November 30, 2022

RESEARCH REPORT | Center for Election Integrity

Elections Systems are Critical Infrastructure and Must Be Protected

Anna Pingel

TOPLINE POINTS

- Voting machines, registration databases, polling locations, and voting storage facilities are designated by the Department of Homeland Security as "critical infrastructure."
- In light of significant concerns, component sourcing for elections infrastructure should be reformed to better consider national security risks.
- Instead of leaving testing and regulation of elections to manufacturers, the federal government and state governments should develop and mandate measures to safeguard elections infrastructure.

Protecting United States critical infrastructure—defined by the Department of Homeland Security (DHS) as "the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety"—is a necessary component of national security (Humphreys, Shanton, 2020). For decades, presidential administrations have recognized the need for oversight, collaboration, and security surrounding critical infrastructure. While typically critical infrastructure is thought of as emergency services, energy, banking, defense, or the like, it also necessarily includes elections infrastructure (the voting machines, voter registration databases, data management, and physical infrastructures such as polling locations and storage).

President Bill Clinton was the first to formalize and protect critical infrastructure when he issued presidential decision directive (PDD) 63 in May 1998 (PPD-63, 1998). This was updated in December 2003 by President George W. Bush through Homeland Security Presidential Directive (HSPD) 7 (HSPD-7, 2003), and then by President Barack Obama when he issued

presidential policy directive (PPD) 21 in February 2013, identifying 16 specific critical infrastructure sectors and the Departments under which they fall (PPD-21, 2013). PPD-21 also directed DHS to coordinate security issues relating to critical infrastructure in collaboration with public and private stakeholders.

In early January 2017, President Obama's DHS announced the designation of election infrastructure as one of the 20 subsectors of the existing Government Facilities Critical Infrastructure Sector (Department of Homeland Security, 2017). The Government Facilities Sector includes general-use office buildings and special-use military installations, embassies, courthouses, national laboratories, and structures that may house critical equipment, systems, networks, and functions. In addition to physical structures, the sector also encompasses cyber elements that contribute to the protection of sector assets as well as individuals who perform essential functions or possess tactical, operational, or strategic knowledge. Under this designation, election infrastructure included but was not limited to voting machines, voter registration databases, and physical infrastructures such as polling locations and storage. DHS' Cybersecurity and Infrastructure Security Agency (CISA) was designated as the lead federal agency for the Election Infrastructure Subsection (EIS).

Supply chains are one facet of elections infrastructure that is important to investigate and regulate. Supply chains primarily affect voting machines but also can impact other physical infrastructures such as security cameras used in polling places or computers used to process voter or voting data. On May 15, 2019, President Trump issued Executive Order 13873 (The White House, 2019), Securing the Information Communications and Technology and Services Supply Chain (ICT). This order declared a national emergency regarding the acquisitions of information and communications technology and services. In response to this Executive Order, CISA's Information and Communications Technology (ITC) Supply Chain Risk Management (SCRM) worked with industry and government partners to apply this to EIS by:

1. Developing a standardized taxonomy of ICT elements (hardware, software, and services)
2. Performing critical assessments on these ICT elements with appropriate stakeholder input
3. Assessing the national security risks stemming from vulnerabilities in ICT hardware, software, and services, including components enabling 5G communications.

In March 2022, the SCRM Working Group released a document as an introduction to how organizations and downstream supply chain partners, including election officials, can better secure their supply chain (CISA, 2022). It provided some information and recommendations for the procurement of

software, hardware, and services, as well as other risk management tactics, but no requirements or action ensued. Two months later, President Joe Biden continued the national emergency declared by President Trump regarding the security of supply chains in information and communications technology and services (The White House, 2022).

In addition to supply chains, the storage and use of personal identifying information (PII) of poll workers and voters are another vulnerability that can compromise the integrity of an election. On October 4, 2022, Eugene Yu, the CEO of Konnech Inc., a voting software company based in Michigan, was arrested after credible accusations of storing American PII in the People's Republic of China (PRC). The contract Konnech had with Los Angeles County did stipulate domestic storage of information, but the District Attorney's office stated that instead, it was stored on servers in the PRC. Konnech services elections offices all over the United States and has done so for years (The Associated Press, 2022).

