Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-14	SBE should ensure that appropriate authority, responsibility and accountability are defined to accomplish the administration of the voting system, and that an appropriate organizational structure is established to effectively carry out program responsibilities.	M	Registration and Election Laws of Maryland and The Code of Maryland Regulations define the authority, responsibility and accountability to accomplish the administration of the voting system and establish the organizational structure.		
M-15	Key duties and responsibilities in authorizing, processing, recording, and reviewing voting transactions and processes should be separated among individuals.	M	Registration and Election Laws of Maryland, The Code of Maryland Regulations, Election Judge manuals and the Procedures for Official Canvass, Verification and Post-Election Audit describe and define and separates the key duties and responsibilities in authorizing, processing, recording, and reviewing voting transactions.		
M-16	SBE should exercise appropriate oversight to ensure individuals do not exceed or abuse their assigned authorities.	M	Registration and Election Laws of Maryland, The Code of Maryland Regulations, and Election Judge manuals provide appropriate oversight to ensure individuals do not exceed or abuse their assigned authorities.		
M-17	Access to resources and records should be limited to authorized individuals, and accountability for the custody and use of resources should be assigned and maintained.	M	Registration and Election Laws of Maryland, The Code of Maryland Regulations, and Election Judge manuals define who is authorized to access resources and records. Challengers and Watchers serve as an additional check for this requirement.		
M-18	Votes should be promptly recorded, properly classified	M	Votes are promptly recorded, classified and accounted for as described in the		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	recorded, properly classified and accounted for in order to prepare timely reporting, auditing and other reports.		and accounted for as described in the Registration and Election Laws of Maryland, COMAR, Election Judge manuals, and the Procedures for Official Canvass, Verification and Post-Election Audit.		
M-19	The documentation for transactions, management controls, and other significant events must be clear and readily available for examination.	P	If documentation for transactions, management controls, and other significant events is not clear and readily available for examination, then the security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised. The State of Maryland has documentation that is clear, but not readily available. **Likelihood: LOW** The State of Maryland controls impede this vulnerability from being exercised. However, the lack of consolidated, available documentation may result in error by election officials and technicians. **Impact: LOW** If the vulnerability is exploited the validity and integrity of the election process may be compromised.	LOW	In the future SBE should consolidate procedures and distribute them to all of the LBEs in order to achieve standardization across the state.
M-20	SBE should promptly evaluate and determine proper actions in response to known deficiencies,	M	This risk assessment and the Risks, Issues, Systems Incidents and Changes (RISC) Plan enable SBE to evaluate and		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	reported audit and other findings, and related recommendations.		determine proper actions in response to known deficiencies and other findings and recommendations.		
M-21	Managers should continuously monitor and improve the effectiveness of security controls associated with the voting process.	M	SBE and LBEs continuously look for ways to improve the security controls of the voting process. The Change Control Process document enable managers to monitor and improve the effectiveness of security controls associated with the voting process. This risk assessment provides another tool to assist with this process.		
M-22	SBE and election officials should identify and report deficiencies, as this reflects positively on the agency's commitment to recognizing and addressing voting problems.	M	The Polling place evaluation process as stated in COMAR 33.07.03.04, Election Judge Manuals and the State of Maryland RISC database, ensure that deficiencies are identified and reported.		
M-23	SBE managers are responsible for taking timely and effective action to correct deficiencies, as appropriate.	M	The State of Maryland RISC Plan provides a framework for identifying and resolving issues and risks. It addresses all artifacts produced during the issue and risk management processes, including: □Risk and Issue descriptions □System Investigation Requests (SIR) □Change Requests (CR) and □Risk and Issue reports		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-24	The extent to which corrective actions are tracked by SBE should be commensurate with the severity of the deficiency.	M	The State of Maryland RISC plan provides the framework for identifying and resolving issues and risks. It addresses all artifacts produced during the issue and risk management processes, including: □Risk and Issue descriptions □System Investigation Requests (SIR) □Change Requests (CR) and □Risk and Issue reports		
M-25	Corrective action plans should be developed for all material weaknesses, and progress against plans should be periodically assessed and reported to SBE management.	M	The State of Maryland RISC plan provides the framework for identifying and resolving issues and risks. It addresses all artifacts produced during the issue and risk management processes, including: □Risk and Issue descriptions □System Investigation Requests (SIR) □Change Requests (CR) and □Risk and Issue reports		
M-26	The SBE security planning shall clearly delineate responsibilities and expected behavior of all individuals with access to the system.	M	Registration and Election Laws of Maryland, The Code of Maryland Regulations, Election Judge manuals and the Procedures for Official Canvass, Verification and Post-Election Audit delineate the responsibilities and		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			expected behavior of all individuals with access to the system.		
M-27	The SBE security planning shall include appropriate limits on interconnections to other systems.	M	Currently, the electronic voting system is not connected to any other system, with the exception of the SBE GEMS server. The SBE GEMS server is not used in the voting process. If there are plans to connect additional components of the voting system in the future, especially the DRE voting terminals, a thorough risk assessment will need to be conducted.		
M-28	The SBE security planning shall define service provision and restoration priorities.	M	The SBE Disaster Recovery and Incident Management Plan provides a plan of action with provision and restoration priorities.		
M-29	The SBE security planning shall be clear about the consequences of behavior not consistent with the rules.	M	Registration and Election Laws of Maryland, and The Code of Maryland Regulations describe the consequences of behavior not consistent with the rules.		
M-30	The SBE security planning shall ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system.	P	If the SBE security planning does not ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system, then the security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised. The SBE has training for all of the election judges, poll workers and technicians. However, this training does	MEDIUM	Training should be established for security awareness and technical security training to ensure that election judges, poll workers and technicians are aware of the rules of behavior and their responsibilities in protecting the organization's mission. This training should include information about threats, vulnerabilities and risks to the voting system.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			not adequately address security issues. **Likelihood: MEDIUM** Without security awareness training the election judges, poll workers and technicians may not be aware of their security responsibilities. **Impact: HIGH** If the vulnerability is exploited the validity and integrity of the election process may be compromised.		
