls all methods of remote access to the information system.<br>Supplemental Guidance: Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publications 800-73 and 800-78. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks. Related security control: IA-2. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.3.1.1 Cryptographic functionality | All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols. | Inspection | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST | IA-7 | Cryptographic Module; Authentication | --- | 16.1.7 | --- | 16.1.7 | --- | National Institute of Standards and Technology Special Publication 800-29, A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2, June 2001.<br>IA-7<br>CRYPTOGRAPHIC MODULE AUTHENTICATION<br>Control: The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.<br>Supplemental Guidance: The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.3.1.2 Required security strength | Cryptographic algorithms and schemas SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records. | Inspection | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST | IA-7 | Cryptographic Module; Authentication | --- | 16.1.7 | --- | 16.1.7 | --- | National Institute of Standards and Technology Special Publication 800-29, A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2, June 2001.<br>IA-7<br>CRYPTOGRAPHIC MODULE AUTHENTICATION<br>Control: The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.<br>Supplemental Guidance: The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | Recommend that authentication schema SHALL be commensurate with the highest level technically feasable. This requirement will constantly change as new schema's become available. |
| 5.3.1.3 Use NIST-approved cryptography for communications | Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites. In addition the implementations of these algorithms SHALL be NIST-approved (Cryptographic Algorithm Validation Program). | Test Method: Function | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST | IA-7 | Cryptographic Module; Authentication | --- | 16.1.7 | --- | 16.1.7 | --- | National Institute of Standards and Technology Special Publication 800-29, A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2, June 2001.<br>IA-7<br>CRYPTOGRAPHIC MODULE AUTHENTICATION<br>Control: The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.<br>Supplemental Guidance: The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.3.2.1 Key generation methods | Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method. | Inspection | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST | SC-12 | Cryptographic Key Establishment and Management | 12.3.1; 12.3.2 | 16.1.7; 16.1.8 | --- | IAKM-1 | 1.G | SC-12<br>CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT<br>Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.<br>Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.3.2.2 Security of key generation methods | Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key. | Inspection | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST | None | None | None | None | None | None | None | National Institute of Standards and Technology Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), March 2007. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.3.2.3 Seed values | If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements in 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures. | Inspection | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST | SC-12 | Cryptographic Key Establishment and Management | 12.3.1; 12.3.2 | 16.1.7; 16.1.8 | --- | IAKM-1 | 1.G | National Institute of Standards and Technology Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), March 2007.SC-12<br>CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT<br>Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.<br>Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5.3.2.4 Use NIST-approved key generation methods for communications | Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used. | Inspection | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST | SC-12 | Cryptographic Key Establishment and Management | 12.3.1; 12.3.2 | 16.1.7; 16.1.8 | --- | IAKM-1 | 1.G | National Institute of Standards and Technology Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), March 2007.SC-12<br>CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT<br>Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.<br>Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.3.2.5 Random number generator health tests | Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck). | Inspection | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST | None | None | None | None | None | None | None | National Institute of Standards and Technology Special Publication 800-90, The health test function determines that the DRBG mechanism continues to function correctly. | Covered in NIST Special Publication 800-90 | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.3.3.1 Key entry and output | Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form. | Inspection | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST | None | None | None | None | None | None | None | National Institute of Standards and Technology Special Publication 800-90, The health test function determines that the DRBG mechanism continues to function correctly. | Covered in NIST Special Publication 800-90 | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.3.4.1 Key storage | Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification. | Inspection | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST | None | None | None | None | None | None | None | National Institute of Standards and Technology Special Publication 800-90, The health test function determines that the DRBG mechanism continues to function correctly. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.3.4.2 Key zeroization | The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST | None | None | None | None | None | None | None | National Institute of Standards and Technology Special Publication 800-90, The health test function determines that the DRBG mechanism continues to function correctly. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.3.4.3 Support for rekeying | The voting system SHALL support the capability to reset cryptographic keys to new values. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST | None | None | None | None | None | None | None | National Institute of Standards and Technology Special Publication 800-90, The health test function determines that the DRBG mechanism continues to function correctly. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.4.1.1 Cast vote integrity; transmission | The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission. | Functional | VSTL | Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. | T=TEST | SC-8 | Transmission Integrity | 10.6.1; 10.8.1; 10.9.1 | 11.2.1; 11.2.4; 11.2.9; 16.2.14 | AC-3.2 | ECTM-1 | 5.B.3.a(11) | ECTM-2 Transmission Integrity Controls<br>Good engineering practices with regards to the integrity mechanisms of COTS, GOTS, and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs). Mechanisms are in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels). | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 5.4.1.2 Cast vote integrity; storage | The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage. | Functional | VSTL | Functional Requirement. Loss of Integrity. | T=TEST | None | None | None | None | None | None | None | Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006. | N/A | | 1 | | | | | 1 | 1 | | 1 | | N/C |
| 5.4.1.3 Cast vote storage | Cast vote data SHALL NOT be permanently stored on the vote capture device. | Functional | VSTL | Functional Requirement. Loss of Integrity. | T=TEST | None | None | None | None | None | None | None | Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006. | N/A | | 1 | | | | | 1 | | | 1 | 1 | N/C |
| 5.4.1.4 Electronic ballot box integrity | The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature. | Functional | VSTL | Functional Requirement. Loss of Integrity and/or Confidentiality. | T=TEST | None | None | None | None | None | None | None | Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006. | N/A | | 1 | | | | | 1 | | | 1 | 1 | N/C |
| 5.4.1.5 Malware detection | The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications. | Inspection | VSTL | Loss of Integrity, Confidentiality and/or Availability. | T=TEST | SI-3<br>SI-4 | Malicious Code Protection Information System Monitoring Tools and Techniques | 10.4.1; 10.6.2; 10.10.1; 10.10.2; 10.10.4 | 11.1.1; 11.1.2 | --- | ECVP-1; VIVM-1; EBBD-1; EBVC-1; ECID-1 | 5.B.1.a(4); 7.B.4.b(1) | | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 5.4.1.6 Updating malware detection | The voting system SHALL provide a mechanism for updating malware detection signatures. | Inspection | VSTL | Loss of Integrity, Confidentiality and/or Availability. | T=TEST | SI-3 | Malicious Code Protection | 10.4.1 | 11.1.1; 11.1.2 | --- | ECVP-1; VIVM-1 | 5.B.1.a(4); 7.B.4.b(1) | NIST Special Publication 800-61 provides guidance on detecting attacks through various types of security technologies. NIST Special Publication 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. NIST Special Publication 800-92 provides guidance on monitoring and analyzing computer security event logs. NIST Special Publication 800-94 provides guidance on intrusion detection and prevention. Related security control: AC-8.<br>National Institute of Standards and Technology Special Publication 800-83, Guide to Malware Incident Prevention and Handling, November 2005. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 5.4.1.7 Validating software on kiosk voting devices | The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations. | Inspection | VSTL | Functional Requirement No direct impact on security. | T=TEST | SI-6 | Security Functionality Verification | --- | 11.2.1; 11.2.2 | SS-2.2 | DCSS-1 | 4.B.1.c(2); 5.B.2.b(2) | SI-6<br>SECURITY FUNCTIONALITY VERIFICATION<br>Control: The information system verifies the correct operation of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered.<br>Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required. | N/A | | 1 | | | | | 1 | 1 | | | | N/C |
| 5.5.1.1 Data integrity protection | Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic. | Functional | VSTL | Integrity Controls for transmission. Impacts confidentiality, Availability and Integrity. | I=INSPECTION | SC-16 | Transmission of Security Parameters | 7.2.2; 10.8.2; 10.9.2 | 16.1.6 | AC-3.2 | ECTM-2 | 4.B.1.a(3) | ECTM-2 Transmission Integrity Controls<br>Good engineering practices with regards to the integrity mechanisms of COTS, GOTS, and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs). Mechanisms are in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels). | N/A | | 1 | | | | | 1 | 1 | | | | N/C |