On the state level, individual states have the option to require that elections infrastructure be subject to testing and examination by the standards set forth by the Voluntary Voting System Guidelines (VVSG) published by the U.S. Election Assistance Commission (EAC). However, even elections infrastructure that is supposedly compliant with the VVSG standards and operated in states that require compliance can still pose security issues. Recently, CISA issued an advisory warning detailing vulnerabilities affecting versions of the Dominion Voting Systems Democracy Suite ImageCast X, a voting system used in marking the ballot (CISA, 2022).

When considering how to implement safe sourcing for critical components best, the Department of Defense (DoD) provides a good model. In the 1990s, the DoD implemented a "trusted foundry" model of sourcing for microchips in an effort to ensure that component sourcing was safe. Under this model, the DoD only contracted with a few trusted foundries, or manufacturers, for microchip creation. However, this resulted in the sources failing to invest and modernize because they knew they had an exclusive financial contract with the DoD and therefore did not need to be competitive against the market in research and development of advanced microchips. Their technology fell behind the pace of the private sector because of the trusted foundry model, which created a competitive disadvantage for the DoD. Learning from this, in 2020, the DoD adopted a "zero-trust" model for critical component sourcing. This assumed that no component was safe and that everything would require testing before use. Both hardware and software involved in voting machines specifically should be subjected to validation and verification in the zero-trust model (Lopez, 2020).

Incidents such as the SolarWinds hack in 2020, in which SolarWinds Orion products were vulnerable to hacking, in

addition to the intentional malfeasance of Konnech's storage of American PII in a country that the Department of State has designated a country of concern, expose the necessity of absolute certainty in the integrity of our voting software and hardware. Especially for voting machines that use electronic tabulation, QR codes, and digital processing, and for voting systems dealing with American PII, it is vital for each component to be subject to the zero-trust model. Again, the DoD models the absolute importance of component integrity; recently, Lockheed's F-35 program, one of the most advanced fighter jet programs in the world, was grounded because one small component was found to be sourced from China. The program only just resumed after an alternative U.S.-based source was substituted (Capaccio, 2022).

Currently, there are plenty of recommendations and optional testing, and each producer of voting machines and critical infrastructure related to elections has immense discretion over the security, sourcing, manufacturing, and transport of their product. Sometimes, malfunction in election systems is due to human error, but sometimes it is not. There are several policy recommendations that would help keep American elections infrastructure safer.

First, adopting a zero-trust model to supply chains for elections infrastructure would be a beneficial measure to protect the integrity of American elections. The responsibility to implement this would fall under EIS, in collaboration with CISA and the EAC.

Second, Congress should consider a ban on sourcing election machine parts from and on producers of election infrastructure contracting or subcontracting with entities or businesses in countries designated as state sponsors of terrorism by the Department of State (currently Iran, Cuba, North Korea, and Syria) as well as the People's Republic of China and the Russian Federation. The Acquisition and Sustainment Office of the Undersecretary of Defense currently prohibits exactly this (DoD, 2021). This list may fluctuate with geopolitical changes, and election machine component import bans should reflect those changes going forward as well. It is worth noting that in 2019, Congress passed the National Defense Authorization Act (NDAA) that banned certain hardware imports from China, citing the risk of use in critical infrastructure in the military (Text - H.R.5515 - 115th Congress, 2019). It is remarkable that the very people who passed this NDAA are elected on voting machines with components sourced in China. Applying this principle to voting machines and election infrastructure is an option that could afford additional security to the EIS.

Third, Congress and the states should also consider a ban on elections infrastructure storing American PII overseas. No elections software should have the option to compromise names, birthdays, social security numbers, addresses, and more to foreign

governments, especially not foreign governments who have a vested interest in economic, social, or military power over the United States. Privacy is a crucial aspect of trusting elections infrastructure. Voters need to know that their data is secure.

It is apparent that our elections infrastructure is not where it should be. Every cycle, there are stories of malfunction, which only further fuel distrust in the election. Increasing the security and standards surrounding elections infrastructure would only serve to make our elections safer, more secure, more transparent, and more accurate. A representative democracy functions when the process of elections has integrity—and the best place to start is the source.