M-31	The SBE security planning shall contain rules of the system and indicate that periodic refresher training shall be required for continued access to the system.	P	If the SBE security planning does not contain rules of the system and indicate that periodic refresher training shall be required for continued access to the system, then the security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised. The DESI contract with the SBE requires that designated election officials and staff receive training in the operation and management of the AccuVote-Touch Screen (AVTS), AccuVote-Optical Scan (AVOS) units, and Global Election Management System (GEMS) software. Many of the LBEs have developed their own training that is specific to their procedures and processes. However, this training does not adequately address	**MEDIUM**	Training should be established for security awareness and technical security training to ensure that election judges, poll workers and technicians are aware of the rules of behavior and their responsibilities in protecting the organization's mission. This training should include information about threats, vulnerabilities and risks to the voting system.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			security issues. **Likelihood: MEDIUM** Without security awareness training the election judges, poll workers and technicians may not be aware of their security responsibilities. **Impact: HIGH** If the vulnerability is exploited the validity and integrity of the election process may be compromised.		
M-32	The SBE's security planning for personnel controls shall require screening of individuals who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause.	P	If the SBE's security planning for personnel controls does not require screening of individuals who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause, then the security controls may be circumvented and the confidentiality, integrity, and availability of the system may be compromised. Personnel who are authorized to bypass technical and operational security controls do not currently go through a vetting process before being place into a position of trust. **Likelihood: LOW** SBE and LBE have implemented	**LOW**	Background investigations should be performed on senior election officials who have access to critical systems.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~controls to mitigate this risk including:~~ ~~□Two-person rule~~ ~~□Separation of duties~~ ~~□Least privilege~~ ~~□Confidentiality agreements~~ ~~**Impact: HIGH**~~ ~~Although the likelihood of an incident occurring at SBE is low, it could have significant impact on SBE's mission if exploited.~~		
~~M-33~~	~~The SBE's security planning for personnel controls screening shall occur prior to an individual being authorized to bypass controls and periodically thereafter.~~	~~**P**~~	~~If the SBE's security planning for personnel controls screening does not occur prior to an individual being authorized to bypass controls and periodically thereafter, then an individual may be granted inappropriate access and the confidentiality, integrity, and availability of the system may be compromised.~~ ~~Personnel who are authorized to bypass technical and operational security controls do not currently go through a vetting process before being place into a position of trust.~~ ~~**Likelihood: LOW**~~ ~~SBE and LBE have implemented~~	~~**LOW**~~	~~Background investigations should be performed on senior election officials who have access to critical systems before their initial access to systems is granted and periodically thereafter.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			~~controls to mitigate this risk including:~~ ~~□Two person rule~~ ~~□Separation of duties~~ ~~□Least privilege~~ ~~□Confidentiality agreements~~ ~~**Impact: HIGH**~~ ~~Although the likelihood of an incident occurring at SBE is low, it could have significant impact on SBE's mission if exploited.~~		
~~M-34~~	~~The SBE security planning shall ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats.~~	~~**M**~~	~~The SBE Disaster Recovery and Incident Management Plan provides a plan of action toward preparations and responses necessary to accomplish the following recovery goals after a disaster/incident occurs:~~ ~~□Determine, in a timely manner, whether the event is of sufficient magnitude and duration to cause unacceptable loss to SBE or LBE business operations~~ ~~□Ensure that appropriate advance measures have been taken to provide for the recovery of business operations in an acceptable period of time~~ ~~□Restore the affected resources or~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			provide a replacement for them within an acceptable period of time □Ensure appropriate internal and external communication is accomplished □Safeguard the public's confidence in elections.		
M-35	The SBE security planning Incident Response capability should assist SBE in pursuing appropriate legal action.	M	The SBE Disaster Recovery and Incident Management Plan along with the Registration and Election Laws of Maryland and The Code of Maryland Regulations assist the SBE in pursuing appropriate legal action.		
M-36	The SBE's security planning for continuity of support shall establish and periodically test the incident response capability to continue providing service within a system based upon the needs and priorities of the participants of the system.	M	The SBE Disaster Recovery and Incident Management Plan specifies review and update on an annual basis. The Incident Management Team Lead assembles the Incident Management Team every year to verify that the procedures are current.		
M-37	The SBE security planning shall ensure that cost-effective security products and techniques are appropriately used within the system.	U	If the SBE security planning does not ensure that cost-effective security products and techniques are appropriately used within the system, then funds may be spent for security controls that are not commensurate with the risk, funds may be depleted and not available for cost effective security controls, and the confidentiality, integrity, and availability of the system may be	MEDIUM	SBE should implement a process for ensuring that cost-effective security products and techniques are appropriately used in the system throughout the system lifecycle.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			compromised. SBE has not ensured that cost-effective security products and techniques are implemented. **Likelihood: MEDIUM** Without appropriately implemented, cost-effective security products and techniques, the system may not be adequately secured. **Impact: HIGH** If vulnerabilities are not exposed or fixed properly, the validity and integrity of the election process may be compromised.		