| 5.5.1.2 TLS/SSL | Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0). | Functional | VSTL | Integrity Controls for transmission. Impacts confidentiality, Availability and Integrity. | T=TEST | SC-8<br>SC-16 | Transmission Integrity | 10.6.1; 10.8.1; 10.9.1 | 11.2.1; 11.2.4; 11.2.9; 16.2.14 | AC-3.2 | ECTM-1 | 5.B.3.a(11) | National Institute of Standards and Technology Special Publication 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, June 2005.<br>IA-3<br>DEVICE IDENTIFICATION AND AUTHENTICATION<br>Control: The information system identifies and authenticates specific devices before establishing a connection.<br>Supplemental Guidance: The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication.<br>NIST Special Publication 800-77 provides guidance on protecting transmission integrity using IPsec. NIST Special Publication 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. | N/A | 1 | 1 | | | | 1 | | 1 | | | | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 6.1 General Requirements | At a minimum, this program SHALL: a. Include procedures for specifying, procuring, inspecting, accepting, and controlling parts and raw materials of the requisite quality; b. Require the documentation of the software development process; c. Require the documentation of the hardware specification and selection process; d. Identify and enforce all requirements for: i. In-process inspection and testing that the manufacturer deems necessary to ensure proper fabrication and assembly of hardware ii. Installation and operation of software and firmware e. Include plans and procedures for post-production environmental screening and acceptance testing; and f. Include a procedure for maintaining all data and records required to document and verify the quality inspections and tests. | Inspection | Manufacturer | Integrity Controls for transmission. Impacts confidentiality, Availability and Integrity. | I=INSPECTION | SA-4 | Acquisitions | 12.1.1 | 3.1.6;<br>3.1.7;<br>3.1.10;<br>3.1.11;<br>3.1.12 | --- | DCAS-1; DCDS-1; DCIT-1; DCMC-1 | DCID: B.2.a; C.2.a; Manual:; 9.B.4 | SA-4<br>ACQUISITIONS<br>Control: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 6.2 Components from Third Parties | A manufacturer who does not manufacture all the components of its voting system, but instead procures components as standard commercial items for assembly and integration into a voting system, SHALL verify that the supplier manufacturers follow documented quality assurance procedures that are at least as stringent as those used internally by the voting system manufacturer. | Inspection | Manufacturer | loss of Integrity, availability and/or Confidentiality | I=INSPECTION | None | None | None | None | None | None | None | Nothing found in referencfed documentation. However, this may be referenced within another publication involving acquisitions. | N/A | 1 | 1 | 1 | | | 1 | | | | 1 | | N/C |
| 6.3 Responsibility for Tests | Manufacturer SHALL be responsible for performing all quality assurance tests, acquiring and documenting test data, and providing test reports for examination by the VSTL as part of the national certification process. These reports SHALL also be provided to the purchaser upon request. | Inspection | Manufacturer | loss of Integrity, availability and/or Confidentiality | I=INSPECTION | None | None | None | None | None | None | None | Nothing found in referencfed documentation. However, this may be referenced within another publication involving acquisitions. | N/A | | 1 | 1 | | | 1 | | | | 1 | | N/C |
| 6.4 Parts and Materials, Special Tests, and Examinations | In order to ensure that voting system parts and materials function properly, manufacturers SHALL: a. Select parts and materials to be used in voting systems and components according to their suitability for the intended application. Suitability may be determined by similarity of this application to existing standard practice or by means of special tests; b. Design special tests, if needed, to evaluate the part or material under conditions accurately simulating the actual voting system operating environment; and c. Maintain the resulting test data as part of the quality assurance program documentation. | Inspection | Manufacturer | loss of Integrity, availability and/or Confidentiality | I=INSPECTION | None | None | None | None | None | None | None | Nothing found in referencfed documentation. However, this may be referenced within another publication involving acquisitions. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 6.5 Quality Conformance Inspections | The manufacturer performs conformance inspections to ensure the overall quality of the voting system and components delivered to the VSTL for national certification testing and to the jurisdiction for implementation. To meet the conformance inspection requirements the manufacturer SHALL: a. Inspect and test each voting system or component to verify that it meets all inspection and test requirements for the voting system; and b. Deliver a record of tests or a certificate of satisfactory completion with each voting system or component. | Inspection | Manufacturer | No specific requirement for vendor testing identified. Loss of Integrity, availability and/or Confidentiality | I=INSPECTION | None | None | None | None | None | None | None | ECMT-2 Conformance Monitoring and Testing<br>Conformance testing that includes periodic, unannounced in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is planned, scheduled, conducted, and independently validated. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 7.1.1 Configuration Management Requirements | The configuration management documentation provided for manufacturer registration SHALL be sufficient for pilot projects. | Inspection | Test Entity: EAC | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | CM-1 | Configuration Management Policy and Procedures | 12.4.1; 12.5.1; 15.1.1 | --- | --- | DCCB-1; DCPR-1; DCAR-1; E3.3.8 | DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5) | CM-1<br>CONFIGURATION MANAGEMENT POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 7.1.2 Audit of Configuration Management Documentation | The manufacturer SHALL provide the following documentation to the EAC for review. This documentation will be audited during the registration review which will be conducted during the pilot testing period. The items which the EAC will audit are the following: a. Application of configuration management requirements; b. Configuration management policy; c. Configuration identification; d. Baseline, promotion, and demotion procedures; e. Configuration control procedures; f. Release process; g. Configuration audits; and h. Configuration management resources. | Inspection | Test Entity: EAC | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION & T=TEST | CM-1 | Configuration Management Policy and Procedures | 12.4.1; 12.5.1; 15.1.1 | --- | --- | DCCB-1; DCPR-1; DCAR-1; E3.3.8 | DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5) | Not vendor specific<br>CM-1<br>CONFIGURATION MANAGEMENT POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. | N/A | | 1 | 1 | | | 1 | | 1 | | | | |
| 7.2.1 Classification and Naming Configuration Items | Manufacturers SHALL describe the procedures and conventions used to classify configuration items into categories and subcategories, uniquely number or otherwise identify configuration items and name configuration items. | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | CM-1 | Configuration Management Policy and Procedures | 12.4.1; 12.5.1; 15.1.1 | --- | --- | DCCB-1; DCPR-1; DCAR-1; E3.3.8 | DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5) | Not vendor specific<br>CM-1<br>CONFIGURATION MANAGEMENT POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 7.2.2 Versioning Conventions | When a voting system component is part of a higher level system element such as a subsystem, the manufacturer SHALL describe the conventions used to: a. Identify the specific versions of individual configuration items and sets of items that are incorporated in higher level system elements such as subsystems; b. Uniquely number or otherwise identify versions; and c. Name versions. | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | CM-1 | Configuration Management Policy and Procedures | 12.4.1; 12.5.1; 15.1.1 | --- | --- | DCCB-1; DCPR-1; DCAR-1; E3.3.8 | DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5) | Not vendor specific<br>CM-1<br>CONFIGURATION MANAGEMENT POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 7.3 Baseline and Promotion Procedures | Manufacturers SHALL establish formal procedures and conventions for establishing and providing a complete description of the procedures and related conventions used to: a. Establish a particular instance of a component as the starting baseline; b. Promote subsequent instances of a component to baseline status as development progresses through to completion of the initial completed version released to the VSTL for testing; and c. Promote subsequent instances of a component to baseline status as the component is maintained throughout its life cycle until system retirement (i.e., the system is no longer sold or maintained by the manufacturer). | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | CM-2 | Baseline Configuration | 7.1.1; 15.1.2 | 1.1.1;<br>3.1.9;<br>10.2.7;<br>10.2.9;<br>12.1.4 | CC-2.3; CC-3.1; SS-1.2 | DCHW-1; DCSW-1 | 2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6) | Not vendor specific<br>CM-2<br>BASELINE CONFIGURATION<br>Control: The organization develops, documents, and maintains a current baseline configuration of the information system. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | |
| 7.4 Configuration Control Procedures | Configuration control is the process of approving and implementing changes to a configuration item to prevent unauthorized additions, changes or deletions. The manufacturer SHALL establish such procedures and related conventions, providing a complete description of those procedures used to: a. Develop and maintain internally developed items; b. Acquire and maintain third-party items; c. Resolve internally identified defects for items regardless of their origin; and d. Resolve externally identified and reported defects (i.e., by customers and VSTLs). | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | CM-3 | Configuration Change Control | 10.1.2; 10.2.3; 12.4.1; 12.5.1; 12.5.2; 12.5.3 | 3.1.4;<br>10.2.2;<br>10.2.3;<br>10.2.8;<br>10.2.10;<br>10.2.11 | SS-3.2; CC-2.2 | DCPR-1 | 2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6); 5.B.2.a(5) | Not vendor specific<br>CM-3<br>CONFIGURATION CHANGE CONTROL<br>Control: The organization authorizes, documents, and controls changes to the information system. | N/A | | 1 | 1 | | 1 | | | 1 | | | | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7.5.1 Physical Configuration Audit (PCA) | For the PCA, a manufacturer SHALL provide: a. Identification of all items that are to be a part of the pilot release; b. Specification of compiler (or choice of compilers) to be used to generate voting system executable programs; c. Identification of all hardware that interfaces with the software; d. Configuration baseline data for all hardware that is unique to the voting system; e. Copies of all software documentation intended for distribution to users, including program listings, specifications, operations manual, voter manual, and maintenance manual; f. Identification of any changes between the physical configuration of the voting system submitted for the PCA and that submitted for the Functional Configuration Audit (FCA), with a certification that any differences do not degrade the functional characteristics; and g. Complete descriptions of its procedures and related conventions used to support this audit by i. Establishing a configuration baseline of the software and hardware to be tested; and ii. Confirming whether the voting system documentation matches the corresponding system components. | Inspection | VSTL | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | CM-2 | Baseline Configuration | 7.1.1; 15.1.2 | 1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4 | CC-2.3; CC-3.1; SS-1.2 | DCHW-1; DCSW-1 | 2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6) | Not vendor specific<br>CM-2<br>BASELINE CONFIGURATION<br>Control: The organization develops, documents, and maintains a current baseline configuration of the information system. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 7.5.2 Functional Configuration Audit (FCA) | The Functional Configuration Audit is conducted by the VSTL to verify that the voting system performs all the functions described in the system documentation. Manufacturers SHALL: a. Completely describe its procedures and related conventions used to support this audit for all voting system components; and b. Provide the following information to support this audit: c. Copies of all procedures used for module or unit testing, integration testing, and system testing; d. Copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for system tests; and e. Records of all tests performed by the procedures listed above, including error corrections and retests. | Functional / Inspection | VSTL | Configuration/Testing | I=INSPECTION | None | None | None | None | None | None | None | | N/A | 1 | 1 | 1 | | | 1 | | | | 1 | | N/C |
