



Homeland
Security

August 24, 2026

White House Transparency Task Force:

We are in receipt of your latest request for the production of documents. We are actively identifying responsive records and reviewing for potential declassification and will continue with the rolling document production. Our initial disclosure included some documents that the White House Transparency Task Force has determined cannot be released at this time. This letter was prepared to fulfill the Task Force's request for an unclassified overview of relevant election infrastructure supply chain vulnerabilities.

Recently declassified records, including a 2024 ODNI Annual Threat Assessment, concluded that "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks. Beijing's cyber espionage pursuits and its industry's export of surveillance, information, and communications technologies increase the threats of aggressive cyber operations against the United States and the suppression of the free flow of information in cyberspace."¹

A National Intelligence Council Memorandum from October 2024 stated, "We assess that some U.S. adversaries—at a minimum China, Iran, and Russia...have the technical capability to access some U.S. election-related networks and systems."²

The declassification of these and other documents supports the need for strong mitigation strategies, particularly considering the known weaknesses in the election infrastructure supply chain. Voting machines with components manufactured by foreign adversaries introduce significant security risks. These vulnerabilities mean that malicious actors could potentially compromise election infrastructure at any stage of the supply chain, even before the machines are assembled or deployed. If a component is tampered with during manufacturing, it could serve as a point-of-entry for hackers, allowing for the possibility of synchronized attacks across multiple machines and jurisdictions.

Unfortunately, the voting-system industry, like other sectors of critical infrastructure, is impacted by the fact that some necessary components cannot be sourced from domestic manufacturers, so vendors are dependent on foreign suppliers. Nine voting system vendors are used in U.S. elections. Three of those vendors, ES&S, Hart InterCivic, and Dominion, make up

¹ <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>.

² <https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Foreign-Threats-to-US-Elections-After-Voting-Ends-in-2024.pdf>.

more than 80% of the market share. Representatives from each of those vendors have acknowledged that their voting machines have parts made in China.

When testifying before Members of Congress, representatives from these vendors detailed universal reliance on foreign-made parts.³ The then-President and CEO of Dominion stated, “voting systems manufacturers would be challenged to source certain product hardware components from outside of China. In some cases, there are simply no alternative suppliers.”⁴

Representatives from ES&S similarly stated, “In some instances, there is no ability to procure from alternative component suppliers. Some components are sole-sourced, protected by a patent and/or intricate to the design of the circuit or sub-assembly.”⁵

Acknowledging the United States’ reliance on component parts that originate from countries accused of committing cyberattacks against the United States, representatives from Hart InterCivic requested “additional guidance and best practices on supply chain security from DHS.”⁶

There is no question that election security is national security. Under the leadership of President Trump, I have directed the Department of Homeland Security to prioritize election security. Electronic voting systems have one job—to accurately count the votes on ballots. The Homeland Security Grant Program requires states to trust but verify the results produced by the voting machines. To receive full grant awards, states must demonstrate that they have conducted random post-election manual counts of paper ballots to ensure that any errors or manipulation is detected. This is in addition to numerous other actions being taken across DHS components to secure election infrastructure.

It is an honor to support President Trump’s mission to have the most transparent administration in history, and I appreciate the work of the White House Transparency Task Force. We look forward to the declassification of additional records so the American people can better understand all of the ways my Department works to protect the homeland.

Sincerely,



Markwayne Mullin
Secretary of Homeland Security

³ 2020 Election Security – Perspectives from Voting System Vendors and Experts: Hearing Before the Comm. on H. Admin., 116th Cong. (2020), <https://nsarchive.gwu.edu/document/24853-document-75-house-committee-house-administration-2020-election-security-perspectives>.

⁴ *Id.* at 222.

⁵ *Id.* at 190.

⁶ *Id.* at 243.