M-38	The SBE security planning shall require written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems.	P	If SBE security planning does not require written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems, then unplanned risks may be introduced to the system, the existing security controls may be circumvented and the confidentiality, integrity, and availability of the system may be compromised. Although the electronic voting system components other than the SBE GEMS server do not currently have any connections with other systems, SBE should have a process for requiring management approval prior for system interconnections.	LOW	Develop a process that requires management approval prior to system interconnections. This process should address the following: □Delineation of interconnection boundaries; □Responsibilities of interconnected agencies within established boundaries; □Roles, Responsibilities, and Points of contact for management officials in both organizations; □System Information protection;

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~interconnections.~~ ~~**Likelihood: LOW**~~ ~~There are currently no connections with other systems with the exception of the SBE GEMS server. Formal interconnection agreements provide both parties with minimum security requirements to limit system exposure against possible threats.~~ ~~**Impact: LOW**~~ ~~There are currently no connections with other systems other than the SBE GEMS server.~~		~~□Certification and Accreditation requirements;~~ ~~□Provisions for data sharing;~~ ~~□Emergency provision/notification procedures (especially for security incidents, disaster, termination or deployment of specific security controls, etc.);~~ ~~□Regular audits and security reviews, including provisions for penetration testing;~~ ~~□Minimum Availability and Service Level expectations;~~ ~~□Penalties and non-compliance.~~
~~M-39~~	~~Where system interconnection is authorized, controls shall be established and documented in SBE security planning that are consistent with the rules of the system and in accordance with DBM Standards.~~	~~**N/A**~~	~~The system does not have any authorized interconnections.~~		
~~M-40~~	~~SBE will review the security controls in each system when significant modifications are made to the system, or at least every three years, if no significant modifications are made.~~	~~**U**~~	~~If SBE does not review the security controls in each system when significant modifications are made to the system, or at least every three years, then unplanned risks may be introduced to the system, the existing security controls may be circumvented and the confidentiality, integrity, and availability~~	~~**HIGH**~~	~~System modifications should be reviewed through a formal implemented process to ensure that the changes do not negate any security controls that are currently in place.~~ ~~Results from this risk assessment will serve as a baseline to determine the~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			of the system may be compromised. SBE does not require a review of security controls when significant modifications are made. **Likelihood: HIGH** Since there is not a formal implemented process to review security controls, SBE cannot ensure that the controls are effective. **Impact: HIGH** Since SBE cannot ensure that the controls are effectivethe impact if this vulnerability were exploited, could be significant.		effectiveness of existing security controls and provide recommendations. Continue the risk assessment process at least every three years or whenever major changes occur throughout all phases of the system's life cycle.
M-41	SBE should also employ network security, including encryption for data in transit and protection for data at rest.	U	If SBE does not employ network security, including encryption for data in transit and protection for data at rest, then the confidentiality, integrity, and availability of the data may be compromised. SBE does not employ cryptography for data in transit. Cryptography would greatly reduce the chance of data being viewed by unauthorized sources if it were intercepted during transmission. **Likelihood: HIGH** Although the data is transmitted over a private point-to-point network, no cryptography is used to ensure the	**HIGH**	Implement cryptographic protocols for the data while it is transit such as hardware link-layer encryption (encrypting modems using 3DES or better encryption) or application-layer encryption (Secure Sockets Layer [SSL], Transport Layer Security [TLS], etc.).

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			integrity and confidentiality of the data being passed. Impact: HIGH A malicious user could intercept the data and read, modify or copy it during transmission.		
M-42	SBE security planning should concentrate the coordination of incident handling into one effort, thereby eliminating duplication of effort.	M	The SBE Disaster Recovery and Incident Management Plan does concentrate the coordination of incident handling efforts and describes the recommended recovery organizations of the SBE and the LBE. It identifies the roles and responsibilities of each team from the point of initial damage assessment until the actual execution of recovery activities.		
M-43	The SBE security planning incident handling requires not only the capability to react to incidents, but the resources to alert and disseminate the information to the appropriate personnel.	M	The SBE Disaster Recovery and Incident Management Plan outlines communication procedures that ensure the appropriate management and recovery team personnel have accurate and timely information.		
M-44	The designated Computer Security Program Manager (and support staff) should direct the organization's day-to-day management of its computer security program.	U	If the designated Computer Security Program Manager and support staff do not direct the organization's day-to-day management of the computer security program, then the security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be	LOW	Formally designate a Computer Security Program Manager to ensure that security issues are addressed and adhere to Maryland Security Policy and Standards.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~compromised.~~ ~~The SBE CIO directs the day-to-day IT operations of the organization, but there is no designated Computer Security Program Manager.~~ ~~**Likelihood: LOW**~~ ~~The security function is being performed by multiple individuals; therefore there is a relatively low likelihood of an attacker exploiting this vulnerability.~~ ~~**Impact: HIGH**~~ ~~The lack of a dedicated individual with accountability for the computer security program may result in security concerns not being addressed.~~		
~~M-45~~	~~Security plans should reflect input from various individuals with responsibilities concerning the system, including functional "end users," Information Owners, the System Administrator, and the Computer Security Program Manager.~~	~~M~~	~~The Polling place evaluation process, Election Judge Manuals and the SBE RISC Plan reflect input from various individuals regarding the system.~~		
~~M-46~~	~~SBE should have a policy on the security planning process.~~	~~M~~	~~DBM Security Policy and Standards covers the security planning process.~~		
~~M-47~~	~~Procedures should be in place outlining who reviews the System Security plans and~~	~~M~~	~~The SBE Disaster Recovery and Incident Management Plan describes a collaborative approach to project risk~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	follows up on planned controls.		management with state and county team members.		
M-48	Organizational policy should define who will provide the independent advice to the system security planning.	M	The State of Maryland has organizational policy for providing independent advice to the system security planning.		
M-49	Individuals providing advice to the system security planning should have adequate knowledge or experience to ensure the plan contains appropriate information and meets organizational security policy and standards.	M	The State of Maryland has contracted with individuals that have knowledge and experience to ensure the plan contains appropriate information and meets organizational security policy and standards.		
M-50	All system security plans, at a minimum, should be marked, handled, and controlled to the level of sensitivity determined by SBE policy.	M	DBM Security Policy and Standards requires security plans to be marked, handled, and controlled to the level of sensitivity commensurate with the risk.		
M-51	All System security plans should be dated for ease of tracking modifications and approvals.	M	All State of Maryland policies, plans and procedures are dated.		
M-52	The security plan should indicate the system's operational status (operational, under development, and /or undergoing a major modification), and if more than one status is selected, it should list which part of the system is	N/A	SBE does not have a security plan in place for this system. This resultant risk is addressed in requirement M-114.		