| 8.1.1.1.1 Identify full system configuration | Manufacturers SHALL submit to the VSTL documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan by the VSTL. | Inspection | Manufacturer | Documentation | I=INSPECTION | CM-2 | Baseline Configuration | 7.1.1; 15.1.2 | 1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4 | CC-2.3; CC-3.1; SS-1.2 | DCHW-1; DCSW-1 | 2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6) | DCHW-1 HW Baseline<br>A current and comprehensive baseline inventory of all hardware (HW) (to include manufacturer, type, model, physical location and network topology or architecture) required to support enclave operations is maintained by the Configuration Control Board (CCB) and as part of the SSAA. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | 1 | N/C |
| 8.1.1.1.2 Required content for pilot certification | Manufacturers SHALL provide a list of all documents submitted controlling the design, construction, operation, and maintenance of the voting system. At minimum, the TDP SHALL contain the following documentation:  Implementation statement;  Voting system user documentation (See Section 9 Voting Equipment User Documentation);  System hardware specification;  Application logic design and specification;  System security specification;  System test specification;  Configuration for testing; and  Training documentation. | Inspection | Manufacturer | Documentation | I=INSPECTION | CM-2 | Baseline Configuration | 7.1.1; 15.1.2 | 1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4 | CC-2.3; CC-3.1; SS-1.2 | DCHW-1; DCSW-1 | 2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6) | DCHW-1 HW Baseline<br>A current and comprehensive baseline inventory of all hardware (HW) (to include manufacturer, type, model, physical location and network topology or architecture) required to support enclave operations is maintained by the Configuration Control Board (CCB) and as part of the SSAA. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original. | N/A | | 1 | | | 1 | | | 1 | | | 1 | N/C |
| 8.1.1.2.1 Table of contents and abstracts | The TDP SHALL include a detailed table of contents for the required documents, an abstract of each document, and a listing of each of the informational sections and appendices presented. | Inspection | Manufacturer | Documentation | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | Hundreds of references to design and documentation requierments | N/A | | 1 | | | 1 | | | 1 | | | 1 | N/C |
| 8.1.1.2.2 Cross-index | A cross-index SHALL be provided indicating the portions of the documents that are responsive to the documentation requirements enumerated in section 8.1.1.1.2. | Inspection | Manufacturer | Documentation | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | Hundreds of references to design and documentation requierments | N/A | | 1 | | | 1 | | | 1 | | | 1 | N/C |
| 8.1.2.1 Identify proprietary data | Manufacturers SHALL identify all documents, or portions of documents, containing proprietary information that is not releasable to the public. | Inspection | Manufacturer | Documentation | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | Hundreds of references to design and documentation requierments | N/A | | 1 | 1 | | 1 | | | 1 | | | 1 | N/C |
| 8.2.1 TDP Implementation Statement | The TDP SHALL include an implementation statement. | Inspection | Manufacturer | Documentation | I=INSPECTION | None | None | None | None | None | None | None | None | N/A | | | 1 | | 1 | | | | | 1 | 1 | N/C |
| 8.3.1 System Hardware Specification Scope | Manufacturers SHALL expand on the system overview included in the user documentation by providing detailed specifications of the hardware components of the voting system, including specifications of hardware used to support the telecommunications capabilities of the voting system, if applicable. | Inspection | Manufacturer | Documentation | I=INSPECTION | MA-1 | System Maintenance Policy and Procedures | 10.1.1; 15.1.1 | 10 | --- | PRMP-1; DCAR-1 | DCID: B.2.a Manual: 2.B.4.e(5); 6.B.2.a(5) | Hundreds of references to design and documentation requierments | N/A | | | 1 | | 1 | | | 1 | | | 1 | N/C |
| 8.3.2.1 Description of hardware characteristics | Manufacturers SHALL provide a detailed discussion of the characteristics of the system, indicating how the hardware meets individual requirements defined in this document, including: a. Performance characteristics: Basic system performance attributes and operational scenarios that describe the manner in which system functions are invoked, describe environmental capabilities, describe life expectancy, and describe any other essential aspects of system performance; b. Physical characteristics: Suitability for intended use, requirements for security criteria, and vulnerability to adverse environmental factors; c. Reliability: System and component reliability stated in terms of the system's operating functions, and identification of items that require special handling or operation to sustain system reliability; and d. Environmental conditions: Ability of the system to withstand natural environments, and operational constraints in normal and test environments, including all requirements and restrictions regarding electrical service, telecommunications services, environmental protection, and any additional facilities or resources required to install and operate the system. | Inspection | Manufacturer | Documentation | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | Hundreds of references to design and documentation requierments | N/A | 1 | 1 | 1 | | 1 | | | 1 | | | 1 | N/C |
| 8.3.3.1 System configuration | Manufacturers SHALL provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for testing. | Inspection | Manufacturer | Documentation | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | Hundreds of references to design and documentation requierments | N/A | | | 1 | | | 1 | | 1 | | | 1 | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8.3.3.2 Photographs for hardware validation | Manufacturers SHALL provide photographs of the exterior and interior of devices included in the system to identify the hardware of the system configuration submitted for testing. | Inspection | Manufacturer | Documentation | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | Hundreds of references to design and documentation requierments | N/A | | | 1 | | 1 | | | 1 | | | 1 | N/C |
| 8.3.3.3 List of materials | Manufacturers SHALL provide a list of materials and components used in the system and a description of their assembly into major system components and the system as a whole. | Inspection | Manufacturer | Documentation | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | Not vendor specific<br>Hundreds of references to design and documentation requierments | N/A | 1 | 1 | 1 | | 1 | | | 1 | | | 1 | N/C |
| 8.3.3.4 Design and construction miscellany | Text and diagrams SHALL be provided that describe: a. Materials, processes, and parts used in the system, their assembly, and the configuration control measures to ensure compliance with the system specification; b. Electromagnetic environment generated by the system; and c. Operator and voter safety considerations and any constraints on system operations or the use environment. | Inspection | Manufacturer | Documentation | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | Hundreds of references to design and documentation requierments | N/A | 1 | 1 | 1 | | 1 | | | 1 | | | 1 | N/C |
| 8.3.4.1 Hardwired and mechanical implementations of logic | For each non-COTS hardware component (e.g., an application-specific integrated circuit or a manufacturer-specific integration of smaller components), manufacturers SHALL provide complete design and logic specifications, such as Computer Aided Design and Hardware Description Language files. | Inspection | Manufacturer | Industrial controll logic could impact Confidentiality, Integrity and/or Availability. | I=INSPECTION | None | None | None | None | None | None | None | NIST SP800-53 Reference: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes. | None | 1 | 1 | 1 | | | | 1 | | | 1 | | N/C |
| 8.3.4.2 Logic specifications for PLDs, FPGAs and PICs | For each Programmable Logic Device (PLD), Field-Programmable Gate Array (FPGA), or Peripheral Interface Controller (PIC) that is programmed with non- COTS logic, manufacturers SHALL provide complete logic specifications, such as Hardware Description Language files or source code. | Inspection | Manufacturer | Industrial controll logic could impact Confidentiality, Integrity and/or Availability. | I=INSPECTION | None | None | None | None | None | None | None | NIST SP800-53 Reference: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes. | None | 1 | 1 | 1 | | | | 1 | | | 1 | | N/C |
| 8.4.1 Application Logic Design and Specification | Manufacturers SHALL expand on the system overview included in the user documentation by providing detailed specifications of the application logic components of the system, including those used to support the telecommunications capabilities of the system, if applicable. | Inspection | Manufacturer | Documentation | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | Not vendor specific. No specific IA Control referenced. | N/A | 1 | 1 | 1 | | 1 | | | 1 | | | 1 | N/C |
| 8.4.2.1 Application logic functions | Manufacturers SHALL describe the function or functions that are performed by the application logic comprising the system, including that used to support the telecommunications capabilities of the system, if applicable. | Inspection | Manufacturer | Documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | No specific IA Control referenced. | N/A | 1 | 1 | 1 | | 1 | | | | | | | N/C |
| 8.4.3.1 Documents controlling application logic development | Manufacturers SHALL list all documents controlling the development of application logic and its specifications. | Inspection | Manufacturer | Documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | No specific IA Control referenced. | N/A | 1 | 1 | 1 | | 1 | | | | | | | N/C |
| 8.4.4.1 Application logic overview | Manufacturers SHALL provide an overview of the application logic. | Inspection | Manufacturer | Documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | No specific IA Control referenced. | N/A | 1 | 1 | 1 | | 1 | | | | | | | N/C |
| 8.4.4.2 Application logic architecture | The overview SHALL include a description of the architecture, the design objectives, and the logic structure and algorithms used to accomplish those objectives. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | PL-2 | System Security Plan | 6.1 | 4.1.5; 5.1.1; 5.1.2; 12.2.1 | SP-2.1 | DCSD-1 | 1.F.6; 2.B.6.c(3); 2.B.7.c(5); 9.E.2.a(1)(d); 9.F.2.a; Appendix C | PL-2<br>SYSTEM SECURITY PLAN<br>Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan. | N/A | 1 | 1 | 1 | | 1 | | | 1 | | | | N/C |
| 8.4.4.3 Application logic design | The overview SHALL include the general design, operational considerations, and constraints influencing the design. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | PL-2 | System Security Plan | 6.1 | 4.1.5; 5.1.1; 5.1.2; 12.2.1 | SP-2.1 | DCSD-1 | 1.F.6; 2.B.6.c(3); 2.B.7.c(5); 9.E.2.a(1)(d); 9.F.2.a; Appendix C | PL-2<br>SYSTEM SECURITY PLAN<br>Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan. | N/A | 1 | 1 | 1 | | 1 | | | 1 | | | | N/C |
| 8.4.4.4 Application logic overview miscellany | The overview SHALL include the following additional information for each separate software package: a. Package identification; b. General description; c. Requirements satisfied by the package; d. Identification of interfaces with other packages that provide data to, or receive data from, the package; and e. Concept of execution for the package. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan. | I=INSPECTION | PL-2 | System Security Plan | 6.1 | 4.1.5; 5.1.1; 5.1.2; 12.2.1 | SP-2.1 | DCSD-1 | 1.F.6; 2.B.6.c(3); 2.B.7.c(5); 9.E.2.a(1)(d); 9.F.2.a; Appendix C | PL-2<br>SYSTEM SECURITY PLAN<br>Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan. | N/A | 1 | 1 | 1 | | 1 | | | 1 | | | | N/C |
| 8.4.5.1 Application logic standards and conventions | Manufacturers SHALL provide information on application logic standards and conventions developed internally by the manufacturer as well as published industry standards that have been applied by the manufacturer. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | PL-2 | System Security Plan | 6.1 | 4.1.5; 5.1.1; 5.1.2; 12.2.1 | SP-2.1 | DCSD-1 | 1.F.6; 2.B.6.c(3); 2.B.7.c(5); 9.E.2.a(1)(d); 9.F.2.a; Appendix C | PL-2<br>SYSTEM SECURITY PLAN<br>Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan. | N/A | 1 | 1 | 1 | | 1 | | | 1 | | | | N/C |
