

Analysis: 2026 Election Infrastructure Security Plan

September 24, 2026

Contact: Keara Mendez, Chief of External Affairs | keara@responsivegov.org

TLDR: Today's new CISA report does not identify new election security programs, risks, threats, or vulnerabilities. It is mostly a repackaging of CISA's existing service catalog.

Today, the White House and CISA released a "[2026 Election Infrastructure Security Plan](#)." The report summarizes DHS's and CISA's approach to safeguarding election infrastructure for the 2026 election. **This is not a new program nor does it appear to present new risks** – this report largely repeats existing past CISA programs and identifies some internal structural changes. It reiterates CISA's existing mission and does not announce a new program or expansion.

The report explains what election infrastructure is, and potential cyber targets and vulnerabilities. The report specifically identifies voter registration databases as threats for cyberattacks. **The report does not identify any specific cyberattacks, threats, or vulnerabilities.**

The report is mostly a repackaging of CISA's existing service catalog. Newer information relates to structural changes within CISA: information sharing now runs through state fusion centers, Regional Directors now carry the election advisor role, and false/misleading narratives remain outside of federal support entirely.

The report closes by listing CISA resources available to state and local election officials. These resources reflect historical offerings from CISA, including offerings that precede the current Administration. Specifically, CISA asserts it will offer an information-sharing platform to exchange "intelligence and situational updates" prior to the 2026 election, CISA Central and federal partners will participate, and it is modeled on the FIFA World Cup 2026 deployment. Although the report describes the platform as free for all fusion centers and state and local election officials, the plan does not name the platform or explain how to get access, so jurisdictions will need to reach out to their regional office for details.

CISA explicitly recommends paper ballots and manual post-election audits before certification of election results – practices already [widely](#) used across the country.

The unveiling of these services in late September will likely lead to minimal uptake, as voting is already underway and any value from these recommendations may not be realized until well after the 2026 midterms. The report also does not discuss staffing, funding, or general capacity.

Many of CISA's election experts were fired or left the agency. CISA's Acting Director [recently announced](#) that the agency is looking to hire additional experts for various cybersecurity purposes, including election security. These new hires can potentially help elections officials, but trust between local and state governments and CISA, and DHS more broadly, is currently

broken. The impact of today's announcement and any hiring surge is expected to be limited with such a late rollout and the general weaponization of the federal government this past year.

Our understanding is at least some of the new hires are credible people who care about cybersecurity, but they are not necessarily election experts. Even if CISA commits support going forward, the agency lost all established expertise in the field of election security, meaning services and offerings will not be as fine-tuned to the needs of elections officials as they were in the past. New CISA hires tend to be general-purpose cybersecurity professionals that lack context in a specific area.

Responsive Gov is monitoring how this report is being distributed and utilized, particularly if there are changes to federal grants and agency policies, and will follow up with any new updates.