Number	~~Baseline Security Requirements~~	M/P/U /NA	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~covered under each status.~~				
~~M-53~~	~~The system security planning should present a brief description of the function or purpose of the system and the information processed.~~	~~M~~	~~Vendor supplied documentation as well as COMAR provides descriptions and function of the system.~~		
~~M-54~~	~~The system security planning should list all applications supported by the general support system.~~	~~M~~	~~Vendor supplied documentation as well as COMAR provides listings of applications for the system.~~		
~~M-55~~	~~The system security planning should describe the processing flow of the application from system input to system output.~~	~~M~~	~~SBE has process workflows for the electronic voting system detailing system input and output.~~		
~~M-56~~	~~The system security planning should list user organizations (internal & external) and type of data and processing provided.~~	~~M~~	~~Each LBE has detailed organizational lists, type of data and processing for all of the voting precincts located within their jurisdiction.~~		
~~M-57~~	~~The system security planning should provide a general description of the technical system, and include any environmental or technical factors that raise special security concerns.~~	~~M~~	~~Vendor supplied documentation as well as the COMAR provides general technical descriptions and environmental factors of the system.~~		
~~M-58~~	~~The system security planning should describe the primary computing platform(s) used and a description of the principal system components, including hardware, software, and~~	~~M~~	~~Vendor manuals describe the primary computer platforms and the principal system components.~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	Risk Rating	~~Mitigation Strategy~~
	~~communications resources.~~				
~~M-59~~	~~The system security planning should include any security software protecting the system and information.~~	~~N/A~~	~~The system has no additional security software other than that provided by the native OS and the GEMS application. These security controls are addressed in the Technical Security Requirements.~~		
~~M-60~~	~~A description of the rules for interconnecting systems and for protecting shared data must be included with the system security planning.~~	~~N/A~~	~~The voting system does not currently have any connections with other systems, with the exception of the SBE GEMS server. The risks associated with the SBE GEMS server interconnections are described in the Operational and Technical Security Requirements.~~		
~~M-61~~	~~The system security planning should list any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of data/information in the system.~~	~~M~~	~~The DBM IT Security Policy and Standards and COMAR provide specific requirements for confidentiality, integrity, or availability of data/information in the system.~~		
~~M-62~~	~~The system security planning should describe, in general terms, the information handled by the system and the need for protective measures; relate the information handled to each of the three basic protection requirements (confidentiality, integrity, and availability); and for each of the three categories, indicate if the requirement is: High, Medium, or Low.~~	~~M~~	~~Results from this risk assessment will determine the effectiveness of existing security controls and provide recommendations for mitigating the identified risks.~~ ~~Note: This risk assessment is the first performed on the Accuvote-TS voting system.~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-63	The system security planning should include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system.	M	Results from this risk assessment will determine the effectiveness of existing security controls and provide recommendations for mitigating the identified risks. Note: This risk assessment is the first performed on the Accuvote-TS voting system.		
M-64	The system security planning should describe the risk assessment methodology used to identify the threats and vulnerabilities of the system, and include the date the review was conducted.	M	This risk assessment describes the methodology used to identify the threats and vulnerabilities of the system and includes the date this review was conducted. Note: This risk assessment is the first performed on the Accuvote-TS voting system.		
M-65	If there is no system risk assessment, the system security planning should include a milestone date (month and year) for completion of the assessment.	M	This risk assessment satisfies this requirement. Note: This risk assessment is the first performed on the Accuvote-TS voting system.		
M-66	The system security planning should list any independent security reviews conducted on behalf of the state on the system in the last three years.	M	This risk assessment satisfies this requirement. Note: This risk assessment is the first performed on the Accuvote-TS voting system.		
M-67	The system security planning should include information	M	If the system security planning does not include information about the type of		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.~~		~~security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result, then the results of the assessment may be misinterpreted or not relevant, and the confidentiality, integrity, and availability of the system may be compromised.~~ ~~Results from this risk assessment determine the effectiveness of existing security controls and provide recommendations for mitigating the identified risks.~~ ~~Note: This risk assessment is the first performed on the Accuvote-TS voting system.~~		
~~M-68~~	~~If the system or part of the system is in the initiation phase, the system security planning should reference the sensitivity of information handled.~~	~~N/A~~	~~The system is not in the initiation phase.~~		
~~M-69~~	~~The system security plan should, during the first part of the development/ acquisition phase, include security requirements, which are developed at the same time system planners define the requirements of the system.~~	~~N/A~~	~~The system is not in the development/ acquisition phase.~~		
~~M-70~~	~~If the system or part of the system is in the development/ acquisition phase, the system~~	~~N/A~~	~~This system is not in the development/ acquisition phase.~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	security planning should include a general description of any specifications that were used and whether they are being maintained.				
M-71	If the system or parts of the system are in the operation/ maintenance phase, the system security planning should document the security activities conducted or planned for in that part of the system.	M	The system is in the operational phase and this Risk Assessment along with the RISC database documents the security activities conducted and planned.		
M-72	The system security planning should provide the date of authorization, name, and title of management official authorizing processing in the system.	M	The SBE has authorized use of this system.		
M-73	If the system is not authorized, the system security planning should provide the name and title of manager requesting approval to operate and date of request.	N/A	The SBE has authorized use of this system.		