BIOGRAPHIES

Anna Pingel *is the Policy Analyst of the Center for Election Integrity at the America First Policy Institute.*

Works Cited

Humphreys, B., & Shanton, K. (2020, March 5). *The Election Infrastructure Subsector: Development and Challenges*. Retrieved September 28, 2022, from Congressional Research Service website: https://crsreports.congress.gov/product/pdf/IF/IF11445

Critical Infrastructure Protection (PDD 63). (n.d.). Irp.fas.org. Retrieved September 28, 2022, from https://irp.fas.org/offdocs/pdd/pdd-63.htm

December 17, 2003, Homeland Security Presidential Directive/Hspd-7. (n.d.). White House Archives. Retrieved September 28, 2022, from https://georgewbushwhitehouse.archives.gov/news/releases/2003/12/20031217-5.html

Presidential Policy Directive -- Critical Infrastructure Security and Resilience. (2013, February 12). White House Archives. Retrieved September 28, 2022, from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/

Statement by Secretary Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector. (2017, January 6). Department of Homeland Security. Retrieved September 29, 2022, from https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

CISA. (n.d.). *Government Facilities Sector | CISA*. Cybersecurity and Infrastructure Security Agency. Retrieved September 29, 2022, from https://www.cisa.gov/government-facilities-sector

Election Infrastructure Subsector-Specific Plan: 2022 Status Update. (n.d.). Cybersecurity and Infrastructure Security Agency. Retrieved September 29, 2022, from https://www.cisa.gov/sites/default/files/publications/ei-ssp-2022-status-update_508.pdf

Supply Chain Risks to Election Infrastructure. (n.d.). Cybersecurity and Infrastructure Security Agency. Retrieved October 3, 2022, from https://www.cisa.gov/sites/default/files/publications/supply-chain-risks-to-election-infrastructure_508.pdf

The White House (2022, May 12). *Notice on the Continuation of the National Emergency with Respect to Securing the Information and Communications Technology and Services Supply Chain*. The White House. Retrieved October 3, 2022, from https://www.whitehouse.gov/briefing-room/presidential-

actions/2022/05/12/notice-on-the-continuation-of-the-national-emergency-with-respect-to-securing-the-information-and-communications-technology-and-services-supply-chain-2/

The Associated Press (2022, October 5). *CEO of election software firm held on ID info theft charges*. Valley News Live. Retrieved October 3, 2022, from https://www.valleynewslive.com/2022/10/05/ceo-election-software-firm-held-id-info-theft-charges/

Konnech Home Page (n.d.). Www.konnech.com. Retrieved October 3, 2022, from https://www.konnech.com/

Voluntary Voting System Guidelines | U.S. Election Assistance Commission. (n.d.). Election Assistance Commission. Retrieved October 5, 2022, https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines

CISA Releases Security Advisory on Dominion Voting Systems Democracy Suite ImageCast X | CISA. (2022, June 3). Cybersecurity and Infrastructure Security Agency. Retrieved October 5, 2022, from https://www.cisa.gov/uscert/ncas/current-activity/2022/06/03/cisa-releases-security-advisory-dominion-voting-systems-democracy

Lopez, C. T. (2020, May 19). *DOD Adopts "Zero Trust" Approach to Buying Microelectronics*. U.S. Department of Defense. Retrieved October 5, 2022, from https://www.defense.gov/News/News-Stories/Article/Article/2192120/dod-adopts-zero-trust-approach-to-buying-microelectronics/

Capaccio, T. (2022, October 8). *F-35 deliveries to resume after Chinese alloy prompted halt*. Billings Gazette, Bloomberg News. Retrieved October 5, 2022, from https://billingsgazette.com/f-35-deliveries-to-resume-after-chinese-alloy-prompted-halt/article_cec16e62-4754-11ed-9ab6-674846811c2d.html

SUBPART 225.7 PROHIBITED SOURCES. (n.d.). Acquisition and Sustainment Office of the Under Secretary of Defense. Retrieved October 6, 2022, from https://www.acq.osd.mil/dpap/dars/dfars/html/current/225_7.htm#225.701

Bureau of Counterterrorism. (2019). *State Sponsors of Terrorism - United States Department of State*. United States Department of State. Retrieved October 6, 2022, from https://www.state.gov/state-sponsors-of-terrorism/

Text - H.R.5515 - 115th Congress (2017-2018): John S. McCain National Defense Authorization Act for Fiscal Year 2019. (2018, August 13). Retrieved October 6, 2022, from http://www.congress.gov/