






Protecting America's Election Infrastructure: Threats, Vulnerabilities, and Countermeasures as a National Security Agenda



The U.S. faces serious threats to its election infrastructure

The vulnerability of election technology is a clear and present threat to our national security. The US election infrastructure has hardware, software, and information limitations that require focused attention:

-  The architecture of U.S. election administration systems was never designed as fault-tolerant to withstand digital compromise;
-  The provisioning of systems was never configured to ensure a rapid, agile innovation cycle to address evolving security threats; and
-  There are vulnerabilities in the cyber supply chain as a consequence.

Threats to our election administration technology infrastructure are inherently threats to our democracy.

Threat #1: Hardware is obsolete and procured in an unsecure manner

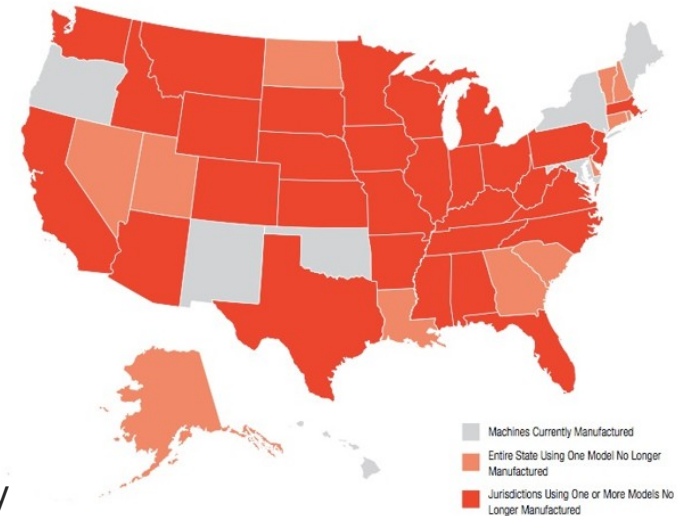
Risk Assessment:

- Vast majority of voting systems hardware is no longer manufactured.
- States (and vendors) now rely on diminishing supply of spare parts from abroad.
- This amounts to an uncontrolled open market of replacement components.

Recourse:

- Establish a trustworthy closed supply chain to drastically reduce foreign adversaries' ability to source tampered hardware components that could pose a threat to integrity of voting systems incorporating such components.

States Using Primary Polling Place Machines That Are No Longer Manufactured



Map Courtesy of the Brennan Center

Dependence on foreign markets for spare parts amounts to a blind spot for securing our election infrastructure.

Threat #2: Software is total mismatch for current threat environment

Risk Assessment:

- The mismatch arises from a core defect, where voting system products are based on ordinary 90's-era PC technology, in which the entire software base is modifiable and every system is capable of running any new software consistent with the hardware.
- Ability to arbitrarily modify, while useful for PCs, is counter-productive in voting systems. With this antithetical foundation, current voting systems are just as vulnerable to attack as the ordinary PC technology in which they are based.

Example:
PLA Unit 61398 —
one of many
foreign cyber-ops
teams with known
activities & agenda.

Recourse:

- To obtain meaningful software assurance, a new generation of election technology must be redesigned, based on practices of fixed-function embedded systems.
- Such security-centric engineering has served well and evolved from years of innovation in military, communications, and aerospace systems.

This fundamental risk cannot be contained, only mitigated, resulting in a must win battle that requires the U.S. to make a complete software redesign.

Threat #3: Election information may not be reliable

The mission of election officials is not just to operate assets and perform procedures to yield the elections' result; it is also to produce sufficient evidence of the accuracy and authenticity of that information. Without such evidence, an election may fail to create the consensus on the results as the basis for an orderly transfer of political power.

Risk Assessment:

- Achieving information assurance is blocked by a lack of at least: 1) system and software integrity measures and validation methods; 2) cryptographic key management; 3) strictly controlled methods for system upgrades; and 4) system logging and data retention functions.
- Required guidelines + standards are outdated; the update of which is bound in bureaucracy.
- Uncertain future of the E.A.C., whose mission is to develop the guidelines and standards.

Recourse:

- To obtain required information assurance, a new generation of technology must be designed, and finishing new certification, design guidelines, and data standards must be accelerated.

Information assurance in an age of “weaponized content” is essential to the operational continuity of our democracy.

Bottom Line Recommendations



New Infrastructure

Rapidly re-engineering the architecture of U.S. election technology infrastructure as fault-tolerant, purpose built, application specific, componentized systems to withstand digital compromise.

(Several R&D projects are already underway, but need funding to accelerate and finish.)



New Certification & Standards

Completing required open data standards, systems design guidelines, and a new certification model for states' adoption to support (*among other things*), a more agile innovation cycle that enables component level updates to address evolving security threats.

(Work is progressing too slowly due to lack of funding.)



Controlled Supply Chain

Establishing a trustworthy closed supply chain that drastically reduces foreign adversaries' ability to source tampered hardware components that could pose a threat to voting system units incorporating such hardware components.

(Reliance on uncontrolled foreign-sourced spare parts is a blind spot risk.)

We must prevent adversarial foreign state actors from disrupting or derailing our most sovereign process of democracy — free and fair elections.

What's Required

1. R&D Funding Grants.

- There are a half dozen high assurance election technology R&D projects currently underway across the U.S., but progressing too slowly to meet the security threats outlined here due to under-funding.
- In total, these projects and others that might emerge can be finished for \$100M including grant program management costs. (That's .03% of 2002 \$3B HAVA Funding)
- Historically, DARPA and NSF have been leaders in government funding of innovation. We believe national security risks and requirements for new technology, including support of UOCAVA military voters warrant DARPA funding support for this work.

2. Funding Grant to Complete Required Certification, Guidelines, & Standards.

- This work is underway at the EAC in collaboration with NIST, but constrained by under-funding. A grant to expedite work would provide desperately needed additional staff and expand workshops for outside volunteer contributors to expedite the process.
- It is estimated this would require \$10M to finish.

3. Develop a Controlled Supply Chain.

- An agency, perhaps DHS, should be chartered to do so.
- Funding required to implement this is unknown at this writing, but it is believed DoD is most experienced and best positioned to provide advice.

Contact



Gregory Miller

Chief Operating Officer, The OSET Institute
gmiller@osetfoundation.org
650.600.1450 [O] or 503.703.5150 [M]

Mr. Miller, a computer scientist and intellectual property lawyer, is a co-founder of the OSET Institute. He serves as a subject matter expert to government on election technology integrity and security. He has provided insight and information to Homeland Security and several House and Senate committees.

The OSET Institute is a 501.c.3 purpose-based non-partisan Silicon Valley election technology research and development organization established in 2006, focused on innovating election technology infrastructure to increase integrity and security, lower cost, and improve trustworthiness to increase confidence in elections and their outcomes in order to preserve our democracy.



www.osetfoundation.org and www.TrustTheVote.org



twitter.com/OSET