| 8.4.5.2 Application logic standards and conventions, checklist | Manufacturers SHALL provide information that addresses the following standards and conventions related to application logic: a. Development methodology; b. Design standards, including internal manufacturer procedures; c. Specification standards, including internal manufacturer procedures; d. Coding conventions, including internal manufacturer procedures; e. Testing and verification standards, including internal manufacturer procedures, that can assist in determining the correctness of the logic; and f. Quality assurance standards or other documents that can be used to examine and test the application logic. These documents include standards for logic diagrams, program documentation, test planning, and test data acquisition and reporting. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | PL-2 | System Security Plan | 6.1 | 4.1.5; 5.1.1; 5.1.2; 12.2.1 | SP-2.1 | DCSD-1 | 1.F.6; 2.B.6.c(3); 2.B.7.c(5); 9.E.2.a(1)(d); 9.F.2.a; Appendix C | PL-2<br>SYSTEM SECURITY PLAN<br>Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan. | N/A | 1 | 1 | 1 | | 1 | | | 1 | | | | N/C |
| 8.4.5.3 Justify coding conventions | Manufacturers SHALL furnish evidence that the selected coding conventions are "published" and "credible" as specified in section 4.3.1. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan under "robustness". Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | None | None | None | None | None | None | None | NIST SP800-137 References coding practices.<br>DCID 6/3: 1.H.1 In the following pages, the term "good engineering practice" refers to the state of the engineering art for commercial systems that have equivalent problems and solutions; a good engineering practice by definition meets commercial requirements. These practices are usually part of the normal installation and operating procedures for systems. When placing security reliance on items that implement good engineering practice (such as commercial off-the shelf [COTS] software), the DAAs or their designees shall verify that the item(s) are set up properly and are operating as expected. | N/A | 1 | 1 | 1 | | 1 | | | | | 1 | | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8.4.6.1 Application logic operating environment | Manufacturers SHALL describe or make reference to all operating environment factors that influence the design of application logic. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan under "robustness". Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | None | None | None | None | None | None | None | None | None | 1 | 1 | 1 | | | 1 | | | | 1 | | N/C |
| 8.4.7.1 Hardware environment and constraints | Manufacturers SHALL identify and describe the hardware characteristics that influence the design of the application logic, such as: a. Logic and arithmetic capability of the processor; b. Memory read-write characteristics; c. External memory device characteristics; d. Peripheral device interface hardware; e. Data input/output device protocols; and f. Operator controls, indicators, and displays. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan under "robustness". Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | None | None | None | None | None | None | None | None | None | 1 | 1 | 1 | | 1 | | | | | 1 | | N/C |
| 8.4.8.1 Operating system | Manufacturers SHALL identify the operating system and the specific version thereof, or else clarify how the application logic operates without an operating system. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | PL-2 | System Security Plan | 6.1 | 4.1.5; 5.1.1; 5.1.2; 12.2.1 | SP-2.1 | DCSD-1 | 1.F.6; 2.B.6.c(3); 2.B.7.c(5); 9.E.2.a(1)(d) ; 9.F.2.a; Appendix C | PL-2<br>SYSTEM SECURITY PLAN<br>Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan. | N/A | 1 | 1 | 1 | | 1 | | | 1 | | | | N/C |
| 8.4.8.2 Compilers and assemblers | For systems containing compiled or assembled application logic, manufacturers SHALL identify the COTS compilers or assemblers used in the generation of executable code, and the specific versions thereof. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | None | None | None | None | None | None | None | None. Only references backups should provide for the protection of compilers. | None. Only references backups should provide for the protection of compilers. | 1 | 1 | 1 | | 1 | | | | | 1 | | N/C |
| 8.4.8.3 Interpreters | For systems containing interpreted application logic, manufacturers SHALL specify the COTS runtime interpreter that SHALL be used to run this code, and the specific version thereof. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | None | None | None | None | None | None | None | None. Only references backups should provide for the protection of compilers. | None. Only references backups should provide for the protection of compilers. | 1 | 1 | 1 | | 1 | | | | | 1 | | N/C |
| 8.4.9.1 Application logic functional specification | Manufacturers SHALL provide a description of the operating modes of the system and of application logic capabilities to perform specific functions. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | None | None | None | None | None | None | None | None | None | 1 | 1 | 1 | | 1 | | | | | 1 | | N/C |
| 8.4.10.1 Functions and operating modes | Manufacturers SHALL describe all application logic functions and operating modes of the system, such as ballot preparation, election programming, preparation for opening the voting period, recording votes and/or counting ballots, closing the voting period, and generating reports. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | MA-1 | System Maintenance Policy and Procedures | 10.1.1; 15.1.1 | 10 | --- | PRMP-1; DCAR-1 | DCID: B.2.a Manual: 2.B.4.e(5); 6.B.2.a(5) | CM-6; DCSS-1; ECSC-1 | N/A | 1 | 1 | 1 | | 1 | | | 1 | | | | N/C |
| 8.4.10.2 Functions and operating modes detail | For each application logic function or operating mode, manufacturers SHALL provide: a. A definition of the inputs to the function or mode (with characteristics, limits, tolerances or acceptable ranges, as applicable); b. An explanation of how the inputs are processed; and c. A definition of the outputs produced (again, with characteristics, limits, tolerances, or acceptable ranges, as applicable). | Inspection | Manufacturer | Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SI-9 | Information Input Restrictions | 12.2.1; 12.2.2 | --- | SD-1 | --- | 2.B.9.b(11) | SI-9<br>INFORMATION INPUT RESTRICTIONS<br>Control: The organization restricts the capability to input information to the information system to authorized personnel.<br>Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities. | N/A | | 1 | | | | 1 | | 1 | | | | N/C |
| 8.4.11.1 Application logic integrity features | Manufacturers SHALL describe the application logic's capabilities or methods for detecting or handling: a. Exception conditions; b. System failures; c. Data input/output errors; d. Error logging for audit record generation; e. Production of statistical ballot data; f. Data quality assessment; and g. Security monitoring and control. | Inspection | Manufacturer | Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SI-11 | Error Handling | 12.2.1; 12.2.2; 12.2.3; 12.2.4 | --- | --- | --- | 2.B.4.d | SI-11<br>ERROR HANDLING<br>Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.12.1 Programming specifications | Manufacturers SHALL provide in this section an overview of the application logic's design, its structure, and implementation algorithms and detailed specifications for individual modules. | Inspection | Manufacturer | Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SI-2 | Flaw Remediation | 10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1 | 10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7 | SS-2.2 | DCSQ-1; DCCT-1; VIVM-1 | 5.B.2.a(5)(a)(3); 6.B.2.a(5) | DCSQ-1 Software Quality<br>Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.13.1 Programming specifications overview, diagrams | This overview SHALL include such items as Unified Modeling Language diagrams, data flow diagrams, and/or other graphical techniques that facilitate understanding of the programming specifications. | Inspection | Manufacturer | Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SI-2 | Flaw Remediation | 10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1 | 10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7 | SS-2.2 | DCSQ-1; DCCT-1; VIVM-1 | 5.B.2.a(5)(a)(3); 6.B.2.a(5) | DCSQ-1 Software Quality<br>Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.13.3 Programming specifications overview, content | Implementation of the functions SHALL be described in terms of the architecture, algorithms, and data structures. | Inspection | Manufacturer | Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SI-2 | Flaw Remediation | 10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1 | 10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7 | SS-2.2 | DCSQ-1; DCCT-1; VIVM-1 | 5.B.2.a(5)(a)(3); 6.B.2.a(5) | DCSQ-1 Software Quality<br>Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.14.1 Programming specifications details | The programming specifications SHALL describe individual application logic modules and their component units, if applicable. | Inspection | Manufacturer | Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SI-2 | Flaw Remediation | 10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1 | 10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7 | SS-2.2 | DCSQ-1; DCCT-1; VIVM-1 | 5.B.2.a(5)(a)(3); 6.B.2.a(5) | DCSQ-1 Software Quality<br>Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.14.2 Module and callable unit documentation | For each application logic module and callable unit, manufacturers SHALL document: a. Significant module and unit design decisions, if any, such as algorithms used; b. Any constraints, limitations, or unusual features in the design of the module or callable unit; and c. A description of its inputs, outputs, and other data elements as applicable with respect to communication over system interfaces. (See section 8.4.16 Interfaces.) | Inspection | Manufacturer | Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SI-2 | Flaw Remediation | 10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1 | 10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7 | SS-2.2 | DCSQ-1; DCCT-1; VIVM-1 | 5.B.2.a(5)(a)(3); 6.B.2.a(5) | DCSQ-1 Software Quality<br>Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8.4.14.3 Mixed-language software | If an application logic module is written in a programming language other than that generally used within the system, the specification for the module SHALL indicate the programming language used and the reason for the difference. | Inspection | Manufacturer | Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SI-2 | Flaw Remediation | 10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1 | 10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7 | SS-2.2 | DCSQ-1; DCCT-1; VIVM-1 | 5.B.2.a(5)(a)(3); 6.B.2.a(5) | DCSQ-1 Software Quality<br>Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.14.4 References for foreign programming languages | If a module contains embedded border logic commands for an external library or package (e.g., menu selections in a database management system for defining forms and reports, on-line queries for database access and manipulation, input to a graphical user interface builder for automated code generation, commands to the operating system, or shell scripts), the specification for the module SHALL contain a reference to user manuals or other documents that explain them. | Inspection | Manufacturer | Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SI-2 | Flaw Remediation | 10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1 | 10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7 | SS-2.2 | DCSQ-1; DCCT-1; VIVM-1 | 5.B.2.a(5)(a)(3); 6.B.2.a(5) | DCSQ-1 Software Quality<br>Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.14.5 Source code | For each callable unit (e.g., function, method, operation, subroutine, procedure) in application logic, border logic, and third-party logic, manufacturers SHALL supply the source code. | Inspection | Manufacturer | Loss of Availability | I=INSPECTION | SA-6 | Software Usage Restrictions | 15.1.2 | 10.2.10; 10.2.13 | SS-3.2; SP-2.1 | DCPD-1 | 2.B.9.b(11) | NIST SP500-209DCID 6/3 Requirement: the original (source) code must be available at any time, the code must be controlled in a configuration management process, and the code must be marked with ownership and authorship.