To counter the ongoing election cybersecurity threat, and echo recommendations recently extended by the U.S. Senate Committee on Intelligence\(^1\), the Cybersecurity Subcommittee of the Election Assistance Commission (EAC) Board of Advisors recommends that the EAC give states the following advice:

1. States should employ information technology cybersecurity best practices outlined by the Center for Internet Security (CIS)\(^2\) and the U.S. Department of Commerce National Institute of Standards and Technology (NIST)\(^3\), as applicable, and specifically address the following –
   a. Evaluate and prioritize steps to safeguard voter registration systems, state election records, pre-election activities, voting machines, election management systems, election reporting systems, and all other associated information technology systems and applications which support elections in its entirety, from malicious cyber activity;
   b. Conduct annual cybersecurity-related audits of information systems;
   c. Roadmap information technology infrastructure investments that reduce risks and vulnerabilities associated to legacy information technology systems*;
   d. Collaborate with the Department of Homeland Security and Office of the Director of National Intelligence Election Threats Executive\(^4\), as able, to improve communication and the sharing of cybersecurity information and best practices.


\(^2\) [https://www.cisecurity.org/controls/cis-controls-list/](https://www.cisecurity.org/controls/cis-controls-list/)

\(^3\) [https://nvd.nist.gov/800-53](https://nvd.nist.gov/800-53)

2. To ensure that states adopt a layered security methodology, the EAC should advise states to –
   a. Use paper ballots as the ballot of record\(^5,6\) to ensure strong software independence, tamper evidence, and resilience;
   b. Ensure that voting systems allow all voters, regardless of ability or age, to cast a paper ballot privately and independently, and that those who so desire may hand mark their paper ballots;
   c. Mandate procedures to ensure that the paper ballots are and remain a trustworthy record of voter intent, including appropriate, tamper-evident physical security measures and verifiable chain of custody for ballots, voting machines, and other election-related items and materials, as well as ballot accounting, cross checks of the number of ballots received against the number of voters, and similar measures;
   d. Conduct routine, transparent, publicly verifiable “compliance audits”\(^*\) to ensure that the cast paper ballots are and remain a trustworthy record of voter choices for the purpose of tabulation, recounts, and audits;
   e. Conduct routine, transparent, publicly verifiable post-election manual audits from the human-readable marks on the physical paper ballot. These audits should compare a sample of the paper ballots to electronic totals, with the goal of adopting statewide audits with a high level of statistical confidence at the earliest feasible time to ensure that tabulation errors did not alter reported election outcomes;
   f. Mandate that any recounts be transparent and manually determine voter intent from the human-readable marks on the physical paper ballot;
   g. Consider the suitability of systems for compliance audits and audits with a high level of statistical confidence when purchasing new equipment\(^7\).

---

* Legacy System Definition - An information system that may be based on outdated technologies but is critical to day-to-day operations. (Gartner)

Adopted November 18, 2019

---


\(^7\) Equipment choice can have a large effect on the cost of sound audits.