M-74	The system security planning should include detailed information on whether all positions have been reviewed for sensitivity level, and if not, statement on the planned date for completion of position sensitivity analysis.	U	If the system security planning does not include detailed information on whether all positions have been reviewed for sensitivity level, and if not, statement on the planned date for completion of position sensitivity analysis, then an individual may be granted inappropriate access and the confidentiality, integrity, and availability of the system may be	LOW	SBE and LBE should implement a formal process for reviewing position descriptions for sensitivity levels on a periodic basis.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~compromised.~~ ~~SBE and LBE do not have a process for reviewing position descriptions for sensitivity levels.~~ ~~SBE and LBE have implemented controls to mitigate this risk including:~~ ~~□Two person rule~~ ~~□Separation of duties~~ ~~□Least privilege~~ ~~□Confidentiality agreements~~ ~~**Likelihood: LOW**~~ ~~While the likelihood of occurrence at the LBE is more likely, the LBE has implemented controls to mitigate this vulnerability. The likelihood at SBE is low, but minimal controls have been implemented.~~ ~~**Impact: HIGH**~~ ~~Although the likelihood of an incident occurring at SBE is low due to this vulnerability, it's exploitation could have significant impact on SBE's mission~~		
~~M-75~~	~~The system security planning should include a statement as to whether individuals have received background~~	~~**N/A**~~	~~No background screenings are conducted. The necessity for background screening is addressed in requirement M-32.~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	screenings appropriate for the position to which they are assigned, and if not, the date by which such screening will be completed should be included.		requirement M-32.		
M-76	The system security planning should describe conditions under which individuals are permitted system access prior to completion of appropriate background screening and any compensating controls to mitigate associated risk.	N/A	No background screenings are conducted. The necessity for background screening is addressed in requirement M-32.		
M-77	The system security planning should include detailed information on whether the type of user access is restricted to the minimum necessary to perform the job (i.e., least privilege).	M	Least Privilege is practiced throughout the SBE and LBEs by the checks and balances of the election process.		
M-78	The system security planning should include detailed information on the process for requesting, establishing, issuing, and closing user accounts.	U	If the system security planning does not include detailed information on the process for requesting, establishing, issuing, and closing user accounts, then an individual may be granted or continue to exercise inappropriate access and the confidentiality, integrity, and availability of the system may be compromised. There is currently not a process in place for establishing, issuing, and closing user accounts on the GEMS server.	MEDIUM	SBE should establish and follow a formal process for requesting, establishing, issuing and closing user accounts. Administrators should periodically delete disabled or dormant accounts after obtaining management approval. Implement a formal policy on dormant account deletion to reduce this risk.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~**Likelihood: MEDIUM**~~ ~~Unless accounts are closed promptly, users that no longer require access could continue to access the system. This is a common access means that terminated and disgruntled employees use to cause harm to their former employers. While the potential threat source may be highly motivated, other security controls such as physical security controls are in place.~~ ~~**Impact: HIGH**~~ ~~Having inactive user accounts or the use of default accounts increases the possibility of unauthorized viewing and/or exploitation of sensitive data or system settings.~~		
~~M-79~~	~~The system security planning should include detailed information on how critical functions are divided among different individuals (i.e., separation of duties).~~	~~**P**~~	~~If the system security planning does not include detailed information on how critical functions are divided among different individuals (i.e., separation of duties), then an individual may be granted inappropriate access and the confidentiality, integrity, and availability of the system may be compromised.~~ ~~Separation of Duties is practiced when possible. Lack of resources at the SBE and LBEs make total separation of duties impractical.~~ ~~**Likelihood: MEDIUM**~~	~~**MEDIUM**~~	~~Perform Separation of Duties of critical functions.~~

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~There are effective deterrents for misusing system privileges.~~ ~~**Impact: MEDIUM**~~ ~~This vulnerability could impact SBE's mission if exploited.~~		
~~M-80~~	~~The system security planning should include detailed information on what mechanisms are in place for holding users responsible for their actions.~~	~~M~~	~~Registration and Election Laws of Maryland and COMAR hold users responsible for their actions.~~		
~~M-81~~	~~The system security planning should include detailed information on the kind of friendly or unfriendly termination procedures used.~~	~~U~~	~~If the system security planning does not include detailed information on the kind of friendly or unfriendly termination procedures used, then a terminated employee may have unauthorized access to the system which may result in the loss of confidentiality, integrity, and availability of the system.~~ ~~There are not documented procedures for handling the termination of an election official or technician with administrator access. Without an established process for promptly closing user accounts upon termination, unauthorized system access may occur.~~ ~~**Likelihood: MEDIUM**~~ ~~Unless accounts are closed promptly, users that no longer require access could~~	~~**MEDIUM**~~	~~Privilege revocation procedures should be developed to address the possibility of a disgruntled election official or system technician.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			~~continue to access the system. This is a common access means that terminated and disgruntled employees use to cause harm to their former employers. While the potential threat source may be highly motivated, other security controls such as physical security controls are in place.~~ ~~**Impact: HIGH**~~ ~~Disgruntled former employees could have unauthorized viewing and/or exploitation of sensitive data or system settings.~~		
~~M-82~~	~~System security planning should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting systems (such as electric power), backup media, and any other elements required for system's operation.~~	~~M~~	~~Vendor manuals and election judge manuals address all of the elements required for system operations.~~		
~~M-83~~	~~System security planning should describe physical protection controls, specifically physical protection for the system, the area where processing takes place, and physical access.~~	~~M~~	~~Vendor manuals, election judge manuals, and the SBE Implementation Plan describe physical protection controls at the polling places as well as the warehouses where equipment is stored.~~		
~~M-84~~	~~System security planning should address fire safety, failure of supporting utilities,~~	~~M~~	~~The SBE Disaster Recovery and Incident Management Plan addresses fire safety, failure of supporting utilities, structural~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	structural collapse, plumbing leaks, interception of data, mobile and portable systems.		collapse, plumbing leaks, interception of data, mobile and portable systems.		
M-85	System security planning should describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media.	M	The COMAR and the Implementation Plan describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media.		
M-86	System security planning should list controls used to monitor the installation of, and updates to, software.	M	The COMAR 33.09.05.12 and ITA certification satisfies this requirement.		
M-87	System security planning should describe the establishment of a user support help desk or group that can offer advice.	M	Vendor supplied support and LBE trained technicians provide help desk support.		
M-88	System security planning should describe procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.	M	In their aggregation, the processes and procedures contained in the Election Judge manuals, Implementation Plan, Administrators Guide and Disaster Recovery and Incident Management Plan satisfy this requirement in totality.		