<br>DCPD-1 Public Domain Software Controls<br>Binary or machine executable public domain software products and other software products with limited or no warranty, such as those commonly known as freeware or shareware are not used in DoD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available. Such products are assessed for information assurance impacts, and approved for use by the DAA. The assessment addresses the fact that such software products are difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government. | N/A | | | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.14.6 Inductive assertions | For each callable unit (e.g., function, method, operation, subroutine, procedure) in core logic, manufacturers SHALL specify: a. Preconditions and postconditions of the callable unit, including any assumptions about capacities and limits within which the system is expected to operate; and b. A sound argument (preferably, but not necessarily, a formal proof) that the preconditions and postconditions of the callable unit accurately represent its behavior, assuming that the preconditions and postconditions of any invoked units are similarly accurate. | Inspection | Manufacturer | Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SA-8 | Security Engineering Principles | 12.1 | 3.2.1 | --- | DCBP-1; DCCS-1; E3.4.4 | 1.H.1 | NIST SP500-209SA-8<br>SECURITY ENGINEERING PRINCIPLES<br>Control: The organization designs and implements the information system using security engineering principles.<br>Supplemental Guidance: NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.14.7 High-level constraints | Manufacturers SHALL specify a sound argument (preferably, but not necessarily, a formal proof) that the core logic as a whole satisfies each of the constraints for all cases within the aforementioned capacities and limits, assuming that the preconditions and postconditions of callable units accurately characterize their behaviors. | Inspection | Manufacturer | Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SA-8 | Security Engineering Principles | 12.1 | 3.2.1 | --- | DCBP-1; DCCS-1; E3.4.4 | 1.H.1 | NIST SP500-209SA-8 (Not in searched Documetation)<br>SECURITY ENGINEERING PRINCIPLES<br>Control: The organization designs and implements the information system using security engineering principles.<br>Supplemental Guidance: NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.14.8 Safety of concurrency | Manufacturers SHALL specify a sound argument (preferably, but not necessarily, a formal proof) that application logic is free of race conditions, deadlocks, livelocks, and resource starvation. | Inspection | Manufacturer | Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SC-6 | Resource Priority | --- | --- | --- | --- | 6.B.3.a(11) | SC-6<br>RESOURCE PRIORITY<br>Control: The information system limits the use of resources by priority.<br>Supplemental Guidance: Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process. | | | 1 | 1 | | | 1 | | 1 | | | | |
| 8.4.15.1 System database | Manufacturers SHALL identify and provide a diagram and narrative description of the system's databases and any external files used for data input or output. | Inspection | Manufacturer | Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity. | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | SA-5<br>INFORMATION SYSTEM DOCUMENTATION<br>Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. | | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.15.2 Database design levels | For each database or external file, manufacturers SHALL specify the number of levels of design and the names of those levels (e.g., conceptual, internal, logical, and physical). | Inspection | Manufacturer | Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality. | I=INSPECTION | SA-8 | Security Engineering Principles | 12.1 | 3.2.1 | --- | DCBP-1; DCCS-1; E3.4.4 | 1.H.1 | NIST SP500-209SA-8<br>SECURITY ENGINEERING PRINCIPLES<br>Control: The organization designs and implements the information system using security engineering principles.<br>Supplemental Guidance: NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.15.3 Database design conventions | For each database or external file, the manufacturer SHALL specify any design conventions and standards (which may be incorporated by reference) needed to understand the design. | Inspection | Manufacturer | Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity. | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | SA-5<br>INFORMATION SYSTEM DOCUMENTATION<br>Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.15.4 Data models | For each database or external file, manufacturers SHALL identify and describe all logical entities and relationships and how these are implemented physically (e.g., tables, files). | Inspection | Manufacturer | Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity. | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | SA-5<br>INFORMATION SYSTEM DOCUMENTATION<br>Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.15.5 Schemata | Manufacturers SHALL document the details of table, record or file contents (as applicable), individual data elements and their specifications, including: a. Names/identifiers; b. Data type (e.g., alphanumeric, integer); c. Size and format (such as length and punctuation of a character string); d. Units of measurement (e.g., meters, seconds e. Range or enumeration of possible values (e.g., 0–99 f. Accuracy (how correct) and precision (number of significant digits); g. Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply; h. Security and privacy constraints; and i. Sources (setting/sending entities) and recipients (using/receiving entities). | Inspection | Manufacturer | Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity. | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | SA-5<br>INFORMATION SYSTEM DOCUMENTATION<br>Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8.4.15.6 External file maintenance and security | For external files, manufacturers SHALL document the procedures for file maintenance, management of access privileges, and security. | Inspection | Manufacturer | Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity. | I=INSPECTION | MA-1 | System Maintenance Policy and Procedures | 10.1.1; 15.1.1 | 10 | --- | PRMP-1; DCAR-1 | DCID: B.2.a Manual: 2.B.4.e(5); 6.B.2.a(5) | MA-1<br>SYSTEM MAINTENANCE POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.16.1 Description of interfaces | Using a combination of text and diagrams, manufacturers SHALL identify and provide a complete description of all major internal and external interfaces. | Inspection | Manufacturer | Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity. | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | DCFA-1 Functional Architecture for AIS Applications<br>For AIS applications, a functional architecture that identifies the following has been developed and is maintained:<br>- all external/internal interfaces, the information being exchanged, and the protection mechanisms associated with each interface<br>- user roles required for access control and the access privileges assigned to each role (See ECAN)<br>- unique security requirements (e.g., encryption of key data elements at rest)<br>- categories of sensitive information processed or stored by the AIS application, and their specific protection plans (e.g., Privacy Act, HIPAA)<br>- restoration priority of subsystems, processes, or information (see COEF). | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.17.1 Interface identification details | For each interface identified in the system overview, manufacturers SHALL: a. Provide a unique identifier assigned to the interface; b. Identify the interfacing entities (e.g., systems, configuration items, users) by name, number, version, and documentation references, as applicable; and c. Identify which entities have fixed interface characteristics (and therefore impose interface requirements on interfacing entities) and which are being developed or modified (thus having interface requirements imposed upon them). | Inspection | Manufacturer | Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity. | I=INSPECTION | MA-1 | System Maintenance Policy and Procedures | 10.1.1; 15.1.1 | 10 | --- | PRMP-1; DCAR-1 | DCID: B.2.a Manual: 2.B.4.e(5); 6.B.2.a(5) | MA-1<br>SYSTEM MAINTENANCE POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.18.1 Interface types | For each interface identified in the system overview, manufacturers SHALL describe the type of interface (e.g., real-time data transfer, data storage-and retrieval) to be implemented. | Inspection | Manufacturer | Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity. | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | SA-5<br>INFORMATION SYSTEM DOCUMENTATION<br>Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.18.2 Interface signatures | For each interface identified in the system overview, manufacturers SHALL describe characteristics of individual data elements that the interfacing entity (ies) will provide, store, send, access, receive, etc., such as: a. Names/identifiers; b. Data type (e.g., alphanumeric, integer); c. Size and format (such as length and punctuation of a character string); d. Units of measurement (e.g., meters, seconds); e. Range or enumeration of possible values (e.g., 0–99); f. Accuracy (how correct) and precision (number of significant digits); g. Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply; h. Security and privacy constraints; and i. Sources (setting/sending entities) and recipients (using/receiving entities). | Inspection | Manufacturer | Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity. | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | SA-5<br>INFORMATION SYSTEM DOCUMENTATION<br>Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.18.3 Interface protocols | For each interface identified in the system overview, manufacturers SHALL describe characteristics of communication methods that the interfacing entity (ies) will use for the interface, such as: a. Communication links/bands/frequencies/media and their characteristics; b. Message formatting; c. Flow control (e.g., sequence numbering and buffer allocation); d. Data transfer rate, whether periodic/aperiodic, and interval between transfers; e. Routing, addressing, and naming conventions; f. Transmission services, including priority and grade; and g. Safety/security/privacy considerations, such as encryption, user authentication, compartmentalization, and auditing. | Inspection | Manufacturer | Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity. | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | SA-5<br>INFORMATION SYSTEM DOCUMENTATION<br>Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.18.4 Protocol details | For each interface identified in the system overview, manufacturers SHALL describe characteristics of protocols the interfacing entity (ies) will use for the interface, such as: a. Priority/layer of the protocol; b. Packeting, including fragmentation and reassembly, routing, and addressing; c. Legality checks, error control, and recovery procedures; d. Synchronization, including connection establishment, maintenance, termination; and e. Status, identification, and any other reporting features. | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | CA-3 | Information System Connections | 10.6.2; 10.9.1; 11.4.5; 11.4.6; 11.4.7 | 1.1.1; 3.2.9; 4.1.8; 12.2.3 | CC-2.1 | DCID-1; EBCR-1; EBRU-1; EBPW-1; ECIC-1 | 9.B.3; 9.D.3.c | CA-3<br>INFORMATION SYSTEM CONNECTIONS<br>Control: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.<br>NIST Special Publication 800-47 provides guidance on connecting information systems. Related security controls: SC-7, SA-9. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 8.4.18.5 Characteristics of interfaces | For each interface identified in the system overview, manufacturers SHALL describe any other pertinent characteristics, such as physical compatibility of the interfacing entity (ies) (e.g., dimensions, tolerances, loads, voltages, plug compatibility). | Inspection | Manufacturer | Loss of Availability | I=INSPECTION | CM-8 | Information System Component Inventory | 7.1.1; 15.1.2 | 1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4 | CC-2.3; CC-3.1; SS-1.2 | DCHW-1; DCSW-1 | 2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6) | CM-8<br>INFORMATION SYSTEM COMPONENT INVENTORY<br>Control: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.<br>Supplemental Guidance: The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system. Related security controls: CM-2, CM-6. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 9.2.1 User Documentation System Overview | In the system overview, manufacturers SHALL 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. | Inspection | Manufacturer | Loss of Availability | I=INSPECTION | CM-1 | Configuration Management Policy and Procedures | 12.4.1; 12.5.1; 15.1.1 | --- | --- | DCCB-1; DCPR-1; DCAR-1; E3.3.8 | DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5) | CM-1<br>CONFIGURATION MANAGEMENT POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. | | | 1 | 1 | | 1 | | | 1 | | | | N/C |
| 9.2.2 System Overview Functional Diagram | The system overview SHALL include a high-level functional diagram of the system that includes all of its components. The diagram SHALL portray how the various components relate and interact. | Inspection | Manufacturer | Loss of Integrity | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | Security Design and Configuration Integrity<br>DCFA-1 Functional Architecture for AIS Applications<br>For AIS applications, a functional architecture that identifies the following has been developed and is maintained:<br>- all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface<br>- user roles required for access control and the access privileges assigned to each role (See ECAN)<br>- unique security requirements (e.g., encryption of key data elements at rest)<br>- categories of sensitive information processed or stored by the AIS application, and their specific protection plans (e.g., Privacy Act, HIPAA)<br>- restoration priority of subsystems, processes, or information (see COEF). | | | 1 | 1 | | 1 | | | 1 | | | | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 9.2.3.1 User documentation system description | The system description SHALL include written descriptions, drawings and diagrams that present: a. A description of the functional components or subsystems, (e.g., environment, election management and control, vote recording, vote conversion, reporting, and their logical relationships); b. A description of the operational environment of the system that provides an overview of the hardware, firmware, software, and communications structure; c. A description that explains each system function and how the function is achieved in the design; d. Descriptions of the functional and physical interfaces between subsystems and components; e. 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; f. Communications (network) software; g. Interfaces among internal components and interfaces with external systems. For components that interface with other components for which multiple products may be used, the manufacturers SHALL identify file specifications, data objects, or other means used for information exchange, and the public standard used for such file specifications, data objects, or other means; and h. Listings of 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. | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | SA-5<br>INFORMATION SYSTEM DOCUMENTATION<br>Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.<br>Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed. | N/A | | 1 | 1 | | 1 | | | 1 | | | | N/C |
| 9.2.3.2 Identify software and firmware by origin | The system description SHALL include the identification of all software and firmware items, indicating items that were: a. Written in-house; b. Written by a subcontractor; c. Procured as COTS; and d. Procured and modified, including descriptions of the modifications to the software or firmware and to the default configuration options. | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | SA-5<br>INFORMATION SYSTEM DOCUMENTATION<br>Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.<br>Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed. | N/A | | 1 | 1 | | 1 | | | 1 | | | | N/C |
| 9.2.3.3 Traceability of procured software | The system description SHALL include a declaration that procured software items were obtained directly from the manufacturer or from a licensed dealer or distributor. | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | None | None | None | None | None | None | None | | | 1 | 1 | 1 | | | 1 | | | | 1 | | N/C |
| 9.2.4.1 User documentation system performance | Manufacturers SHALL provide system performance information including: a. Device capacities and limits that were stated in the implementation statement; b. 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; c. Quality attributes such as reliability, maintainability, availability, usability, and portability; d. Provisions for safety, security, voter privacy, ballot secrecy, and continuity of operations; and e. Design constraints, applicable standards, and compatibility requirements. | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | SA-4 | Acquisitions | 12.1.1 | 3.1.6; 3.1.7; 3.1.10; 3.1.11; 3.1.12 | --- | DCAS-1; DCDS-1; DCIT-1; DCMC-1 | DCID: B.2.a; C.2.a; Manual:; 9.B.4 | SA-4 ACQUISITIONS<br>Control: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.<br>Supplemental Guidance:<br>Solicitation Documents<br>The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST Special Publication 800-36 provides guidance on the selection of information security products. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.<br>Information System Documentation<br>The solicitation documents include requirements for appropriate information system documentation. The documentation addresses user and systems administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the FIPS 199 security category for the information system.<br>Use of Tested, Evaluated, and Validated Products<br>NIST Special Publication 800-23 provides guidance on the acquisition and use of tested/evaluated information technology products.<br>Configuration Settings and Implementation Guidance<br>The information system required documentation includes security configuration settings and security implementation guidance. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST Special Publication 800-70 provides guidance on configuration settings for information technology products | N/A | | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 9.3.1 User Documentation, System Functionality Description | Manufacturers SHALL provide a listing of the system's functional processing capabilities, encompassing capabilities required by the UOCAVA Pilot Program Testing Requirements, and any additional capabilities provided by the system, with a description of each capability. a. Manufacturers SHALL explain, in a manner that is understandable to users, the capabilities of the system declared in the implementation statement; b. Additional capabilities (extensions) SHALL be clearly indicated; c. Required capabilities that may be bypassed or deactivated during installation or operation by the user SHALL be clearly indicated; d. Additional capabilities that function only when activated during installation or operation by the user SHALL be clearly indicated; and e. Additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user SHALL be clearly indicated. | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | SA-5<br>INFORMATION SYSTEM DOCUMENTATION<br>Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.<br>Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed. | N/A | 1 | 1 | | | 1 | | | 1 | | | | N/C |
| 9.4.1.1 Access control implementation, configuration, and management | Manufacturers SHALL provide user documentation containing guidelines and usage instructions on implementing, configuring, and managing access control capabilities. | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | AC-1 | Access Control Policy and Procedures | 11.1.1; 11.4.1; 15.1.1 | 15.; 16. | --- | ECAN-1; ECPA-1; PRAS-1; DCAR-1 | 2.B.4.e(5); 4.B.1.a(1)(b) | AC-1<br>ACCESS CONTROL POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.<br>Supplemental Guidance: The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. | N/A | 1 | 1 | | | | 1 | | 1 | | | | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 9.4.1.2 Access control policy | Manufacturers SHALL provide, within the user documentation, the access control policy under which the system was designed to operate. | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | AC-1 | Access Control Policy and Procedures | 11.1.1; 11.4.1; 15.1.1 | 15.; 16. | --- | ECAN-1; ECPA-1; PRAS-1; DCAR-1 | 2.B.4.e(5); 4.B.1.a(1)(b) | AC-1<br>ACCESS CONTROL POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.<br>Supplemental Guidance: The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. | N/A | 1 | 1 | | | | 1 | | 1 | | | | N/C |
| 9.4.1.3 Privileged account | Manufacturers SHALL disclose and document information on all privileged accounts included on the system. | Inspection | Manufacturer | Loss of Integrity, Availability and/or Confidentiality | I=INSPECTION | AC-2 | Account Management | 6.2.2; 6.2.3; 8.3.3; 11.2.1; 11.2.2; 11.2.4; 11.7.2 | 6.1.8; 15.1.1; 15.1.4; 15.1.5; 15.1.8; 15.2.2; 16.1.3; 16.1.5; 16.2.12 | AC-2.1; AC-2.2; AC-3.2; SP-4.1 | IAAC-1 | 4.B.2.a(3) | AC-2<br>ACCOUNT MANAGEMENT<br>Control: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [Assignment: organization-defined frequency, at least annually].<br>Supplemental Guidance: Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know/need-to-share changes. | N/A | 1 | 1 | 1 | | | | 1 | | | | | N/C |
| 9.4.2.1 System event logging | Manufacturers SHALL provide user documentation that describes system event logging capabilities and usage. | Inspection | Manufacturer | Loss of Integrity and/or Confidentiality | I=INSPECTION | AU-2 & AU-3 | Auditable Events | 10.10.1 | 17.1.1; 17.1.2; 17.1.4 | --- | ECAR-3 | 4.B.2.a(4)(d) | AU-2<br>AUDITABLE EVENTS<br>Control: The information system generates audit records for the following events: [Assignment: organization-defined auditable events].<br>Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management. | N/A | | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 9.4.2.2 Log format | Manufacturers SHALL provide fully documented log format information. | Inspection | Manufacturer | Provides forensic capability in the event of data loss. Provides troubleshooting abilitieis. | I=INSPECTION | AU-3 | Content of Audit Records | 10.10.1; 10.10.4 | 17.1.1 | --- | ECAR-1; ECAR-2; ECAR-3; ECLC-1 | 4.B.2.a(4)(a); 4.B.2.a(5)(a) | AU-3<br>CONTENT OF AUDIT RECORDS<br>Control: The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.<br>Supplemental Guidance: Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. NIST Special Publication 800-92 provides guidance on computer security log management. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 9.4.3.1 Ballot decryption process | Manufacturers SHALL provide documentation on the proper procedures for the authorized entity to implement ballot decryption while maintaining the security and privacy of the data. | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | CM-1 | Configuration Management Policy and Procedures | 12.4.1; 12.5.1; 15.1.1 | --- | --- | DCCB-1; DCPR-1; DCAR-1; E3.3.8 | DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5) | CM-1<br>CONFIGURATION MANAGEMENT POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.<br>Supplemental Guidance: The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. | N/A | 1 | 1 | | | | | 1 | 1 | | | | N/C |