M-89	System security planning should describe procedures for ensuring that only authorized users pick up, receive, or deliver equipment, input and	M	The SBE AccuVote Touch Screen Voting System Phase II Implementation Plan describes procedures for ensuring that only authorized users pick up, receive, or deliver equipment, input and output		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	output information and media.		information and media.		
M-90	The system security planning should describe the use of audit trails for receipt of sensitive inputs/outputs.	M	The GEMS Server Administration guide describes the use of audit trails for receipt of sensitive election inputs/outputs.		
M-91	System security planning should describe procedures for restricting access to output products.	M	Access to output products, i.e., the election results, is restricted to individuals with a need to know as described in the Election Judge Manual, 2002 Election Results Transfer Memorandum, and Election Night Results Processing.		
M-92	System security planning should describe procedures and controls used for transporting Diebold equipment and election results.	M	The SBE AccuVote Touch Screen Voting System Phase II Implementation Plan, Election Judge manuals, Election Administrator Guide describes procedures and controls used for transporting Diebold equipment and election results.		
M-93	System security planning should describe the use of internal/external labeling for sensitivity.	N/A	No labeling is used for sensitivity levels.		
M-94	The system security planning should describe the use of external labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates).	N/A	No labeling is used for sensitivity levels.		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-95	System security planning should describe the use of audit trails for inventory management.	M	The SBE AccuVote Touch Screen Voting System Phase II Implementation Plan, Election Judge manuals, Election Administrator Guide describes the use of audit trails for inventory management.		
M-96	System security planning should describe media storage vault or library physical, environmental protection controls/procedures.	M	The SBE AccuVote Touch Screen Voting System Phase II Implementation Plan, Election Judge manuals, Election Administrator Guide describes media storage vault or library physical, environmental protection controls/procedures.		
M-97	System security planning should describe procedures for sanitizing electronic media for reuse (e.g., overwriting or degaussing electronic media).	M	COMAR article 33.10.01.41 describes procedures for reuse (e.g., overwriting or degaussing electronic media).		
M-98	System security planning should describe procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse.	P	If system security planning does not describe procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse, then the media may be obtained by an unauthorized user. The COMAR article 33.10.01.41 describes procedures for controlled storage and handling of results media. The destruction of spoiled media is not addressed. **Likelihood: MEDIUM**	**LOW**	Develop and implement a policy for destroying spoiled media.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~An attacker may exploit this vulnerability by gaining access to spoiled media that is improperly discarded.~~ ~~**Impact: LOW**~~ ~~Once an election is concluded, the media does not contain sensitive information. Election results, once released, are public information. Spoiled media, such as PCMCIA cards that may be improperly discarded during an election could potentially be recovered using advanced techniques. However, the information that could potentially be recovered from an individual PCMCIA card would be of little value, as it would be limited to vote information from a single terminal.~~		
~~M-99~~	~~System security planning should describe procedures for shredding or other destructive measures for hardcopy media when no longer required.~~	~~U~~	~~If system security planning does not describe procedures for shredding or other destructive measures for hardcopy media when no longer required, then information may be inadvertently disclosed to unauthorized individuals resulting in the potential loss of confidentiality of the voting system.~~ ~~There are no procedures that address user actions for disposing of system documentation to prevent unauthorized viewing.~~ ~~**Likelihood: HIGH**~~	~~**MEDIUM**~~	~~Develop and implement a policy for destroying hardcopy media when no longer required.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			~~There are no controls to ensure that system documentation is destroyed when no longer needed, an attacker is can exploit this vulnerability by gaining access to improperly disposed of sensitive documentation.~~ **~~Impact: MEDIUM~~** ~~A successful attack may violate confidentiality, integrity, and/or availability of the system possibly delaying the SBE's mission and damaging its reputation or interests.~~		
~~M-100~~	~~System security planning should describe contingency plan procedures that would be followed to ensure the system continues to process all processes if a disaster should occur and provide a reference to the detailed plans.~~	~~M~~	~~The SBE Disaster Recovery and Incident Management Plan details the procedures for the SBE and LBE to recover from a disaster/incident.~~		
~~M-101~~	~~System security planning should address procedures in place to ensure that maintenance and repair activities are accomplished without adversely affecting the security of the system.~~	~~M~~	~~The legal agreement with Diebold includes provisions for compliance with the State of Maryland Information and Security Policy and Standards.~~		
~~M-102~~	~~System security planning should describe configuration management procedures for the system.~~	~~M~~	~~The SBE AccuVote Voting System Change Control Plan outlines the standard and systematic process that will be used for all Change Requests for the AccuVote-TS voting system project~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			AccuVote-TS voting system project.		
M-103	System security planning should describe policies for handling copyrighted software or shareware.	M	The State of Maryland Information and Security Policy and Standards contain policies for handling copyrighted software or shareware.		
M-104	System security planning should describe any controls that provide assurance to users that the information has not been altered and that the system functions as expected.	M	In their aggregation, the processes and procedures contained in the Election Judge manuals, Implementation Plan, Administrators Guide and Disaster Recovery and Incident Management Plan satisfy this requirement.		
M-105	System security planning should list the documentation maintained for the general support system.	M	SBE has a listing of documentation for the electronic voting system.		
M-106	System security planning requires a standardized log-on banner where appropriate be included in the system documentation.	M	The log on banner is detailed in the State of Maryland Information and Security Policy and Standards.		
M-107	System security planning should include information on security awareness and training.	U	If system security planning does not include information on security awareness and training then the security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised. The training for the electronic voting system does not include an information security component. The increasing number of threats to IT systems has	HIGH	Implement a formal security awareness, training, and education program appropriate for each user's level of access.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			resulted in the need for security awareness, training, and education at all levels. Failure to conduct security awareness, training and education leaves election officials at all levels potentially unaware of the vulnerabilities and threats to their system. Without this awareness, the officials may not correctly or completely carry out vital security duties. **Likelihood: HIGH** Since the security of the AccuVote-TS system relies on non-technical controls performed by personnel, such as election judges, this awareness is vital to ensuring the security of the system. The lack of a security awareness training program provides an opportunity for a motivated attacker to exploit the system. **Impact: HIGH** The impact of the election officials potentially failing to carry out vital security duties could significantly impair the SBE mission.		
M-108	System security planning should describe incident handling procedures in place for the general support system.	**M**	The SBE Disaster Recovery and Incident Management Plan, The Risks, Issues, Systems Incidents, and Changes (RISC) Plan and Election Judge manuals describe incident handling procedures.		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-109	System security planning should describe how the general support system identifies access to the system, specifically, unique identification, correlate actions to users, maintenance of user IDs, and inactive user IDs.	U	If system security planning does not describe how the general support system identifies access to the system, specifically, unique identification, correlate actions to users, maintenance of user IDs, and inactive user Ids, then an individual may be granted inappropriate access and the confidentiality, integrity, and availability of the system may be compromised. There is no documentation that identifies the process for maintaining appropriate access controls for the system. Lack of proper documentation has resulted in the vendor default settings being left in place with the default user ID and password in the configurations. This information (i.e., passwords) is also documented in various manuals. **Likelihood: HIGH** Vendor default settings are in place with the default user ID and password in the configurations. This password information is also documented in various manuals, thus making this vulnerability easily exploitable. **Impact: HIGH** An unauthorized user that gains access to the system via the default and/or published user ID and password will be able to take any action that an authorized user could take. These actions include accessing sensitive information,	HIGH	Document procedures that describe how the general support system identifies access to the system, specifically, unique identification, correlate actions to users, maintenance of user IDs, and inactive user IDs. Ensure that the identification and authentication and auditing mechanisms employed comply with State of Maryland Security Policies and Standards.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			introducing malicious code, deleting or modifying data, and impeding the mission of the SBE.		
M-110	System security planning should describe the general support system's authentication control mechanisms.	M	In their aggregation, the processes and procedures contained in the Election Judge manuals, Implementation Plan, Administrators Guide and Disaster Recovery and Incident Management Plan satisfy this requirement.		
M-111	System security planning requires the minimum number of characters for a password to be between six and eight characters in a combination of alpha, numeric, or special characters.	U	If system security planning does not require the minimum number of characters for a password to be between six and eight characters in a combination of alpha, numeric, or special characters, then passwords may be guessed resulting in an individual being granted inappropriate access and the confidentiality, integrity, and availability of the system may be compromised. This requirement fails due to the use of vendor supplied default passwords, which do not meet the State of Maryland Information Security Policy and Standards. Therefore, passwords may be easily compromised. **Likelihood: MEDIUM** With physical access to the system and the assistance of a password dictionary or similar password cracking software, or by brute force, the threat source can figure out the password and authenticate to the system as a legitimate user. This	**MEDIUM**	The system should adhere to the State of Maryland Security Policy and Standards for password complexity.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			can be more damaging if the exploited user account has elevated privileges. Impact: HIGH Unauthorized logon use can result in a variety of consequences ranging from accessing, sensitive information and introducing malicious code, to the destruction, modification, and/or defacement of data, impeding the mission of the SBE and its image/trust among its customers, peers, and the general public.		
M-112	System security planning should discuss logical access controls in place to authorize or restrict the activities of users and system personnel within the general support system.	M	In their aggregation, the processes and procedures contained in the Election Judge manuals, Implementation Plan, Administrators Guide and Disaster Recovery and Incident Management Plan satisfy this requirement.		
M-113	System security planning should describe hardware and software features designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and/or to detect unauthorized access activities.	M	The vendor-supplied manuals describe hardware and software features designed to permit only authorized access and transactions, particularly through the use of the voter access cards.		
M-114	There should be a System Security Plan, which should: (1) Describe formal policies that define the authority that will be	U	If there is a not a System Security Plan, that: 1) Describes formal policies that define the authority that will be granted to each	HIGH	SBE should develop and document a System Security Plan. The System Security Plan should: (1) Describe formal policies that define

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	granted to each user or class of users; (2) Indicate if these policies follow the concept of least privilege which requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more; and, (3) Include in the description the procedures for granting new users access and the procedures for when the role or job function changes.		user or class of users; 2) Indicates if these policies follow the concept of least privilege which requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more; and, (3) Includes in the description the procedures for granting new users access and the procedures for when the role or job function changes, then the security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised. There is no System Security Plan for the electronic voting system. The purpose of the system security plan is to provide an overview of the security requirements of the system and describe controls in place or planned responsibilities and expected behavior of all individuals who access the system. **Likelihood: HIGH** The System Security Plan provides the mechanism for structured planning of adequate, cost-effective security controls for the system. Without the System Security Plan control, a threat source		the authority that will be granted to each user or class of users; (2) Indicate if these policies follow the concept of least privilege, which requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more; and, (3) Include in the description the procedures for granting new users access and the procedures for when the role or job function changes.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			~~may exploit vulnerabilities that are inherent to the system and that do not have adequate security controls in place.~~ ~~**Impact: HIGH**~~ ~~This vulnerability can expose the SBE's data to destruction, alteration, disclosure, and unavailability of critical system resources, impeding or delaying its mission, and damaging its reputation or interest.~~		
~~M-115~~	~~The System security planning should describe the system's capability to establish an Access Control List or register of the users, and the types of access they are permitted.~~	~~**M**~~	~~The SBE and LBEs have a manual register of users and technicians throughout the precincts and each of their respective areas of coverage. The SBE and LBE procedures specify the access each group of users is allowed to possess.~~		
~~M-116~~	~~System security planning should indicate whether a manual Access Control List is maintained.~~	~~**M**~~	~~The SBE and LBEs have a manual register of users and technicians throughout the precincts and each of their respective areas of coverage.~~		
~~M-117~~	~~System security planning should indicate if the security software allows application owners to restrict the access rights of other application users, the general support system administrator, or operators to the application programs, data, or files.~~	~~**M**~~	~~In their aggregation, the processes and procedures contained in the Election Judge manuals, Implementation Plan, Administrators Guide and vendor manuals satisfy this requirement.~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-118	System security planning should describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.	M	In their aggregation, the processes and procedures contained in the Election Judge manuals, Implementation Plan, Administrators Guide and vendor manuals satisfy this requirement by ensuring the principle of least privilege.		
M-119	The System security planning should indicate how often Access Control Lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application.	U	If the System security planning does not indicate how often Access Control Lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application, then an individual may retain inappropriate access and the confidentiality, integrity, and availability of the system may be compromised. System security planning documents do not indicate that Access Control Lists are reviewed regularly to identify and remove users who no longer require access. **Likelihood: MEDIUM** This vulnerability could be exploited if a user changes job functions or leaves the organization and is not removed from the system. **Impact: MEDIUM** Users that no longer require access to the system may view information that they are unauthorized to view or may	**MEDIUM**	SBE should generate, maintain, and secure a list of approved users and their accesses. Maintaining a current list of approved users and their accesses will reduce the likelihood of leaving privileges unchanged when users change job functions or leave the organization.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~change system settings inappropriately..~~		
~~M-120~~	~~System security planning should describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users, and document any evaluation made to justify/support use of "discretionary access control.~~	~~P~~	~~If system security planning does not describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users, and document any evaluation made to justify/support use of "discretionary access control, then unauthorized individuals may gain access to the information and the confidentiality, integrity, and availability of the system may be compromised.~~ ~~DAC or MAC provide for granular security.~~ ~~Vendor guides describe how both the server and the voting terminals practice discretionary and mandatory access controls over the data. However, copying of files or information is not covered.~~ ~~Lack of controls over data duplication may result in a user viewing data that was not explicitly authorized for the user to view.~~ ~~**Likelihood: MEDIUM**~~ ~~Without proper controls specifying the rules for the copying of information, an authorized user may make copies for unauthorized individuals.~~	~~**LOW**~~	~~SBE should develop and document a System Security Plan that includes controls specifying who is authorized to make copies of files or information accessible to other users.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			Impact: LOW While the copying of information may result in damage to SBE or LBE's reputation, it would not significantly impact the SBE and LBE mission.		
M-121	System security planning should describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users.	U	If system security planning does not describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users, then unauthorized attempts may go undetected resulting in the failure to identify new and emerging threat sources which may eventually lead to the compromise of the system confidentiality, integrity, and/or availability. There is no documentation that describes controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Likelihood: HIGH Threat sources are more likely to exploit a system if evidence against his/her actions cannot be gathered or obtained. Impact: HIGH The absence of this security control may lead to unauthorized, undetected, or unknown system access orchanges to system settings, resulting in significant impairment of the SBE mission.	HIGH	Document and implement security controls to detect unauthorized transaction attempts by authorized and/or unauthorized users.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	Risk Rating	Mitigation Strategy
~~M-122~~	~~Logical access controls in the system security planning should indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.~~	~~M~~	~~The State of Maryland Information and Security Policy and Standards indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.~~		
~~M-123~~	~~System security planning should describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends, and discuss in-place restrictions.~~	~~N/A~~	~~The systems are only in use during scheduled elections and in authorized election preparation activities.~~		
~~M-124~~	~~System security planning should discuss cryptographic methodology and key management procedures, if encryption is used.~~	~~N/A~~	~~If system security planning does not discuss cryptographic methodology and key management procedures, if encryption is used, then weak or poor cryptography may be implemented resulting in the potential disclosure or modification of sensitive information by unauthorized users.~~ ~~Encryption is not used for data stored on the PCMCIA cards or the transmissions from the DRE to the GEMS server. The data in DRE memory is encrypted using DES, but the memory is cleared when~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			the machine is powered off.		
M-125	The system security planning should discuss additional hardware or technical controls installed and implemented to provide protection against unauthorized system penetration and other known Internet threats and vulnerabilities, if general support system is connected to the Internet or other wide area network.	N/A	If the system security planning does not discuss additional hardware or technical controls installed and implemented to provide protection against unauthorized system penetration and other known Internet threats and vulnerabilities, when the support system is connected to the Internet or other wide area network, then unplanned risks may be introduced to the system and the existing security controls may be circumvented and the confidentiality, integrity, and availability of the system may be compromised. There are no additional hardware or technical controls installed or implemented on the SBE GEMS server for discussion.		
M-126	System security planning should describe any type of secure gateway or firewall in use, including its configuration.	N/A	A firewall is not in use.		
M-127	System security planning should provide information regarding any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices and if additional passwords or tokens are required.	N/A	If system security planning does not provide information regarding any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices and if additional passwords or tokens are required, then the security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			may be compromised. There are not any port protection devices in use.		
M-128	System security planning should identify whether internal security labels are used to control access to specific information types or files, and if such labels specify protective measures or indicate additional handling instructions.	N/A	There are no security labels used to control access in the electronic voting process.		
M-129	System security planning should indicate if host-based authentication is used.	N/A	Host based authentication is not used.		
M-130	System security planning should describe the rationale for electing to use or not use warning banners and provide an example of the banners used.	M	The log on banner is detailed in the State of Maryland Information and Security Policy and Standards.		
M-131	The security planning should describe audit trail mechanisms in place.	M	The Election Judge manuals and the Election Administrator Guide describe manual audit trail mechanisms through the use of signed affidavits and checklists. The GEMS server administrator guide describes audit trail mechanisms on the server side.		
M-132	System security planning should address if the audit trails provide accountability by providing a trace of user	M	The Election Judge manuals and the Election Administrator Guide provide accountability through the use of signed affidavits and checklists. The GEMS		