| 9.4.3.2 Ballot decryption key reconstruction | Manufacturers SHALL provide documentation describing the proper procedure for the authorized entity to reconstruct the election private key to decrypt the ballots. | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | IA-5 | Authenticator Management | 11.5.2; 11.5.3 | 15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3 | AC-3.2 | IAKM-1; IATS-1 | 4.B.2.a(7); 4.B.3.a(11) | IA-5<br>AUTHENTICATOR MANAGEMENT<br>Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically. | N/A | | 1 | | | | | 1 | 1 | | | | N/C |
| 9.4.3.3 Ballot decryption key destruction | Manufacturers SHALL document when any cryptographic keys created or used by the system may be destroyed. The documentation SHALL describe how to delete keys securely and irreversibly at the appropriate time. | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | SC-12 | Cryptographic Key Establishment and Management | 12.3.1; 12.3.2 | 16.1.7; 16.1.8 | --- | IAKM-1 | 1.G | SC-12<br>CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT<br>Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.<br>Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 9.4.4.1 Physical security | Manufacturers SHALL provide user documentation explaining the implementation of all physical security controls for the system, including procedures necessary for effective use of countermeasures. | Inspection | Manufacturer | Loss of Confidentiality, Integrity and/or availability. | I=INSPECTION | PE-1 | Physical and Environmental Protection Policy and Procedures | 15.1.1 | 7 | PETN-1; DCAR-1 | DCID: B.2.a; Manual: 2.B.4.e(5) | 8.D | PE-1<br>PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.<br>Supplemental Guidance: The physical and environmental protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. | | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 9.4.5.1 Ballot count and vote total auditing | The system's user documentation SHALL fully specify a secure, transparent, workable and accurate process for producing all records necessary to verify the accuracy of the electronic tabulation result. | Inspection | Manufacturer | Loss of data Integrity | I=INSPECTION | None | None | None | None | None | None | None | None | None | 1 | 1 | 1 | | | | 1 | | | 1 | | N/C |
| 9.5.1.1 Software list | Manufacturers SHALL provide a list of all software to be installed on the programmed devices of the system and installation software used to install the software. | Inspection | Manufacturer | Loss of system Integrity and availability. Provides disaster recovery capability. | I=INSPECTION | CM-8 | Information System Component Inventory | 7.1.1; 15.1.2 | 1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4 | CC-2.3; CC-3.1; SS-1.2 | DCHW-1; DCSW-1 | 2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6) | CM-8<br>INFORMATION SYSTEM COMPONENT INVENTORY<br>Control: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.<br>Supplemental Guidance: The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system. Related security controls: CM-2, CM-6. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 9.5.1.2 Software information | Manufacturers SHALL provide at a minimum, the following information for each piece of software to be installed or used to install software on programmed devices of the system: software product name, software version number, software manufacturer name, software manufacturer contact information, type of software (application logic, border logic, third party logic, COTS software, or installation software), list of software documentation, component identifier(s) (such filename(s)) of the software, type of software component (executable code, source code, or data). | Inspection | Manufacturer | Loss of system Integrity and availability. Provides disaster recovery capability. | I=INSPECTION | CM-8 | Information System Component Inventory | 7.1.1; 15.1.2 | 1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4 | CC-2.3; CC-3.1; SS-1.2 | DCHW-1; DCSW-1 | 2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6) | CM-8<br>INFORMATION SYSTEM COMPONENT INVENTORY<br>Control: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.<br>Supplemental Guidance: The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system. Related security controls: CM-2, CM-6. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 9.5.1.3 Software location information | Manufacturers SHALL provide 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 system. | Inspection | Manufacturer | Loss of system Integrity and availability. Provides disaster recovery capability. | I=INSPECTION | CM-8 | Information System Component Inventory | 7.1.1; 15.1.2 | 1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4 | CC-2.3; CC-3.1; SS-1.2 | DCHW-1; DCSW-1 | 2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6) | CM-8<br>INFORMATION SYSTEM COMPONENT INVENTORY<br>Control: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.<br>Supplemental Guidance: The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system. Related security controls: CM-2, CM-6. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 9.5.1.4 Election specific software identification | Manufacturers SHALL identify election specific software in the user documentation. | Inspection | Manufacturer | No securiyt impact | I=INSPECTION | None | None | None | None | None | None | None | None | Special denotation within the supplied documentation | | 1 | | | | 1 | | | | 1 | | N/C |
| 9.5.1.5 Installation software and hardware | Manufacturers SHALL provide a list of software and hardware required to install software on programmed devices of the system in the user documentation. | Inspection | Manufacturer | System integrity and availability | I=INSPECTION | CM-8 | Information System Component Inventory | 7.1.1; 15.1.2 | 1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4 | CC-2.3; CC-3.1; SS-1.2 | DCHW-1; DCSW-1 | 2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6) | Security Design and Configuration Availability<br>DCSW-1 SW Baseline<br>A current and comprehensive baseline inventory of all software (SW) (to include manufacturer, type, and version and installation manuals and procedures) required to support DoD information system operations is maintained by the CCB and as part of the C&A documentation. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original. | N/A | | 1 | 1 | | 1 | | | 1 | | | | N/C |
| 9.5.1.6 Software installation procedure | Manufacturers SHALL document the software installation procedures used to install software on programmed devices of the system. | Inspection | Manufacturer | System integrity and availability | I=INSPECTION | CM-8 | Information System Component Inventory | 7.1.1; 15.1.2 | 1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4 | CC-2.3; CC-3.1; SS-1.2 | DCHW-1; DCSW-1 | 2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6) | Security Design and Configuration Availability<br>DCSW-1 SW Baseline<br>A current and comprehensive baseline inventory of all software (SW) (to include manufacturer, type, and version and installation manuals and procedures) required to support DoD information system operations is maintained by the CCB and as part of the C&A documentation. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original. | N/A | | 1 | 1 | | 1 | | | 1 | | | | N/C |
| 9.5.1.7 Compiler installation prohibited | The software installation procedures used to install software on programmed devices of the system SHALL specify that no compilers SHALL be installed on the programmed device. | Inspection | Manufacturer | No direct security implication of this addition to the documentation. However, installation of compilers could impact confidentiality, availablity and integrity. | I=INSPECTION | None | None | None | None | None | None | None | End user software is prohibited. However, no specific guidance on compilers within the referenced documetation. | None | 1 | 1 | 1 | | | 1 | | | | 1 | | N/C |
| 9.5.1.8 Procurement of system software | The software installation procedures SHALL specify that system software SHALL be obtained from the VSTL or approved distribution repositories. | Inspection | Manufacturer | Approved software use only. Potential loss of availability, integrity and confidentiality. | I=INSPECTION | SA-1 | System and Services Acquisition Policy and Procedures | 12.1; 15.1.1 | 3 | --- | DCAR-1 | DCID: B.2.a; Manual: 2.B.4.e(5) | No direct security implication of this addition to the documentation. However, installation of compilers could impact confidentiality, availablity and integrity. | None | | 1 | 1 | | 1 | | | | | | | N/C |
| 9.5.1.9 Erasable storage media preparation | The software installation procedures SHALL specify how previously stored information on erasable storage media is removed before installing software on the media. | Inspection | Manufacturer | Medium: Loss of Integrity | I=INSPECTION | MP-1<br>MP-6 | Media Protection Policy and Procedures | 10.1.1; 10.7; 15.1.1; 15.1.3 | 8.2 | --- | PESP-1; DCAR-1 | DCID: B.2.a Manual:; 2.B.6.c(7); 8.B.2 | MP-1<br>MEDIA PROTECTION POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls. | N/A | 1 | 1 | | | 1 | | | 1 | | | | Recommend that DoD guidance for erasable media be used. |
| 9.5.1.10 Installation media unalterable storage media | The software installation procedures SHALL specify that unalterable storage media SHALL be used to install software on programmed devices of the system. | Inspection | Manufacturer | Medium: Loss of Integrity | I=INSPECTION | MP-1 | Media Protection Policy and Procedures | 10.1.1; 10.7; 15.1.1; 15.1.3 | 8.2 | --- | PESP-1; DCAR-1 | DCID: B.2.a Manual:; 2.B.6.c(7); 8.B.2 | MP-1<br>MEDIA PROTECTION POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 9.5.1.11 Software hardening | Manufacturers SHALL provide documentation that describes the hardening procedures for the system. | Inspection | Manufacturer | High: Loss of Integrity, Availability, and/or Confidentiality | I=INSPECTION | SA-11 | Developer Security Testing | 12.5.1; 12.5.2 | 3.2.1;<br>3.2.2;<br>10.2.5;<br>12.1.5 | SS-3.1; CC-2.1 | E3.4.4 | 4.B.4.b(4) | NIST SP800-137: A security configuration checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration, is essentially a document that contains instructions or procedures for configuring an information technology (IT) product to a baseline level of security.<br>SA-11<br>DEVELOPER SECURITY TESTING<br>Control: The organization requires that information system developers create a security test and evaluation plan, implement the plan, and document the results.<br>Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security certification and accreditation process for the delivered information system.<br>Related security controls: CA-2, CA-4. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 9.6.1 Setup inspection process | Manufacturers SHALL provide a setup inspection process that the system was designed to support. | Inspection | Manufacturer | High: Loss of Integrity, Availability, and/or Confidentiality | I=INSPECTION | None | None | None | None | None | None | None | DCID 6/3 Requirement:<br>4.B.2.b(7)(b) A test plan and procedures shall be developed and include:<br>4.B.2.b(7)(b)(1) A detailed description of the manner in which the system's Security Support Structure meets the technical requirements for the Protection Levels and Levels-of-Concern for integrity and<br>availability.<br>4.B.2.b(7)(b)(2) A detailed description of the assurances that have been implemented, and how this implementation will be verified.<br>4.B.2.b(7)(b)(3) An outline of the inspection and test procedures used to verify this compliance. | N/A | 1 | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 9.6.1.1 Minimum properties included in a setup inspection process | A setup inspection process SHALL, at a minimum, include the inspection of system software, storage locations that hold election information that changes during an election, and execution of logic and accuracy testing related to readiness for use in an election. | Inspection | Manufacturer | High: Loss of Integrity, Availability, and/or Confidentiality | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3;<br>3.2.4;<br>3.2.8;<br>12.1.1;<br>12.1.2;<br>12.1.3;<br>12.1.6;<br>12.1.7 | CC-2.1 | DCCS-1;<br>DCHW-1;<br>DCID-1; DCSD-1; DCSW-1;<br>ECND-1;<br>DCFA-1 | 4.B.2.b(2);<br>4.B.2.b(3);<br>4.B.4.b(4);<br>9.C.3 | SA-5<br>INFORMATION SYSTEM DOCUMENTATION<br>Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.<br>Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 9.6.1.2 Setup inspection record generation | The setup inspection process SHALL describe the records that result from performing the setup inspection process. | Inspection | Manufacturer | | I=INSPECTION | None | None | None | None | None | None | None | NIST SP800-100 States: In addition, developing a security requirements checklist based on the security requirements specified for the system during the conceptual, design, and implementation phases of the SDLC can be used to provide a 360-degree inspection of the system. | | 1 | 1 | 1 | | | 1 | | | | 1 | | N/C |
| 9.6.1.3 Installed software identification procedure | Manufacturers SHALL provide the procedures to identify all software installed on programmed devices. | Inspection | Manufacturer | High: Loss of Integrity, Availability, and/or Confidentiality | I=INSPECTION | SI-1 | System and Information Integrity Policy and Procedures | 15.1.1 | 11 | --- | DCAR-1 | DCID: B.2.a; Manual: 2.B.4.e(5); 5.B.1.b(1) 5.B.2.a(5)(a)(1) | SI-1<br>SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.<br>Supplemental Guidance: The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 9.6.1.4 Software integrity verification procedure | Manufacturers SHALL describe the procedures to verify the integrity of software installed on programmed devices of system. | Inspection | Manufacturer | High: Loss of Integrity, Availability, and/or Confidentiality | I=INSPECTION | SI-1 | System and Information Integrity Policy and Procedures | 15.1.1 | 11 | --- | DCAR-1 | DCID: B.2.a; Manual: 2.B.4.e(5); 5.B.1.b(1) 5.B.2.a(5)(a)(1) | SI-1<br>SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.<br>Supplemental Guidance: The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. | N/A | | 1 | | | | | 1 | 1 | | | | N/C |
| 9.6.1.5 Election information value | Manufacturers SHALL provide the values of system storage locations that hold election information that changes during the election, except for the values set to conduct a specific election. | Inspection | Manufacturer | Medium: Loss of Integrity, Availability and/or confidentiality | I=INSPECTION | MP-4 | Media Storage | 10.7.1; 10.7.2; 10.7.3; 10.7.4; 15.1.3 | 7.1.4;<br>8.2.1;<br>8.2.2;<br>8.2.9;<br>10.1.2 | AC-3.1 | PESS-1 | 2.B.9.b(4);<br>4.B.1.a(7) | MP-4<br>MEDIA STORAGE<br>Control: The organization physically controls and securely stores information system media within controlled areas. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 9.6.1.6 Maximum values of election information storage locations | Manufacturers SHALL provide the maximum values for the storage locations where election information is stored. | Inspection | Manufacturer | Medium: Loss of Integrity, Availability and/or confidentiality | I=INSPECTION | MP-4 | Media Storage | 10.7.1; 10.7.2; 10.7.3; 10.7.4; 15.1.3 | 7.1.4;<br>8.2.1;<br>8.2.2;<br>8.2.9;<br>10.1.2 | AC-3.1 | PESS-1 | 2.B.9.b(4);<br>4.B.1.a(7) | MP-4<br>MEDIA STORAGE<br>Control: The organization physically controls and securely stores information system media within controlled areas. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 9.6.1.7 Backup power operational range | Manufacturers SHALL provide the nominal operational range for the backup power sources of the voting system. | Inspection | Manufacturer | Medium: Loss of Integrity, Availability and/or confidentiality | I=INSPECTION | PE-11 | Emergency Power | 9.2.2 | 7.1.18 | SC-2.2 | COPS-1;<br>COPS-2;<br>COPS-3 | 6.B.2.a(6);<br>6.B.2.a(7) | PE-11<br>EMERGENCY POWER<br>Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.<br>Supplemental Guidance: None. | N/A | 1 | 1 | 1 | | 1 | | | 1 | | | | N/C |
| 9.6.1.8 Backup power inspection procedure | Manufacturers SHALL provide the procedures to inspect the remaining charge of the backup power sources of the voting system. | Inspection | Manufacturer | Medium: Loss of Integrity and/or Availability | I=INSPECTION | PE-1 | Physical and Environmental Protection Policy and Procedures | 15.1.1 | 7 | PETN-1; DCAR-1 | DCID: B.2.a; Manual: 2.B.4.e(5) | 8.D | PE-1<br>PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 9.6.1.9 Cabling connectivity inspection procedure | Manufacturers SHALL provide the procedures to inspect the connectivity of the cabling attached to the vote capture device. | Inspection | Manufacturer | Medium: Loss of Integrity and/or Availability | I=INSPECTION | PE-1 | Physical and Environmental Protection Policy and Procedures | 15.1.1 | 7 | PETN-1; DCAR-1 | DCID: B.2.a; Manual: 2.B.4.e(5) | 8.D | PE-1<br>PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. | N/A | | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 9.6.1.10 Communications operational status inspection procedure | Manufacturers SHALL provide the procedures to inspect the operational status of the communications capabilities of the vote capture device. | Inspection | Manufacturer | Medium: Loss of Integrity and/or Availability | I=INSPECTION | PE-1 | Physical and Environmental Protection Policy and Procedures | 15.1.1 | 7 | PETN-1; DCAR-1 | DCID: B.2.a; Manual: 2.B.4.e(5) | 8.D | PE-1<br>PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. | N/A | | 1 | 1 | | | | 1 | 1 | | | | N/C |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 9.6.1.11 Communications on/off status inspection procedure | Manufacturers SHALL provide the procedures to inspect the on/off status of the communications capabilities of the vote capture device. | Inspection | Manufacturer | Medium: Loss of Integrity and/or Availability | I=INSPECTION | PE-4 | Access Control for Transmission Medium | 9.2.3 | 7.2.2; 16.2.9 | --- | --- | 8.D.2; 4.B.1.a(8) | PE-4<br>ACCESS CONTROL FOR TRANSMISSION MEDIUM<br>Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.<br>Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. | N/A | | 1 | 1 | | | | 1 | 1 | | | | N/C |
| 9.6.1.12 Consumables quantity of vote capture device | Manufacturers SHALL provide a list of consumables associated with the vote capture device, including estimated number of usages per quantity of consumable. | Inspection | Manufacturer | No known security risk. | I=INSPECTION | None | None | None | None | None | None | None | No specific IA Control referenced. | None | | | 1 | | 1 | | | | | 1 | | N/C |
| 9.6.1.13 Consumable inspection procedure | Manufacturers SHALL provide the procedures to inspect the remaining amount of each consumable of the vote capture device. | Inspection | Manufacturer | No known security risk. | I=INSPECTION | None | None | None | None | None | None | None | No specific IA Control referenced. | None | | | 1 | | 1 | | | | | 1 | | N/C |
| 9.6.1.14 Calibration of vote capture device components nominal range | Manufacturers SHALL provide a list of components associated with the vote capture devices that require calibration and the nominal operating ranges for each component. | Inspection | Manufacturer | No known security risk. | I=INSPECTION | None | None | None | None | None | None | None | No specific IA Control referenced. | None | | 1 | | | | 1 | | | | 1 | | N/C |
| 9.6.1.15 Calibration of vote capture device components inspection procedure | Manufacturers SHALL provide the procedures to inspect the calibration of each component. | Inspection | Manufacturer | No known security risk. | I=INSPECTION | None | None | None | None | None | None | None | No specific IA Control referenced. | None | | 1 | | | | 1 | | | | 1 | | N/C |
| 9.6.1.16 Calibration of vote capture device components adjustment procedure | Manufacturers SHALL provide the procedures to adjust the calibration of each component. | Inspection | Manufacturer | Calibration could impact system Integrity | I=INSPECTION | CM-1 | Configuration Management Policy and Procedures | 12.4.1; 12.5.1; 15.1.1 | --- | --- | DCCB-1; DCPR-1; DCAR-1; E3.3.8 | DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5) | CM-1<br>CONFIGURATION MANAGEMENT POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. | N/A | | 1 | 1 | | | 1 | | | | | | N/C |
| 9.6.1.17 Checklist of properties to be inspected | Manufacturers SHALL provide a checklist of other properties of the system to be inspected. | Inspection | Manufacturer | Checklists are important, but may not have direct impact on security. | I=INSPECTION | CM-1 | Configuration Management Policy and Procedures | 12.4.1; 12.5.1; 15.1.1 | --- | --- | DCCB-1; DCPR-1; DCAR-1; E3.3.8 | DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5) | CM-1<br>CONFIGURATION MANAGEMENT POLICY AND PROCEDURES<br>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. | N/A | | 1 | 1 | | | 1 | | | | | | N/C |
| 9.7.1.1 System operations manual | The system operations manual SHALL provide all information necessary for system set up and use by all personnel who administer and operate the system at the state and/or local election offices and at the kiosk locations, with regard to all system functions and operations identified in Section 9.3 System Functionality Description. | Inspection | Manufacturer | High: Loss of Integrity, Availability, and/or Confidentiality | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | SA-5<br>INFORMATION SYSTEM DOCUMENTATION<br>Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.<br>Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 9.7.1.2 Support training | The system operations manual SHALL contain all information that is required for the preparation of detailed system operating procedures and for the training of administrators, state and/or local election officials, election judges, and kiosk workers. | Inspection | Manufacturer | High: Loss of Integrity, Availability, and/or Confidentiality | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | Nothing found about training the operators! | | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 9.7.2.1 Functions | Manufacturers SHALL provide a summary of system operating functions to permit understanding of the system's capabilities and constraints. | Inspection | Manufacturer | High: Loss of Integrity, Availability, and/or Confidentiality | I=INSPECTION | SA-5 | Information System Documentation | 10.7.4 | 3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7 | CC-2.1 | DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1 | 4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3 | DCSQ-1 Software Quality<br>Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives. | N/A | 1 | 1 | 1 | | | 1 | | 1 | | | | N/C |
| 9.7.2.2 Roles | The roles of operating personnel SHALL be identified and related to the functions of the system. | Inspection | Manufacturer | High: Loss of Integrity, Availability, and/or Confidentiality | I=INSPECTION | AC-2 | Account Management | 6.2.2; 6.2.3; 8.3.3; 11.2.1; 11.2.2; 11.2.4; 11.7.2 | 6.1.8; 15.1.1; 15.1.4; 15.1.5; 15.1.8; 15.2.2; 16.1.3; 16.1.5; 16.2.12 | AC-2.1; AC-2.2; AC-3.2; SP-4.1 | IAAC-1 | 4.B.2.a(3) | DCPR-1 CM Process<br>A configuration management (CM) process is implemented that includes requirements for:<br>(1) Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation;<br>(2) A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include inter-connections to other DoD information systems;<br>(3) A testing process to verify proposed configuration changes prior to implementation in the operational environment; and<br>(4) A verification process to provide additional assurance that the CM process is working effective | N/A | | | 1 | | 1 | | | 1 | | | | N/C |
| | | | | | | | | | | | | | | Totals | **150** | **246** | **191** | **0** | **41** | **130** | **88** | **186** | **0** | **28** | **58** | **15** |

| NIST Security Objective | Potential Impact | | |
|---|---|---|---|
| | **Low** | **Medium** | **High** |
| **Confidentialy**<br>Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.<br>[44 U.S.C., SEC. 3542] | The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or |
| **Integrity**<br>Guarding against improper information modification or destruction, and includes ensuring information non repudiation and authenticity.<br>[44 U.S.C., SEC. 3542] | The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |
| **Availability**<br>Ensuring timely and reliable access to and use of information. Basic Testing A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object.<br>[44 U.S.C., SEC. 3542] | The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |