IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Kari Lake, *et al.*, Plaintiffs, v. Katie Hobbs, Arizona Secretary of State, *et al.*, Defendants.	)	No. 2:22-cv-00677-JJT

Declaration of Shawn A. Smith

I, SHAWN A. SMITH, declare under penalty of perjury that the following is true and correct:

1. I have personal knowledge of the matters set forth below and could and would testify competently to them if called upon to do so.

2. My name is Shawn A. Smith. I am a retired military officer. I have Master's degrees in National Security Affairs from the Naval Postgraduate School and in Aeronautical Science from Embry-Riddle Aeronautical University. I have held an active Top Secret security clearance since 1992 and have been cleared for Sensitive Compartmented Information since 1996.

3. My military occupational specialty was space and missile operations, and I have extensive experience over 25+ years of active duty service in operating, specifying requirements for, planning the procurement of, training, testing, and commanding the employment of complex, computer-based military weapon systems.

4. My military service included significant experience in Special Technical Operations, involving advanced technology, at every level from tactical employment through operational planning, national-level policy, Presidential tasking, and requirements definition and procurement of future sensitive capabilities. I have

conceived, and advised agencies within the United States Government on, opportunities and technical approaches for supply chain compromise to affect foreign adversaries' ability to wage war against the United States, and to benefit United States national security.

5. My final active duty assignment prior to retirement in 2017 was for four years as the Senior Military Evaluator for Space and Intelligence, Surveillance, and Reconnaissance systems in the office of the Director, Operational Test & Evaluation, under the Office of the Secretary of Defense. In that role, I was responsible to execute the Director's oversight of operational testing of all non-satellite communications space systems in the Department of Defense, including the Global Positioning System, the Space-Based Infrared System, the Space Fence, the Geosynchronous Space Situational Awareness Program, and many others. Execution of that oversight required subject-matter expertise in the space domain, in the technologies involved in each system, in Scientific Test and Analysis Techniques to determine adequate and efficient test designs, and in the threat capabilities and modus operandi of foreign nation states, with respect to U.S. national security.

6. After retirement, I continued to support the Director, Operational Test & Evaluation as a consultant to adversarial assessment project teams which reviewed the results of cyber threat conduct against U.S. governmental and non-governmental national security targets by foreign adversaries, drew conclusions about the risks and impacts of that conduct, and wrote recommendations for responsive and preventive changes in technology, force structure, and defense policy, which the Director provided under his signature to the heads of the military Departments, the Secretary of Defense, and the President of the United States.

7. I have been asked to testify about the threat of supply chain compromise and attack to U.S. national security systems and critical infrastructure, in particular to election-related systems, including voting systems and, consequently, to elections. This

declaration will define and describe supply chain compromise threats, provide examples, explain that they have become pervasive and sophisticated, affecting and placing at risk the supply chain for U.S. computer systems and components, and explain the consequent ramifications for and vulnerability of U.S. election and voting systems. The information presented is unclassified and based upon my personal experiences, publicly available reporting, studies, events, incidents, policy, and de-classified U.S. Government information.

8. Given my background, experience, education, and training, and now my exposure to and understanding of the technology employed in U.S. election systems, my conclusion is that U.S. elections are critically vulnerable to exploitation by foreign adversaries through supply chain compromise of our computerized election systems.

9. Although elements of the U.S. Government appear keenly aware of the risk of supply chain compromise to our critical systems, that awareness does not appear to extend to any agency responsible for the procurement, security, certification, or use of election and voting systems, nor to imbue them with any capacity to respond effectively. Whether or not they are aware, their conduct reflects no defensive adaptation or response to that risk to protect the security and integrity of U.S. election systems or the elections using them. Given the proliferation of supply chain threats and the origin of so many attacks with deliberate, well-funded, large-scale, targeted foreign nation governmental programs, the near-universal foreign sourcing of our computers and computer components, and this lack of awareness and/or response in agencies responsible for U.S. election and voting systems, it is highly likely that numerous supply chain compromises have already been introduced to our election and voting systems and it is improbable and unwarranted to assume those compromises have not been introduced.

10. In fact, targeting U.S. voting and election systems must be an extraordinarily high priority for foreign powers; it is inconceivable that, given the opportunity, foreign

powers would not have taken the opportunity to exercise control or influence over U.S. elections, elected leadership, and thus U.S. foreign and domestic policy through supply chain attacks on U.S. election systems.

11. A "supply chain" is the aggregate of organizations, activities, people, and resources required to produce and provide a service or product. With respect to national security computer and communication systems and critical infrastructure, including election-related and voting systems, the supply chain includes computer hardware, hardware components, software, and firmware, as well as mechanisms for delivery of services, updates, modifications, and maintenance of those aggregate devices and networks comprised of or including that hardware, software, and firmware.

12. A "supply chain compromise" or "supply chain attack" (used interchangeably, throughout, though a compromise is technically one potential outcome or result from an attack) is the deliberate introduction of flaws, covert access or functionality, malicious code, and other undesirable attributes into a product or service, without the knowledge of the consumer or customer intended to receive or use the product or service, in the supply chain lifecycle of the product or service. A compromise or attack can be intended to make a device, network, or service unreliable, accessible to unauthorized parties, or to fail or behave differently when locally or remotely commanded, or when triggered autonomously by singular conditions or combinations of criteria (such as time, system state, user state, geolocation, etc.).

13. For integrated circuits (also known as "computer chips," such as the central processing unit (CPU) of a computer workstation or server), components, and computing systems, the "supply chain lifecycle" stages include "1. Conceptual, 2. Design, 3. Integration, 4. Fabrication, 5. Testing, 6. Provisioning, and 7. Deployment," and there are methods and types of attack unique or common to each of those stages. Of those stages, the Manufacturing stage is subject to the greatest variety of attack methods, including Insider Threats, Trojan Circuitry, Trojan Components, Design Alterations,

Component Replacement, Reverse Engineering, Unauthorized Disclosure, and Attacks on Design Networks.[1] According to MITRE,[2] "supply chain compromise can take place at any stage of the supply chain including: Manipulation of development tools, Manipulation of a development environment, Manipulation of source code repositories (public or private), Manipulation of source code in open-source dependencies, Manipulation of software update/distribution mechanisms, Compromised/infected system images (multiple cases of removable media infected at the factory), Replacement of legitimate software with modified versions, Sales of modified/counterfeit products to legitimate distributors, and Shipment interdiction."[3] MITRE's 2013 "Supply Chain Attack Framework and Attack Patterns" Technical Report identified 89 different attacks across and specific to the acquisition and lifecycle phases for national security systems, with all but 22 of those attacks applicable to phases prior to operational use and support.[4]

14. Supply chain compromise is no longer a hypothetical risk; it is pervasive, sophisticated, and widespread, and the most urgent, important question is not whether our computer systems are at risk of supply chain attack, but what is the precise extent of undetected supply chain attack. A 2018 global software supply chain survey reported that 66% of senior information technology (IT) decision-makers and security professionals had experienced a software supply chain attack.[5] By 2021, 93% of

---

[1] https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/supply-chain-threats-v1.pdf

[2] MITRE is a Federally-funded research and development center which operates, among other centers, the National Cybersecurity FFRDC (NCF), sponsored by the National Institute of Standards, advising the Federal government on cybersecurity threats and mitigation.

[3] https://attack.mitre.org/techniques/T1195/.

[4] https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf

[5] https://www.crowdstrike.com/resources/wp-content/brochures/pr/CrowdStrike-Security-Supply-Chain.pdf

companies surveyed had suffered a cybersecurity supply chain breach, and 97% of companies had been negatively impacted by cybersecurity breaches in their supply chain.[6] Supply chain attack is so pervasive that it must be assumed to threaten and affect all computers, computer components, hardware with embedded electronics, software, and firmware, to the extent that any aspect of them is accessible, at any time in their lifecycle from conception through end-of-life, to malicious or self-interested domestic or non-governmental actors but especially to foreign nation states and their agents.

15. A 2020 National Counterintelligence and Security Center report stated: "The exploitation of key supply chains by foreign adversaries—especially when executed in concert with cyber intrusions and insider threat activities—represents a complex and growing threat to strategically important U.S. economic sectors and critical infrastructure. Foreign adversaries are attempting to access our nation's key supply chains at multiple points—from concept to design, manufacture, integration, deployment, and maintenance—by inserting malware into important information technology networks and communications systems. The increasing reliance on foreign-owned or controlled hardware, software, or services as well as the proliferation of networking technologies, including those associated with the Internet of Things, creates vulnerabilities in our nation's supply chains. By exploiting these vulnerabilities, foreign adversaries could compromise the integrity, trustworthiness, and authenticity of products and services that underpin government and American industry, or even subvert and disrupt critical networks and systems, operations, products, and weapons platforms in a time of crisis."[7]

---

[6] https://www.bluevoyant.com/resources/managing-cyber-risk-across-the-extended-vendor-ecosystem/

[7] National Counterintelligence and Security Center, "Supply Chain Risk Management: Reducing Threats to Key U.S. Supply Chains," 20200925, at:

16. The National Institute of Standards and Technology's (NIST) Information Technology Laboratory (ITL) discussed the risk of information and communications technology (ICT) supply chain attacks in a June, 2015 publication, stating:

> "Without effective security processes and practices throughout the life cycle of a system, intentional and unintentional vulnerabilities can be placed into systems. The systems may then be exploited by attackers who insert malicious content, capture data, or take other advantages, resulting in untrustworthy products or services, unanticipated failure rates, or compromise of federal missions and information."[8]

17. The Office of the Director of National Intelligence agreed, in a 2021 report: "Global trends indicate supply chain risk management is becoming one of the most prevalent areas of cybersecurity vulnerability. The increasing volume and scale of supply chain compromises and rapid advancement of technology makes standardizing a Supply Chain Risk Management (SCRM) practice crucial for organizations to protect against current supply chain threats and prepare for the future."[9]

18. The Department of Commerce (DoC) is similarly aware; in 2021, the DoC's Office of the Inspector General (OIG) stated, in a report on FirstNet Authority's management of security for the Nationwide Public Safety Broadband Network (NPSBN) that "Cyber threats to critical infrastructure, such as the NPSBN, pose a significant risk for 'wide scale or high-consequence events' that could harm or disrupt services essential to U.S. economy, business, and communities." The OIG asked MITRE to assess NPSBN security risks and MITRE concluded "The NPSBN security architecture may be susceptible to supply chain attacks due to FirstNet Authority's inability to validate AT&T's Supply Chain

---

https://www.dni.gov/files/NCSC/documents/supplychain/20200925-NCSC-Supply-Chain-Risk-Management-tri-fold.pdf

[8] https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2015-06.pdf

[9] Office of DNI, April 2021, Annual Threat Assessment of the U.S. Intelligence Community, and Homeland Security, October 2020, Homeland Threat Assessment

Risk Management (SCRM)," because "FirstNet had not performed supply chain risk assessment" for NPSBN since its inception in 2017 and "Consequently...has limited visibility into the NPSBN supply chain and is not fully aware of the level of risk it has taken on."[10]

19. The supply chain threat against computers, computer components, computer networks, and computer-enabled systems and infrastructure is particularly dire, for several reasons. In the first place, the U.S. no longer manufactures the majority of computer chips or hardware it uses. While in 1990 the U.S. manufactured 37% of the world's semiconductors, or computer chips, by 2019 the U.S. made just 12% of world semiconductors and 8% of U.S. computing hardware, and those numbers have continued to fall.[11] Many of the computer chips and hardware in use in the U.S. may be designed in the U.S., but those designed components and devices are then manufactured, tested, integrated and configured mostly overseas, using foreign raw materials and foreign labor, with little to no U.S. government oversight to ensure that no supply chain compromise occurs. The People's Republic of China (PRC), in particular, is estimated to manufacture about 70% of U.S. mobile phones[12] and 90% of the world's personal computers,[13] and the PRC is the primary source for U.S. computer imports.[14] Secondly, the convergence of exponentially-increased computer complexity, power, and miniaturization and the meteoric increase and ubiquity of embedded computers in

---

[10] https://www.oversight.gov/report/DOC/FirstNet-Authority-Must-Increase-Governance-and-Oversight-Ensure-NPSBN-Security

[11] https://www.semiconductors.org/wp-content/uploads/2020/09/Government-Incentives-and-US-Competitiveness-in-Semiconductor-Manufacturing-Sep-2020.pdf

[12] https://www.androidauthority.com/70-percent-us-smartphones-made-in-china-1146888/

[13] https://archive.ph/2i0ur

[14] The U.S. imports three times as many computers from the PRC as the U.S. exports, total, to all countries. https://oec.world/en/profile/bilateral-product/computers/reporter/usa

connected and connectable devices, from smartphones to appliances to industrial control systems to vehicles to wearable electronics ensures that the opportunities for malicious actors to reach and compromise targeted systems and networks proliferate at a scale unmatched *and unmatchable* by U.S. governmental and private industry detection and defensive capability.

20. The supply chain threat for critical computer-based infrastructure is so severe and extensive that the computer networks of the Cybersecurity and Infrastructure Security Agency (CISA), the very U.S. government institution responsible for critical infrastructure security, were compromised by software supply chain attacks in 2020, the SolarWinds SUNBURST[15] and SUPERNOVA[16] attacks, for ten months or more without detection and, even then, that compromise only became known to CISA due to the intervention of a private company.[17] It may be true that CISA successfully defended its own networks and other critical U.S. infrastructure against many, or most attacks, but that possibility is irrelevant under conditions in which a single successful attack means failure or catastrophe. This is the threat environment for computer-based critical infrastructure, and the offense has the advantage- perhaps permanently.

21. In light of CISA's inability to defend even its own computer systems from nation-state-level supply chain attacks from March through December 2020, little credence can be given to CISA's July 2020 declaration that the 2020 election would "be the most secure election in modern history,"[18] and its declaration in November 2020 that the 2020 election was the "most secure in American history."[19] Many public officials and media have repeated and cited those claims as rationale for their own confidence in

---

[15] https://www.cisa.gov/uscert/ncas/alerts/aa20-352a
[16] https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-112a
[17] https://www.mandiant.com/resources/sunburst-additional-technical-details
[18] https://www.meritalk.com/articles/krebs-says-2020-will-be-the-most-secure-election-yet-still-recommends-backup-paper-ballots/
[19] https://www.youtube.com/watch?v=YzBJJ1sxtEA

election security, and for their unwillingness to undertake or support independent investigation.

22. For the public and for public officials such as state and local election officials, to whom much of the computer technology intertwined in the fabric of our society, including carelessly so in our election and voting systems, is sufficiently complex to be incomprehensible, the claims made by officials such as CISA's head and their repetition by trusted institutions and media impede public awareness, and thus, adequate public and governmental response to the supply chain threat.

23. Because the SolarWinds supply chain attack is relatively well-known to the public,[20] it is most unusual and most distinguished from other supply chain attacks by that very fact. Most such attacks are never brought to the public's attention. Other recent significant supply chain attacks largely unknown to the public include the insertion of malware into the software utilities on USB flash drives included with solar electric monitoring devices in widespread use,[21] the insertion of malware into the USB flash drives included with IBM network storage systems,[22] the insertion of keylogger[23] malware into the installation files of personal computer utility software in widespread

---

[20] Not that the public necessarily understands what happened in the attack, but the term "Solarwinds" is familiar enough that members of the public with no computer or cyber expertise may be able to associate the term with "hacking."

[21] https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SESN-2018-236-01+Conext+USB+Malware.pdf&p_Doc_Ref=SESN-2018-236-01

[22] https://www.ibm.com/support/pages/storwize-usb-initialization-tool-may-contain-malicious-code

[23] A keylogger records the keystrokes on victims' computers, and relays the keystrokes to the perpetrators, thereby allowing the perpetrator to, e.g., obtain victim username and passwords and access the victims' sensitive accounts and information. Keyloggers may be introduced through hardware, such as USB device, cable, and keyboard keyloggers, introduced by vendors in the supply chain or by interdiction of shipments.

use,[24] insertion of malicious code in a JavaScript module which was being downloaded by approximately two million victims per week,[25] a series of eight different zero-day vulnerability attacks executed by Chinese hackers against Google, Adobe, and Microsoft services and infrastructure, using 18 different command and control servers,[26] and the reported compromise of U.S. company Super Micro's PRC-manufactured motherboards through covert insertion of hardware during the manufacturing, integration, or shipping phase, affecting U.S. companies including Amazon and Apple,[27] which Super Micro has denied and has denied is possible.[28] Seventeen individuals, including 6 former senior national security officials, have confirmed the Super Micro supply chain compromise occurred, and security researchers have demonstrated it is possible.[29] If true, the Super Micro compromise would have affected not only Amazon and Apple, but dozens of other companies, and potentially U.S. military warships, the Department of Homeland Security, and both houses of Congress.[30]

24. The Super Micro attack reflects an instructive pattern:

a. a U.S. company, products of which are manufactured overseas, in the PRC, and used by other U.S. companies and government agencies;

---

[24] https://blog.avast.com/new-investigations-in-ccleaner-incident-point-to-a-possible-third-stage-that-had-keylogger-capacities

[25] https://www.trendmicro.com/vinfo/dk/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-steal-from-bitcoin-wallets

[26] https://web.archive.org/web/20190717233006/http://www.symantec.com/content/en/us/enterprise/media/ security_response/whitepapers/the-elderwood-project.pdf

[27] https://archive.ph/2i0ur

[28] https://www.cyberscoop.com/supermicro-bloomberg-big-hack-investigation-no-tampering/

[29] https://securityledger.com/2019/01/more-questions-as-expert-recreates-chinese-super-micro-hardware-hack/

[30] https://archive.ph/2i0ur

b. an emerging report that the products may be compromised through supply-chain hardware and/or software insertion attacks;

c. denial by both the company and its customers that any compromise has occurred or is possible, in particular because of the company's and customers' procedural or technical "safeguards;" and

d. independent expert investigation demonstrating that the compromise is possible, or that it has, in fact, occurred.

25. The first public reporting on the alleged Super Micro supply chain compromise was in October, 2018, but the attack itself took place years earlier and was reportedly first detected by a private company and reported to the Federal government in 2015. The Federal government reportedly chose to notify only "a small number of important Supermicro customers."[31] The public, whose data and services and lives and businesses would have been dependent on the integrity of those companies' and institutions' Super Micro-equipped infrastructure, was left vulnerable.

26. Part of the reason for the public's lack of awareness of the severity and pervasiveness of supply chain compromise threats is that malicious cyber activity is commonly portrayed in media as a real-time or near-real-time function of opportunistic "hackers," which are usually presented as some malicious non-governmental organization or individual hobbyist. In fact, the most severe threat posed to computer systems, including all computer-enabled and –embedded systems[32] are nation state-operated or –sponsored advanced persistent threat (APT) groups.

---

[31] https://archive.ph/2i0ur

[32] Most people don't think of a power plant or a passenger aircraft as a computer, but all modern utility-scale power plants and passenger aircraft are, to some extent if not fully, computer-controlled. The threshold at which those become not, e.g. an "airplane with computers" but a "computer which flies" is not clear, but certainly when most or all critical functions for the vehicle, facility, or process are controlled by or must have the reliable operation of computers to function, the facility or vehicle must be

27. MITRE has identified over 120 sophisticated cyber threat groups in unclassified publications, including 18 named and dozens of other probable APTs.[33] There may well be more threat groups, including APTs, identified in classified fora and publications. Publicly known APTs include Iranian, North Korean, and other foreign nations' cyber threat teams, but primarily the APTs are associated with one of two countries: Russia and the PRC, and the number of PRC APTs far exceeds the number of Russian APTs.

28. What distinguishes APTs from the popular cultural portrayal and public misconception of the cyber threat as comprised of real-time/near-real-time "hackers," is that the APTs are organizations composed of multiple, sometimes hundreds or thousands, of state-trained, state-sponsored cyber experts engaged in deliberate years- and decades-long campaigns to not only discover and exploit vulnerabilities in targeted institutions and systems, but to create those vulnerabilities. The APTs are not merely opportunistic actors, finding the occasional misconfiguration which allows access to a system discovered or targeted in real-time, but sophisticated, methodical creators of vulnerability which may employ 25 or more distinct, known attack techniques against a single target,[34] creating novel attacks and tools tailored to their targets or to leverage vulnerabilities they have installed in hardware and software they and affiliates have compromised through supply chain attacks.

29. Mandiant, the same company that discovered and reported the SolarWinds supply-chain attack in 2020, after it had been operating undetected on CISA's networks for ten months, also released a detailed public report in 2013 on the PRC's APT1.

---

considered, for cyber-defensive purposes, to actually BE a computer. In fact, former United States Air Force Chief of Staff, General David Goldfein, has been quoted as describing the F-35, Joint Strike Fighter, as "a computer that happens to fly." https://breakingdefense.com/2018/04/a-computer-that-happens-to-fly-usaf-raf-chiefs-on-multi-domain-future/

[33] https://attack.mitre.org/groups/

[34] https://businessinsights.bitdefender.com/chinese-apt-targeting-asian-government-institutions

Although that report was widely distributed in the cybersecurity community, posted or mentioned tens of thousands of times online, it remains largely unknown to the American public, and likely unknown to most public officials. Mandiant estimated that APT1, also known as Unit 61398 of the PRC's military (People's Liberation Army (PLA)), has manpower in the "hundreds, and perhaps thousands," including human resources functions sufficiently extensive and sophisticated to not only recruit top university graduates in cybersecurity and computer engineering, English linguistics, and software programming, but to groom them through recommended coursework. The report showed APT1, Unit 61398, as part of the PRC military's PLA General Staff Department (GSD) (akin to the U.S. Department of Defense's Joint Staff), occupying a compound that includes a 12-story headquarters, medical clinic, kindergarten, and guesthouses, with technical infrastructure partly equipped by China Telecom[35] for "national defense." APT1 resources include not only cyber operators, but linguists, open source researchers and partnerships with other PLA-controlled Bureaus and with research institutes within the Chinese Academy of Sciences.[36]

30. The 2013 Mandiant report showed APT1 targeting and compromising at least 141 organizations in the U.S. and other English-speaking western nations from 2006 through the end of 2012, including at least 16 organizations in the Information Technology sector, at least six organizations in the High-Tech Electronics sector, and 10 organizations in the Public Administration sector, which APT1 began to focus on in 2009,

---

[35] China Telecom Corp, LTD is a subsidiary of PRC state-owned China Telecommunications Corporation. It is the second largest wireless carrier in the PRC, with more subscribers than the entire U.S. population, and helps implement the PRC CCP's social credit/monitoring/conduct program. CTC was listed and traded on the NYSE and did business in the United States until delisted from the NYSE, prohibited from investment by U.S. entities, and prohibited from doing business in the U.S. in January, 2021, along with 34 other CCP-controlled parent companies and over 1,100 of their subsidiaries, by Executive Order 13959 of President Trump.

[36] http://www.mandiant.com/apt1

after spending at least three years compromising the Information Tech and High-Tech Electronics sectors.[37] The scale of this compromise, from one APT alone, is staggering. Mandiant reported that APT1 stole 6.5 terabytes of compressed intellectual property (IP) data from a single organization in a 10-month period.[38] When that 6.5 terabytes is uncompressed, it is roughly equivalent to the information contained in the 26 million books of the Library of Congress circa 2000.[39] APT1's resources were sufficient to compromise at least 17 new targets in 10 different industries in a single month in 2011. The cyberoperators themselves are not reading all the compromised, exfiltrated data; it is distributed to other APTs, and to state-owned and -controlled research institutes and corporations, to be studied for purposes from vulnerability exploitation to counterfeiting to contractual, political, and financial leverage.

31. One of the other APTs to which APT1 distributes exfiltrated, compromised, stolen IP data from U.S. companies and governmental and non-governmental organizations is APT17, a threat group specializing in supply-chain compromise, run by the PRC's Jinan Bureau of the Chinese Ministry of State Security (MSS).[40]

32. The MSS is responsible for foreign intelligence and counterintelligence operations, but is much more similar to the former Soviet KGB than to the U.S. CIA. Like the KGB and CIA, the MSS collects and analyzes information on foreign adversaries, from both open sources and espionage, and works with its nation's military intelligence services in a two-way exchange of information. Unlike the CIA, but like the KGB, the

---

[37] Ibid.

[38] http://160592857366.free.fr/joe/ebooks/ShareData/A%20Comparitive%20Study%20of%20Text%20Compression%20Algorithms.pdf

[39] https://www2.sims.berkeley.edu/research/projects/how-much-info/how-much-info.pdf#page=110

[40] https://www.cfr.org/cyber-operations/apt-17

MSS is as focused on what the KGB called "active measures,"[41] as on intelligence collection. For example, at the peak of KGB operations in the U.S., which the USSR and KGB had designated the "Main Enemy," the KGB had not only infiltrated and stolen technical and scientific information from the U.S. that enabled the USSR's ultimate development of nuclear weapons, but had also infiltrated the U.S. Departments of Treasury and State, the White House, and U.S. Congress, using those infiltrators to influence and change U.S. foreign and national security policy.[42]

33. The MSS, or its precursor known as the "Ministry of Public Security" (MPS),[43] infiltrated the U.S. Department of the Army during WWII, before the Department of Defense existed, and later the CIA, and some of that infiltration went undetected for four decades, passing critical information to the PRC, e.g. directly affecting Nixon's 1972 rapprochement with the PRC.[44] The Cox Report in 1999 concluded that the PRC, through MSS espionage targeting U.S. national laboratories over an approximately 20 year period, had "obtained at least basic design information on several modern U.S. nuclear reentry vehicles...a variety of U.S. weapon design concepts and weaponization features, including those of the neutron bomb."[45] In 2020, a former CIA officer was arrested for spying for the PRC's MSS from 2001 through 2020, in cooperation with a relative who

---

[41] "Active Measures" include not only disinformation and influence operations, but active subversion of both organizations, societies, governments, and discrete efforts (e.g., the Manhattan Project) to demoralize and undermine identified enemies, but also, importantly, sabotage. https://www.cia.gov/static/79ba0e7b5cfc2541728b7d646353fc13/active-measures-and-information-wars.pdf and "Active Measures, The Secret History of Disinformation and Political Warfare," Thomas Rid, Library of Congress ISBN: 978-0-374-28726-9

[42] https://thescholarship.ecu.edu/bitstream/handle/10342/6426/NCLA%20FSB%20KGB-Final.pdf?sequence=1

[43] "Ministry of Public Security" (MPS), before 1983; now largely separate; MSS merged the Central Investigation Department and MPS' counter-intelligence organization.

[44] https://www.courtlistener.com/opinion/506679/in-the-case-of-united-states-v-larry-wu-tai-chin-united-states-of-america/

[45] https://sgp.fas.org/news/dci042199.html

had been a CIA officer in the 1970s.[46] In each of these cases, the MSS' recruitment and use of infiltrators and technical collection against the U.S. were not discovered until long after the damage to U.S. national security had been done. These publicized incidents are a small subset of the total incidents discovered, and it can reasonably be assumed that discovered incidents are only a portion of total incidents.[47]

34. In 2020, the U.S. Department of Justice indicted five APT41 operatives who helped hack more than 100 U.S. companies, and the FBI was well-aware that the operatives were working for the MSS.[48,49] The FBI's and DOJ's public statements acknowledge APT41's supply chain attacks and association with the MSS.[50]

35. CISA has acknowledged, as early as October 2020, that APTs have targeted not only Federal government, but state, local, tribal, and territorial (SLTT) government, critical infrastructure, and elections organizations, including successful APT establishment of unauthorized access to election support systems.[51] With respect to that unauthorized access to election support systems, CISA stated "...however, CISA has

---

[46] https://www.justice.gov/opa/pr/former-cia-officer-arrested-and-charged-espionage

[47] MSS active measures in the U.S. are not often or deeply covered in U.S. media, and are therefore reduced or non-existent in the public awareness. For example, the MSS is also responsible for the recruitment of Senator Dianne Feinstein's long-time driver as an operative, as well as Fang Fang (aka Christine Fang), who reportedly had a romantic relationship with Representative Eric Swalwell and other government officials in the U.S., and who placed at least one intern in Swalwell's Congressional office.

[48] https://www.justice.gov/opa/press-release/file/1317206/download

[49] https://www.fbi.gov/wanted/cyber/china-mss-guangdong-state-security-department-hackers

[50] The inconsistency of US Government (USG) reporting and warnings on PRC APT groups is of some concern. Although MITRE's ATT&CK database information for APT41, et al, is unambiguous regarding APT41's campaign of supply chain attacks (https://attack.mitre.org/groups/G0096/), contemporaneous CISA alerts in the National Cyber Awareness System make no mention of APT41's supply-chain attack techniques (https://www.cisa.gov/uscert/ncas/alerts/aa22-131a)

[51] https://www.cisa.gov/uscert/ncas/alerts/aa20-283a

no evidence to date that integrity of elections data has been compromised,"[52] but CISA's credibility in their conclusion must be tempered by knowledge that this was during the same period that CISA was unaware that its own networks had been compromised.

36. Mandiant again reported on APT41 activity in March 2022, stating that systems, particularly internet-facing web applications, of at least six U.S. state governments had been attacked and compromised by APT41 over an eight month period in 2021 and 2022.

37. The above discussion covered only a subset of the activity of three of eighteen named APTs acknowledged in unclassified sources, among over 120 named, sophisticated cyber threat groups acknowledged in unclassified sources and engaged, relentlessly, in the development and exploitation of vulnerabilities in western, and particularly U.S., critical and national security systems. It is the tip of the iceberg. In the year 2000, the U.S. was dominant in cyber; now, due to foreign advances in capability, the off shoring of our electronics and computer manufacturing, our monumental expansion of dependence on computers and networked systems, and our naivety with respect to their vulnerability, we are vulnerable beyond comprehension. We face an offensive cyber juggernaut, and supply chain attacks are the most difficult of all threats, often impossible, to detect, prevent, and mitigate.

38. In a May 2022 Alert, CISA advised Managed Service Providers (MSP) and their customers, to mitigate the expected increased targeting of MSPs and their customers by APTs, to enable/improve monitoring and logging processes, enforce multifactor authentication, manage internal architecture risks and segregate internal networks, apply the principle of least privilege, deprecate obsolete accounts and infrastructure, apply updates, backup systems and data, develop and exercise incident response and

---

[52] Ibid.

recovery plans, understand and proactively manage supply chain risk, promote transparency, and manage account authentication and authorization.[53]

39. As applied to computerized voting systems, which fall under CISA's protective mandate, and for which voting system vendors function as MSPs with state and local public officials as "customers," CISA's alert is like advising the ordinary consumer to implement enterprise security policy changes on their personal electronics. Those public officials responsible for the voting systems have little idea what CISA's recommendations mean, and they lack the ability to implement CISA's recommendations. More importantly, the complexity of the devices means that the policy changes at best present a superficial veneer of increased security, like fresh paint over rust. With computerized systems, what is not secure from inception can never be secured.

40. The time-sensitive nature of elections, the exceedingly small windows of time for the public or candidates to gather facts and challenge election results, the strong incentives of public officials and related institutions to dismiss public concerns and queries, and the rarity and delay in public access to voting system monitoring and logging processes means that no satisfactory "incident response and recovery plan" for an election system compromised by a supply chain attack is possible.

41. Arrayed against the offensive cyber threat juggernaut, for elections, is an ecosystem of organizations led by a Federal agency, the U.S. Election Assistance Commission (EAC), the priorities of which are illustrated by the fact that it has devoted its resources to passing out named awards for "Creative and Original 'I Voted'

[53] https://www.cisa.gov/uscert/ncas/alerts/aa22-131a

Stickers,"[54] but has only just now in 2022 pledged to add "Supply chain risk management and security testing" to voting system manufacturer agreements.[55]

42. The NIST is the technical body and agency identified in Title 52, U.S.C.[56] to advise the EAC, and NIST has repeatedly recommended,[57] at least as early as 2012,[58] to secure ICT against supply chain attacks. The EAC, however, has effectively provided no standards, procedures, or safeguards to implement those recommended protections for election systems and elections.[59] Many states use the Federal Election Commission's 2002 Voting System Standards (VSS) as their minimum statutory basis for certification of voting systems, but the VSS doesn't even mention supply chain security.

43. The VSS does not specify standards, procedures, or safeguards to protect election systems and elections against supply chain attacks, stating only that voting system vendors must "Ensure that components provided by external suppliers are free from damage or defect that could make them unsatisfactory for their intended purpose."[60] Nor do the EAC's first successor standards to the VSS, the 2005 Voluntary Voting System Guidelines (VVSG) mention or describe supply chain attack risks, or methods or

---

[54] U.S. Election Assistance Commission Chairman Donald Palmer, presentation "Updates – Colorado County Clerks Association," January 2022, obtained through Colorado Open Records Act.

[55] Ibid.

[56] https://www.law.cornell.edu/uscode/text/52/20971

[57] https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=918801

[58] https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=913338

[59] The EAC actually published a draft "Election Operations Assessment – Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA)" document in December, 2009, but the document was focused on taxonomy and methods of representing attack actions and scope, rather than on actionable mitigation of risk, leading to "recommended controls" for supply chain attack such as "establish chain of custody and system and services acquisition controls."

[60] https://www.eac.gov/sites/default/files/eac_assets/1/28/Voting_System_Standards_Volume_I.pdf

standards for mitigation in election systems.[61] The same is true for the 2015 VVSG Version 1.1. Nearly all certified voting systems in use in the United States have been certified to the 2015 or prior standards; i.e., the voting systems used in U.S. elections have no and have had no supply chain security, nor any testing or verification of that security.

44. U.S. voting methods have careened from manually-hand-counted paper ballots at the precinct-level to increasingly centralized mechanical, electro-mechanical, electronic, and now computer-based and completely computerized voting, with a relentless institutional pressure toward not only computerized, but remote and even mobile computerized voting. All while the institutions intended and required to safeguard and secure elections and elections systems lag further and further behind the event horizon beyond which they can neither understand nor control the technology involved, or the inherent risks in that architecture. An apt comparison would be like watching an organization and system of rules and standards built to regulate horse-drawn carriage safety failing to recognize its anachronism, and failing to adapt, in the face of ubiquitous internal-combustion engine automobile and jet turbine aircraft transportation.

45. The latest version of the VVSG,[62] Version 2.0 approved in February 2021, finally acknowledges supply chain risk management as a necessity, but treats the threat as if it can be mitigated by paperwork, the way vehicle speeds are "limited" by speed limit signs. These standards are barely better than the EAC's non-existent standards for electronic poll books, centralized statewide voter registration systems, and election auditing systems.

---

[61] https://www.eac.gov/sites/default/files/eac_assets/1/28/VVSG.1.0_Volume_1.PDF

[62] https://www.eac.gov/sites/default/files/TestingCertification/Voluntary_Voting_System_Guidelines_Version_2_0.pdf

46. These are the requirements of VVSG 2.0, Section 14.3-A, Supply chain risk management strategy: "The voting system's documentation must contain a supply chain risk management strategy that at minimum includes the following:

1. a reference to the to the template or standard used, if any, to develop the supply chain risk management strategy;
2. the assurance requirements to mitigate supply chain risks
3. the contract language that requires suppliers and partners to provide the appropriate information to meet the assurance requirements of the supply chain risk management strategy;
4. the plan for reviewing and auditing suppliers and partners; and
5. the response and recovery plan for a supply chain risk incident."

47. Accompanying the EAC's VVSG are a published set of "test assertions" for the VVSG, which are meant to translate each VVSG requirement into an unambiguous, specific, testable condition so that the Voting System Testing Lab (VSTL) may verify the conformance of a given voting system to the VVSG standard. Here's what the EAC's VVSG Test Assertions state for supply chain security of voting system components: "2.1.1-A – General build quality, …TA211A-2: IF components from third-party suppliers are used for their intended purpose within the voting system, THEN the voting system manufacturer MUST ensure that third-party suppliers document the quality assurance procedures used to ensure components supplied from third parties are free from damage or defect."[63]

48. The correlating EAC Testing and Certification Program Manuals and VSTL Program Manuals intended to ensure that VSTLs are capable of properly testing voting systems to verify their conformance with VSS and VVSG, and that their tests ensure the security

---

[63] https://www.eac.gov/sites/default/files/TestingCertification/VVSG_2_0_Test_Assertions_1_0.pdf

and integrity of voting systems, do not address supply chain attack threats or their mitigation or their assessment, at all. Instead, the program manuals and certification program requirements reflect an assumption that "commercially available models of general purpose information technology equipment" and "production models of special purpose information technology equipment," and "ancillary devices" can be trusted.[64] Security testing guidelines do not even require VSTLs to review the publicly available common vulnerabilities and exploits (see Appendix 3) associated with commercial hardware and software, and the latest VVSG requires only that: "The underlying system platform generally needs to be free of well-known vulnerabilities before certification, *unless the certification authority allows it*." (emphasis added). "Generally," "unless allowed" is not a standard that can reasonably be assumed to ensure voting system integrity; it is a loophole precisely as large as the standard, itself.

49. Eight years after Mandiant's 2013 report on APT1, six years after the NIST's 2015 warning about supply chain vulnerability and attack, and five years after the Department of Homeland Security declared election infrastructure to be "critical infrastructure" of the U.S.,[65] it is inexplicable that the EAC, responsible for security standards for voting systems, has yet to promulgate standards which reflect the advanced persistent threat against them and their supply chains. The EAC's standards of accreditation for VSTLs do not even ask, let alone require, awareness in the VSTLs of supply chain vulnerabilities in computerized voting systems, much less awareness or proficiency in the detection of supply chain compromises, or in their assessment of effective mitigation, where even possible, by voting system vendors.

50. For those, like myself, with experience in government office or working closely with government agencies in regulated, technically complex domains, the EAC's

---

[64] https://www.eac.gov/voting-equipment/manuals-and-forms

[65] https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

immensely inadequate response is unsurprising and potentially attributable to two phenomena: bureaucracy and regulatory capture. Bureaucracy is merely a fact of life for any government enterprise; except in the most unusual, extraordinary, and rare circumstances, the government, particularly the Federal government, does not adapt well or quickly. Its organizations and agencies are often preoccupied by struggles over autonomy and funding, rather than focused on public interest. Consensus is more important than quality; constituency in power corridors is more important than service. These are truisms for anyone who has worked in or had more than incidental contact with governmental bureaucracy.

51. In this case, because the EAC is intended and authorized to provide a degree of regulation to the election industry, it is subject to and fully entangled in regulatory capture, which is the corruption of a regulatory authority and agency by sympathy toward and influence from the industry it is intended to regulate. In addition to the typical "revolving door" where individuals rotate directly from the election industry or associated non-profits in and out of EAC positions, one need look no further than the EAC's Technical Guidelines Development Committee (TGDC), an advisory body established by HAVA to "assist the (EAC) in the development of (VVSG)." Its fifteen appointed members include far more lawyers, politicians, public affairs, and psychology grads than computer scientists or software experts, at a 4:1 ratio, and those few computer scientists and software experts include, e.g., the director for software development at one of the largest U.S. voting system vendors. The American National Standards Institute (ANSI) representative is a public affairs specialist. The NIST representative and chair is a physicist.[66] This bodes ill for the likelihood of significant or influential cyber technical expertise shaping the technical guidelines for voting system

---

[66] https://www.eac.gov/sites/default/files/tgdc/TGDC_Roster_as_of_October_18_2021.pdf

standards at the EAC and that is evident in TGDC's recommendations. Although the NIST Security and Transparency Subcommittee was recommending to the TGDC that no wireless devices be permitted on voting systems as early as 2006,[67] the TGDC in 2020 still recommended a "compromise position" with no prohibition on wireless devices for the latest, 2021 VVSG.[68] This "compromise" illustrates the pressure placed on a regulatory agency to acquiesce to the regulated industry's preference as opposed to fulfilling its charter, in this case, attempting to ensure the security of computerized voting systems.

52. Permitting wireless devices in computerized voting systems is irrational and indefensible in light of the known and persistent threats to those systems. The Federal government's Security Technical Implementation Guide (STIG), published in 2011, covering wireless systems requires removal of wireless radios from all computers used to transfer, receive, store, or process classified information,[69] stating "simply disabling the transmit capability is an inadequate solution." The fact that wireless capability has been allowed to continue in voting systems and the reasons for that compromise illustrate key effects which characterize and shape government regulation and conduct, broadly, and the security of election and voting systems, specifically. In particular, it is not only that EAC staff and advisors rotate in and out of the elections industry, so that they may develop affinity and sympathy which interfere with their effective action to secure voting systems. It is also that rapid advancement of technology and the inverse

---

[67] https://www.nist.gov/system/files/documents/itl/vote/DraftWhitePaperOnWirelessInVVSG2007-20061120.pdf

[68] https://www.eac.gov/sites/default/files/TestingCertification/VVSG_2_Dispelling_Misinformation.pdf

[69] https://www.stigviewer.com/stig/final_draft_general_wireless_policy/2011-09-30/finding/V-19813

relationship of illiteracy in a domain to capacity to recognize that illiteracy, play a significant role failing to address such threats.

53. For example, in 2013, a computer security consultant presented a practical demonstration using an Android phone application he'd authored to remotely attack and take control of a commercial aircraft in flight, exploiting two common avionics information services, known as Automatic Dependent Surveillance-Broadcast (ADS-B) and Aircraft Communications Addressing and Reporting System (ACARS).[70] Back in 2010, the Federal Aviation Administration (FAA) had mandated that all aircraft, including commercial passenger aircraft, military fighter and transport aircraft, and even Air Force One, employ ADS-B in U.S. airspace.[71] ACARS is not mandated by the FAA, but is one of several aircraft data link systems approved for use in U.S. airspace, which allows operators to access particular airspace planning and operations features, critical for efficient operations.[72] ACARS use by U.S. commercial and military aircraft is widespread.

54. In 2016, the FAA used a joint Government-industry working group to develop recommendations to increase cybersecurity for aircraft systems; among its 30 recommendations was "detecting vulnerabilities in (ADS-B)"—the system that was shown three years earlier to be exploitable to help an attacker to take control of commercial aircraft in flight using a smartphone. Despite the demonstrated vulnerability, and despite the cybersecurity working group's recommendation, the vulnerability was not only not addressed, it was expanded through mandated ADS-B adoption.

55. In 2019, a computer security consultant firm presented their findings of critical exploitable vulnerabilities in the Boeing 787 which could include supply chain attack and

---

[70] https://www.helpnetsecurity.com/2013/04/10/hijacking-airplanes-with-an-android-phone/

[71] https://www.law.cornell.edu/cfr/text/14/91.225

[72] https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_90-117_(E-update).pdf

misuse of aircraft data link systems to take control of an aircraft, in flight.[73] In the same year, the Department of Transportation Inspector General noted that the FAA had still not implemented the ADS-B cybersecurity recommendation discussed above.[74] Despite the FAA having a cybersecurity testing and certification program[75] which is, by all appearances, significantly more capable and comprehensive than the EAC's regime for voting systems, and despite the FAA being well-aware of identified catastrophic cyber risks to in-flight aircraft, the FAA has not implemented the 2016 recommendations regarding ADS-B and aircraft data systems risks. A 2021 Government Accountability Office (GAO) report helps explain why; the FAA's Cybersecurity Steering Committee (CSC) receives technical reports and discusses vulnerabilities, but does not follow up or through.[76] The CSC members, as it turns out, have almost no practical cybersecurity experience, beyond program management and policy recommendations, leaving them unable to adequately assess and address, from a technical perspective, what is a credible and plausible, even urgent threat.[77] In other words, technical illiteracy suppresses recognition of technical risk; people have a blind spot for what they do not understand.

56. The EAC has demonstrated inadequate awareness, comprehension, and response to the clear and present danger posed by foreign nation states' supply chain attacks against the computers and components used in U.S. voting systems. It cannot be relied upon to protect U.S. elections by competently examining voting systems, prior to use,

---

[73] https://i.blackhat.com/USA-19/Wednesday/us-19-Santamarta-Arm-IDA-And-Cross-Check-Reversing-The-787-Core-Network.pdf

[74] https://www.oig.dot.gov/sites/default/files/FAA%20Cybersecurity%20Program%20Final%20Report%5E03.20.19.pdf

[75] https://www.faa.gov/air_traffic/technology/cas/ct/

[76] https://www.gao.gov/assets/gao-21-86.pdf

[77] https://www.linkedin.com/pulse/cybersecurity-aviation-government-where-weve-been-we-today-natke/?trackingId=6iUunn6TTvW5nN23Na%2BjMw%3D%3D

for indicators of compromise and vulnerability. Nor can we rely upon the expertise and professionalism of EAC-accredited VSTLs and their staff, particularly in the absence of adequate EAC standards, to protect U.S. elections by competently examining our voting systems for indicators of supply chain compromise. In federal court testimony in 2020, the Laboratory Director (and corporate principal) for Pro V&V, one of only two accredited VSTLs in the U.S., stated that he had no "specialized expertise in cybersecurity testing or analysis or cybersecurity risk analysis."[78] The EAC accredited a VSTL led by someone with no specialized expertise in cybersecurity testing or analysis or risk analysis.

57. These same VSTLs, with no specialized expertise in cybersecurity testing or analysis or cybersecurity risk analysis, have been responsible to not only conduct initial and modification testing, but to assess proposed engineering change orders (ECO) from voting system vendors, and to recommend to the EAC whether those changes may be implemented without testing, as "de minimis."[79] The EAC has approved at least 150 of these engineering changes to currently certified voting systems. One ECO, representative of many, perfectly epitomizes the inconceivable inadequacy and unsuitability of this approach and the utter ignorance or disregard for cybersecurity risk the approach entails: DVS ECO 100833.[80] DVS ECO 100833 was "analyzed" in April,

---

[78] *Curling v. Raffensperger,* 493 F.Supp.3d 1264, 1277 (N.D. Ga. 2020).

[79] A "De minimis" change, according to the EAC, is a change to a certified voting system's hardware, software, TDP, or data, the nature of which will not materially alter the system's reliability, functionality, capability, or operation. I.e., if a vendor submits a recommended or requested change for approval as a de minimis change, a VSTL then provides analysis and a recommendation to the EAC on whether the change should be approved as a "de minimis" change, and then the EAC approves the request, and the change, as a modification to the certified system configuration which neither invalidates the certification (of conformance with voting system certification standards or guidelines) nor requires additional testing.

[80] https://www.eac.gov/sites/default/files/eoc-documents/ECO%20Analysis%20Form%20100833.pdf

2022, and approved, as recommended by Pro V&V, by the EAC within three days of Pro V&V's recommendation. DVS ECO 100833 affects four different DVS D-Suite EAC-certified versions, and at least 17 different versions certified at the state level, including D-Suite voting systems used in Arizona, California, Georgia, Iowa, Louisiana, Michigan, Missouri, Nevada, New Jersey, New Mexico, New York, Ohio, Pennsylvania, Tennessee, Utah, Virginia, and Washington states.

58. In other words, this ECO affects the voting systems in states which represent over half the population of the U.S. What was the "de minimis" change approved in this ECO? A completely different CPU on the aValue ImageCast X motherboard, and a new Basic Input/Output System (BIOS), which is the firmware that controls basic functions for the CPU, motherboard, and respective computer. In other words, the vendor proposed, the VSTL recommended, and the EAC approved a modification, without testing, to a voting system which involved the complete replacement of what are probably the two most critical, fundamental components which determine the function and security of a computer. This would be like the FAA allowing an aircraft manufacturer to change the wing design and engine design for a passenger aircraft, without additional testing.

59. It is difficult to convey the magnitude of inadequacy of the EAC's guidelines and response to the threat of supply chain attack facing voting and election systems. In order to protect against supply chain attack and compromise for computers and computer components, including software and firmware it is necessary to have qualified experts monitor, without exception or hiatus: the purity of every single material used in your device; the digital design templates and controls for fabrication; the fabrication of every single component, the resulting fabricated components, the assembly of all those components, composed of materials you have verified, according to your design, into a finished product. The same vigilance must be applied to uninterrupted expert monitoring of the finished product itself, including configuration, maintenance, and

updates, including 100% of installed code, for its entire lifecycle from concept through end-of-use. Only then is there even a reasonable chance to secure a system against supply chain attack. And, if all those measures are not vigilantly undertaken, then there is a reasonable chance of an undetected supply chain attack. None of those measures are or have been in place for our voting systems.

60. In comparison, the Department of Commerce Inspector General formally expressed concern that the FirstNet Authority had not conducted a supply chain risk assessment for the NPSBN in its four years of existence. How immeasurable is our risk if the EAC and state governments have not conducted a supply chain risk assessment for U.S. election and voting systems in the 20 years since the EAC was created?

61. What Peter Neumann, Principal Scientist at the Computer Science Laboratory of SRI International, wrote in 1995 seems prescient and still applicable: "Existing standards for designing, testing, certifying and operating computer-based vote-counting systems are inadequate and voluntary, and provide few hard constraints, almost no accountability, and no independent expert evaluations. Vendors can hide behind a mask of secrecy with regard to their proprietary programs and practice, especially in the absence of controls. Poor software engineering is thus easy to hide. Local election officials are typically not sufficiently computer-literate to understand the risks. In many cases, the vendors run the elections. Providing sufficient assurances for computer-based election integrity is an extremely difficult problem. Serious risks will always remain and some elections will be compromised."[81] Neumann wrote that expert assessment before the majority of U.S. computers and computer components were manufactured overseas, and before the threat became so pervasive that nearly 100% of companies had been affected by supply chain attacks.

[81] Peter G. Neumann, "Computer Related Risks," 1995. ISBN: 020155805X.

62. The situation is worse than it first seems. Decades ago, many states had their own voting system examiners, of varying capability. However, most of the voting systems at that time were electro-mechanical or had relatively simple embedded computers. The complexity of modern computer-based voting systems and the relentless advance of cyber threat actor capabilities now demands a skillset for cybersecurity that few, if any, states and localities possess or can afford. Even if states and localities could afford the caliber of cybersecurity expertise needed to defend voting systems, the U.S. workforce of qualified cyber professionals is too small to staff voting systems offices in our 50 states, much less our over 3,000 U.S. counties. A trade organization's annual report shows a cybersecurity workforce gap in the U.S. of 377,000 skilled professionals,[82] and state and county government cybersecurity position salaries typically top out at or below the median starting salaries for the same skillset in the private sector. States and counties are thus exposed to vast unmitigated cybersecurity risk in our election and voting systems.

63. The lack of skilled, qualified expert cybersecurity personnel at state and local government helps explain the insecure state of our nation's centralized statewide voter registration systems. An August, 2020 Center for Election Innovation and Research (CEIR) report, "Voter Registration Database Security (VRDB)," concluded:

a. Only 25 states reported meeting an eight-character password length requirement to access their VRDB.

b. Only 15 states required multi-factor authentication to access their VRDB.

c. Only 27 of 29 responding states "currently conduct systems audits," and many of those states audited their systems less than once per year.[83]

---

[82] https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

[83] The inadequacy of any auditing approach, other than "persistent, constant, and real-time" for an internet-connected device or service cannot be overstated. The SolarWinds

d. Only 26 of 28 responding states reported monitoring both successful and unsuccessful login attempts.

e. Only 19 of 24 states monitored signatures of database injection threats.

f. A Cloudflare Area 1 Security report stated "less than half of America's local election officials use even basic protections to ward off the threat of phishing," and "The federal government has immense resources and capability, but little authority. Local officials...find themselves in the crosshairs of nation-state cyber warfare without the knowledge or tools to fight back...from a cybersecurity perspective this complex system is a cluster[REDACTED] of vulnerability."

64. The futility of "Logic and Accuracy Tests" (LAT) that vendors and government election officials rely upon as a verification and demonstration of voting system security perfectly illustrates the nexus of false assurance, technical illiteracy, and unmitigated risk inherent in our current architecture of technology, procedures, and standards. First instituted when voting machines were mechanical or electro-mechanical, a LAT made perfect sense; when a machine is barely or un-reconfigurable, a simple demonstration with a few repetitions, particularly with prior testing, is sufficient to verify the function of a mechanical system. As the machine becomes more complex, and particularly when the machine is computerized, reconfigurable by code, amenable to covert and

---

SUNBURST software supply-chain compromise malware was deployed in February 2020 on thousands of corporate, institutional, and U.S. government systems, including on networks within the Departments of Defense, Homeland Security, Justice, and Treasury which are monitored in real-time by skilled cyber defenders using intrusion-prevention and –detection tools tuned to their systems and networks. The malware was not detected until 13 December 2020, after nearly 10 months of operation, and even then was not detected by any of those government agencies or their billions of dollars in cyber defense capability. The U.S. Government only, and finally, became aware of SUNBURST because Mandiant's FireEye team detected SUNBURST on their own systems and notified the USG of the attack signature.

undisclosed functions and functionality, and when the tester doesn't even have full access to all available controls on the system under test, a LAT's adequacy diminishes to zero. This is not new information; in 2004, an associate professor of computer science at Rice University stated in his testimony before an Ohio Legislature committee that "while 'logic and accuracy testing' can sometimes detect flaws, it will never be comprehensive; important flaws will always escape any amount of testing."[84]

65. A March, 2022 EAC report underscores this point. Despite certification of the DVS D-Suite 5.5-B voting system by an EAC-accredited VSTL, and despite the "trusted build" procedures recommended by the EAC, and despite the conduct of a LAT by county staff, some precinct-level ImageCast Precinct (ICP) DVS tabulators in Williamson County, TN in an October, 2021 municipal election did not properly tabulate the votes from a large number of ballots, nor include them in the final tally the machines produced.[85] An EAC "investigation," with no independent examiners involved, reported "the direct cause of the anomaly was inconclusive," but also that the system had outdated configuration files ("erroneous code") installed and that post-investigation ECOs for modified ICP software source code "fixed" the problem. Obvious deficiencies in the EAC's report and process include that:

a. There is evidence of the failure of internal controls (e.g., certification, trusted build, LAT), but the EAC has not acknowledged the failures nor initiated the external, independent audit which an internal control failure should trigger;

---

[84] https://votingmachines.procon.org/questions/is-logic-and-accuracy-testing-an-effective-method-of-assuring-that-electronic-voting-machines-are-operating-properly-before-an-election/

[85] https://www.eac.gov/sites/default/files/TestingCertification/EAC_Report_of_Investigation_Dominion_DSuite_5.5_B.pdf

b. The correct election results in Williamson County were finally obtained by rescanning ballots on a central scanner and then verifying the tallies with a hand-count, but the EAC didn't complete its report until over five months after the affected election and didn't notify other users, much less the public, of the problem with the D-Suite 5.5-B (and 5.5-C), so the public should have no confidence in any other election result tabulated on those systems, in any jurisdiction, and also no confidence in the EAC.

c. Had the Williamson County staff not noticed the anomaly, they would have reported inaccurate election results, and only after hand-counting did they have confidence in their results. In other words, no safeguard professed by the EAC or election officials or the election industry functioned properly to prevent or detect the introduction of erroneous code in our computerized voting systems, and the mechanism for producing trustworthy results was a hand-count of paper ballots. If our voting systems were passenger aircraft, they would all be grounded.

66. The fact of that anomaly, the EAC report, and its findings is almost non-existent in any news source, over six months after the election, over a month after the report, and on the precipice of new primary elections, so the American public remains, by-and-large, uninformed regarding the failure of the voting system safeguards and the possibility of erroneous software that would change their election results.

67. It is the same with the declarations of J. Alex Halderman, a professor of computer science at the University of Michigan and a widely-recognized expert on voting system security whose written testimony in the case of Curling v. Raffensperger in the U.S. District Court for the Northern District of Georgia expose a number of critical points[86], including:

[86] https://gaverifiedvoting.org/pdf-litigation/20200819-785_2-Declaration-Alex-Halderman.pdf

a. "The Director of Product Strategy and Security for Dominion Voting Systems does not dispute that its products can be hacked by sufficiently capable adversaries."

b. "Software of the size and complexity of the Dominion code inevitably has exploitable vulnerabilities."

c. "Nation-state attackers often discover and exploit novel vulnerabilities in complex software."

d. "...the Dominion software used in Georgia utilizes a wide range of outdated off-the-shelf software..." and "outdated software components are a security risk because they frequently contain known, publicly documented vulnerabilities"

e. "Malware could potentially be introduced in several ways, including: ...(b) through an attack on the hardware or software supply-chain"

f. "Rigorous post-election audits are necessary in order to reliably prevent attacks that compromise election results by manipulating ballot scanners" and "post-election audits are not sufficient to detect attacks against BMDs, since such attacks could change both the printed and electronic records of the votes."

g. Halderman discovered multiple severe security flaws in Georgia's Dominion Voting Systems which would also affect voting systems in numerous other states, and which, if exploited, would subvert "all procedural protections practiced by the State, including acceptance testing, hash validation, logic and accuracy testing, external firmware validation, and risk-limiting audits (RLAs)."[87]

[87] https://www.documentcloud.org/documents/21038844-20210802-expert-rebuttal-declaration-of-j-alex-halderman

68. Halderman explicitly refers to RLAs as one of the subvertible "procedural protections practiced by states." The election industry is increasingly adopting and promoting RLAs as their preferred approach to verify election accuracy and integrity. The premise of RLAs is that, by comparing a small, randomly-selected sample of the total individual digital cast vote records (CVR) for an election to ballot images and original paper ballots, where available, election officials can *efficiently* confirm, to a degree of statistical confidence, that voting systems correctly tabulated the election results. Paraphrased, RLAs assert "if we find no error in this random sample, then we can assume no error[88] in the total calculation, with X confidence."

69. The concept behind RLA comes from industrial quality control acceptance sampling originated to spot check production bullet quality in World War II. RLAs are attractive to many election officials for their "efficiency," in time and cost, compared to alternative and traditional post-election auditing. Indeed, much of the election industry and many public officials refer to RLAs by the marketing label "gold standard" for post-election audits, even referring to them as "forensic risk-limiting audits," which is deeply misleading. There are profound differences between RLAs and "forensic audits;" see Appendix 5 for a brief comparison.

70. Whatever their "efficiency," RLAs do not offer a panacea for election auditing. Philip Stark, Professor of Statistics at the University of California, Berkeley, and the "father" of the RLA, is a critic of the way RLAs have been oversold through overstated validity, inappropriate application, and non-adherence to required principles stated, "Whitewashing inherently untrustworthy elections by overclaiming what applying RLA procedures to an untrustworthy paper trail can accomplish sets back election integrity.

---

[88] More accurately, "little error," or "too little error to have affected the race/issue outcome."

This is security theater, not election integrity."[89] Professor Stark expressed that opinion in a two-and-a-half page resignation letter from the board of Verified Voting (VV), writing "Instead, we're saying, 'Don't worry: VV will teach you to sprinkle magic RLA dust and fantasies about parallel testing on your untrustworthy election. All will be fine; you can use our authority and reputation to silence your critics.'"

71. The flaws inherent in RLAs as a safeguard for election accuracy and integrity far exceed Stark's concerns. In the first place, RLAs are spot check sampling; even where appropriate for an industrial production process, which elections are not,[90] spot check sampling was always intended as a supplement to a broader quality control plan, not as a substitute for that comprehensive, adequate quality control plan. Second, auditing is an academic and professional discipline with a body of theoretical and philosophical standards, including among seven assumed postulates that: "An audit requires independence and freedom," and "Auditors are skilled judges who are able to measure and compare actual performance against standards of accountability." Neither of these is true of an RLA, which relies upon opaque, untested, uncertified software running on opaque, untested, uncertified hardware, with no transparency to the public, executed by public officials with no independence and no expertise in either auditing or the computer software and hardware involved. RLAs, despite the name, do not satisfy the criteria for audits.

---

[89] https://www.stat.berkeley.edu/~stark/Preprints/vv-resign-19.pdf?utm_source=JangoMail&utm_medium=Email&utm_campaign=Are+all+audits+created+equal%3f+(341331552)&utm_content=

[90] Industrial processes, e.g., manufacturing, often involve machine production and spot check sampling at the batch or lot level to verify manufacturing quality. Those industrial processes are designed to detect error, not deliberate sabotage – the equivalent of fraud in an election. Spot checks provide little chance of detecting sabotage, if the individual saboteur is cognizant of the spot check approach, because the saboteur can avoid sabotaging the spot checked samples, influence the sample selection to avoid sabotaged products, or spoil or change the spot check records.

72. An election audit must be able to do more than check that voting system computers can successfully execute addition for a small subset of ballots cast. The purpose of auditing elections is to satisfy the legal obligations of election officials that elections are free and fair, and to provide a warranted, transparent basis for public confidence that election results accurately reflect the sum of votes cast by eligible voters in a given contest, race, or ballot issue. An adequate audit should confirm or refute each of the following four statements:

a. No ineligible voters' ballots, nor ineligible ballots (e.g., a subsequent, illicit ballot cast from an otherwise eligible voter, or a ballot cast too late to be counted, or without proper credential verifying eligibility) were counted.

b. Each eligible voter's cast ballot was counted, and only once.

c. All legitimate ballots were counted accurately.

d. Tallies for each contest, race, or ballot issue accurately reflect the sum of votes on eligible voters' cast ballots; no more and no less.

73. In other words, election audits must be able to detect fake voters, fake ballots, and fake ballot counts. The adequacy of any audit method is a function of the extent to which the audit method can or cannot confirm or refute those four statements, and the question of efficiency should be a distant consideration, after adequacy to answer the four statements is confirmed. An RLA is completely incapable of detecting fake voters and fake ballots, and is unlikely to detect fake ballot counts, in part because RLAs not only rely upon black-box RLA software and hardware, so that the "randomness" of "random" CVR selections must be in question, but because they rely upon data provided by the voting systems themselves to identify and select CVRs for comparison and are executed without independence, expertise, or access to full forensic evidence.

74. In financial auditing, required of all publicly-traded companies to assure investors and regulators that company financial statements are authentic and accurate, a method like RLA would be considered an "internal control." Internal controls are a management

tool for process monitoring, not a substitute for independent external auditing by skilled experts with full access to all evidence. Regardless of how a recount or a partial recount for post-election audits is conducted, recounting ballots cannot detect fake voters or fake ballots, and is unlikely to detect the sophisticated, complex manipulation possible through supply chain attack.

75. Arizona is one of several states that allow for or require limited hand count post-election audits, under the assumption that they can reduce or eliminate risk of erroneous or fraudulent machine counts for the entire election. Arizona's approach to hand counts entails several inherent weaknesses, from an auditing standpoint. The first, again, is the "spot check" approach to limited sampling, in that Arizona only requires counties to hand count a small subset of ballots from a small subset (2% of precincts or 2 precincts, whichever is greater) of jurisdictions. This means that as many as 98% of precincts are not hand count audited. Since early voting (mail-in and drop box) ballots in Arizona are returned to counties and not precincts, counties must also hand count 1% of the total early ballots cast, or approximately 5,000 early ballots, whichever is less.[91] This means that in Maricopa County, AZ, where only 5,165 early ballots were hand counted out of more than 1.9 million "early votes" cast in 2020, less than three tenths of one percent of the early votes were hand counted in the post election audit.

76. The method of hand counting prescribed by the Arizona Secretary of State's Election Procedures Manual makes that small proportion of hand counting auditing even less valuable. There are two generally-recognized methods of hand counting,

---

[91] https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf

called "Sort-and-Stack,"[92] and "Read-and-Mark,"[93] respectively. The Arizona Secretary of State requires the Sort-and-Stack method. The Sort-and-Stack method is known to be significantly more error-prone than Read-and-Mark, with a mean error rate between 35 percent and 78% greater than Read-and-Mark. When total error, including standard error (or uncertainty in error) is included, Sort-and-Stack can have a total error rate in excess of 2.5 percent.[94] Given this error rate, it is remarkable that Maricopa County's 2020 hand count audit report shows zero differences between the hand count and machine count, for 5,165 early voting ballots.

77. Making matters worse, the Arizona Secretary of State's procedures do not require video recording of hand counting, and prohibit video recording of the ballot content for hand counts, so there is no opportunity for citizens to verify that even those extremely-limited hand counts are accurate. That is, if the hand count post election audit is even conducted; Arizona's procedures allow the county officer in charge of elections to cancel the hand count and use the electronic tabulation of ballots as the

---

[92] Sort-and-Stack is a hand count method which counts one race at a time by placing each ballot to be audited into a stack which corresponds to the vote choice in the race being audited. For example, in a race between Candidate A and Candidate B, there would be one stack for each candidate, comprised of ballots sorted into those stacks. After sorting, the total quantity of ballots in each stack would represent the vote totals for those candidates.

[93] Read-and-Mark is a hand count method which counts a single, multiple, or all races and issues on a ballot by having one or more counters read the marks on the ballot, either simultaneously or in turn, and then mark a tally sheet formatted to show aggregate marks, corresponding to ballot votes, for each candidate.

[94] Stephen N. Goggin, Michael D. Byrne, and Juan E. Gilbert, *Post-Election Auditing: Effects of Procedure and Ballot Type on Manual Counting Accuracy, Efficiency, and Auditor Satisfaction and Confidence*, 11 Election L.J. 36 (2012), *available at* https://www.liebertpub.com/doi/epdf/10.1089/elj.2010.0098.

official count, by simply removing Hand Count Board members until there are too few to conduct the hand count.[95]

78. Numerous independent forensic examination reports mirror Professor Halderman's findings, including reports from Antrim County, MI,[96] and Maricopa County, AZ,[97] and Mesa County, CO,[98,99,100] which all show critical security vulnerabilities, non-compliance with published voting system standards, and anomalies and phenomena attributable to unauthorized and malicious activity, and which demonstrate that existing safeguards for U.S. voting system security are ineffective to detect even simple misconfiguration, much less more complex and sophisticated supply chain attacks of the kind that CISA could not detect in its own networks for ten months or more. The pattern is clear: no one who has asserted that U.S. voting systems are secure has been independent and expert, with access to full forensic evidence; every single independent expert with access to forensic evidence in an election or election system has concluded that the voting systems are not secure.

79. The first four appendices to this Declaration show, respectively, 1) voting systems used in Arizona's five largest counties, by population; 2) ownership of the companies which provide those voting systems; 3) some known, published vulnerabilities of components, mostly software, of those voting systems; and 4) country of manufacture or origin for a representative sampling of computers and computer hardware

---

[95] Arizona Secretary of State, 2019 Elections Procedures Manual, p. 214, available at https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf

[96] https://www.depernolaw.com/all-expert-reports.html

[97] https://www.azsenaterepublicans.com/cyber-ninjas-report

[98] https://useipdotus.files.wordpress.com/2021/09/21.09.21-amended-exhibit-f-ex-f-1-1.pdf

[99] https://useipdotus.files.wordpress.com/2022/03/mesa-county-forensic-report-no.-2.pdf

[100] https://useipdotus.files.wordpress.com/2022/03/mesa-3-report.pdf

components used in those voting systems. These counties represent 6.46 million, or 85%, of Arizona's 7.6 million residents, and include Maricopa, the fourth largest county, by population, in the U.S. The voting systems used in these counties represent three of the top four U.S. voting system vendors, whose voting systems are used to cast and or tabulate over 80% of votes in U.S. elections. The third largest U.S. voting system vendor, not shown in the appendices, is Hart InterCivic; unlike the Dell computers used in ES&S, DVS, and Unisyn voting systems, Hart InterCivic seems to use Hewlett-Packard (HP) computers. It is a difference without distinction, as HP computers are also manufactured and assembled overseas, primarily in the PRC, of overseas-manufactured components, by foreign workers, with no U.S. government oversight and effectively no safeguards in the entirety of the testing and certification regime for voting systems. The voting system vendors all use "Commercial, Off-The-Shelf" (COTS) software with collectively thousands of known vulnerabilities that might be exploited before or after delivery of voting system components.

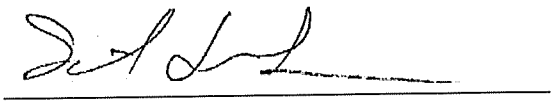
80. If these systems used in Arizona are compromised through supply chain attacks, for which there is ample, undetectable opportunity, then it is reasonable to conclude that U.S. elections are compromised through supply chain attacks. And it is reasonable to conclude that we do not know whether these systems have been compromised. Without access to comprehensive real-time and post-election data, and a cadre of cyber expertise that exceeds U.S. workforce quantity and quality resources, we may never know. This is true not only because supply chain attacks can be extraordinarily difficult to detect,[101] but also because the safeguards inherent in the U.S. voting system testing and certification regime are practically non-existent, and because the nation in which

[101] Supply chain attacks may be impossible to detect in complex computer systems without external validation and real-time data, like trying to determine if a drunk driver crossed over a lane divider on a deserted highway at night, at an undetermined time, without video evidence or telematics from the vehicle or occupant electronic devices.

most of the systems and their components are manufactured and assembled is engaged in a decades-long campaign to infiltrate, corrupt, and compromise western, and especially U.S., computers and computer-based systems, including government and election systems. There is no reason to suspect, much less believe, that Arizona's voting systems have not been compromised by supply chain attack. There is every reason to believe that they would already have been attacked and compromised. Overseas manufacture and supply, without oversight, provides both opportunity and means. The prospect of influencing or controlling U.S. policy provides incentive or motive. There is no effective deterrent. The attack either has happened or will happen.

81. In summary, the complexity, adoption, and connectivity of computers and computer-enabled systems in the U.S. have increased exponentially over the last decade, but the overseas manufacturing, assembly, integration, and configuration of the majority of U.S. computers and computer components, and significant proportions of the software supply chain, including those used in our voting systems, exposes those systems to the advanced persistent threat of massive, well-funded, decades-long nation-state efforts to subvert U.S. national security. Those advanced persistent threats are known to have targeted and penetrated all aspects of the USG, our state governments, defense industry, advanced technology industries, and our election systems, including the principal USG organization responsible to defend election systems against that threat. The American public is largely unaware of the juggernaut of nation-state offensive cyber warfare, including supply chain attacks, arrayed against their voting systems and elections, and due to the categorization of election and voting systems as "critical infrastructure," and the bias of the associated government and non-government institutions against sharing vulnerability and compromise information, our public officials and public are hearing almost exclusively what is simply not true: that our voting systems are both securable and secure.

I declare under penalty of the perjury laws of the United Sates that the foregoing is true and correct and that this declaration was executed this 7th day of June 2022.



Shawn A. Smith

5 Appendices

Appendix 1. Voting Systems of Arizona Largest 5 Counties, by Population

Appendix 2 – Voting System Vendor Ownership

Appendix 3 – Known Voting System Vulnerabilities

Appendix 4 – Country of Manufacture or Origin for Voting System Components

Appendix 5 – Comparison of Risk-Limiting Audit and Full, Independent Forensic Audit

Appendix 1. Voting Systems of Arizona Largest 5 Counties, by Population:

County	Population	Voting System	ePollBook
Maricopa	4.5M	Democracy Suite (D-Suite) 5.5-B Ballot Marking Device (BMD) – ImageCast X (ICX) Optical Scanner (OS) - ImageCast Precinct (ICP) OS – ImageCast Central (ICC) Internet Voting System (UOCAVA) Election Management System (EMS) - EMS	Robis-AskED
Pima	1.05M	ES&S EVS 6.0.4.0 OS - DS850 BMD – ExpressVote Internet Voting System (UOCAVA) EMS - Electionware	Tenex-PrecinctCentral
Pinal	450K	ES&S EVS 6.0.4.0 OS – DS850 BMD – ExpressVote EMS – Electionware Internet Voting System (UOCAVA)	KNOWINK – Poll Pad
Yavapai	242K	Unisyn OpenElect 2.2 Voting System (OVS) BMD - OpenElect Freedom Vote BMD – OpenElect OVI-VC Unisyn – OpenElect 2.2 Internet Voting System (UOCAVA)	ES&S - ExpressPoll

Mohave	218K	EMS- OpenElect Central Suite (OCS) ES&S EVS 6.0.4.0 OS – DS850 BMD – ExpressVote Internet Voting System (UOCAVA) EMS - Electionware	Robis - AskED

Appendix 2 – Voting System Vendor Ownership

Company	Ownership	Notes
Unisyn Voting Solutions	International Lottery & Totalizator Systems (ILTS), Inc (CA) merged w/ILTS (DE) (2014), owned by Berjaya Lottery Management (H.K.) Limited	Berjaya Chairman Vincent Tan has close business ties to Huawei/ZTE and PRC CCP leadership
Election Systems & Software (ES&S)	U.S.*	*Private equity firm McCarthy Group, which does not disclose investors' information, including any other investments or financial interests, owns a controlling interest in ES&S.
Dominion Voting Systems (DVS)	U.S.*	*According to DVS, it is a U.S. company. It was founded in Toronto, by Canadians. Its U.S. patents were mostly filed by Canadians, though they have since been assigned to Dominion Voting

		Systems, Inc., incorporated in the U.S. as branches of a home corporation originally filed in Delaware. Its U.S. trademark registrations are held by Dominion Voting Systems Corporation of Toronto, Canada. Controlling interest was acquired by Staple Street Capital, a private investment firm which does not disclose its investors, in 2018. Dominion, while owned/controlled by Staple Street Capital, collateralized its patents through Hong Kong Shanghai Banking Corporation (HSBC)'s Toronto office in 2019, and UBS Securities LLC, a division of UBS Americas, Inc, under UBS Group AG (Swiss) invested $400M in Staple Street Capital III,

		L.P. in October, 2020, at the same time that UBS AG was allowed by the PRC's Office of Financial Stability and Development Committee and the State Administration of Foreign Exchange to increase its ownership in UBS Securities China from 51 percent to 100 percent.

Appendix 3 – Known Voting System Vulnerabilities

Not a single one of the CVE-listed, known vulnerabilities for hardware and software identified in this appendix were noted or analyzed in any certification testing report for the respective voting systems.

System	Tests/Audits/Examination	Known Vulnerabilities
DVS D-Suite 5.5B		a. Election Management System (EMS) uses Microsoft (MS) Windows Server[102] 2012 R2 Standard – 2,042 vulnerabilities in CVE, 153 in 2022 alone.[103] b. EMS clients use Windows 10 – 2,693 vulnerabilities in CVE, 204 in 2022 alone. c. EMS uses MS .NET framework – over 10 years old – 56 vulnerabilities in CVE since release. d. EMS uses Visual J#, discontinued by MS in 2007, unsupported since 2017, with a single known critical vulnerability in CVE snice 2004.

[102] Windows Server Remote Desktop Gateway vulnerability – pre-authentication, no user interaction, Win Remote Desktop Client Vuln. This was Jan 14, 2020. https://www.cisa.gov/uscert/ncas/alerts/aa20-014a

[103] CVE is Common Vulnerabilities and Exposures, a MITRE database of known computer software and hardware vulnerabilities at https://cve.mitre.org/

e. EMS uses MS Visual C++ 2013 Redistributable, with 28 known vulnerabilities in CVE.

f. EMS uses Java Runtime Environment (JRE) 7 Update 80 and 8 Update 144 – there are 256 known vulnerabilities in JRE published in CVE since 2015.[104] The current version of JRE is 333, and each version update typically addresses security vulnerabilities.

g. EMS uses MS SQL Server 2016 Standard, MS SQL Server 2016 Service Pack (SP) 1, and MS SQL Server 2016 SP1 Express with Advanced Services – with 11 known vulnerabilities in CVE.

h. EMS uses Adobe Reader DC, with 118 known vulnerabilities in CVE.

i. EMS uses MS Access Database Engine 2010, with 8 known vulnerabilities in CVE.

j. EMS uses Open XML SDK 2.0 for MS Office, with 81 known vulnerabilities in CVE.

[104] https://www.oracle.com/java/technologies/javase/8u77-relnotes.html

k. EMS uses NetAdvantage Win Forms 2011 and WPF 2012.1 with 1 known vulnerability in CVE.

l. EMS uses NLog, with one known vulnerability in CVE.

m. EMS uses iTextSharp, with one known vulnerability in CVE.

n. EMS, ImageCast Precinct (ICP), and ImageCast Central (ICC) use OpenSSL, with two known vulnerabilities in CVE.

o. EMS and ImageCast X (ICX) use SQLite, with 46 known vulnerabilities in CVE.

p. EMS uses Lame, with 15 known vulnerabilities in CVE.

q. EMS uses Speex, with two known vulnerabilities in CVE.

r. EMS uses Ghostscript, with 9 known vulnerabilities in CVE.

s. EMS uses Apache Batik, with 6 known vulnerabilities in CVE.

t. EMS uses Apache Avalon, retired by Apache in 2010, and no longer supported for any purpose, including security patches.

	u. EMS uses Apache FOP, with one known vulnerability in CVE. v. EMS and ICX use Entity Framework, with one known vulnerability in CVE. w. ICP uses Zlib, with one known vulnerability in CVE. x. EMS uses Visual Studio 2015, with 24 known vulnerabilities in CVE. y. Adjudication uses MS Enterprise Library, with one known vulnerability in CVE. z. D-Suite uses Dell Optiplex 7440 All In One computers, with one known vulnerability in CVE. Serial HVNRFB2,[105] aa. D-Suite uses Dell servers with iDRAC9, with 15 known firmware vulnerabilities in CVE.
ES&S EVS 6.0.4.0	a. Uses Windows 7 SP1, with over 2,000 known vulnerabilities in CVE.

[105] Dell OptiPlex 7440 All-in-One computers HVNRFB2, HVNQFB2, HVNPFB2, listed as exemplar in the "Test Report for EAC 2005 VVSG Certification Testing Dominion Voting Systems Democracy Suite (D-Suite) Version 5.5-B Voting System," EAC Project Number: DVS-DemSuite5.5-B, Version: Rev. 02, Date: 08/21/2019

	b. Uses Windows Server 2008 R2, with over 2,200 known vulnerabilities in CVE. c. Uses Symantec Endpoint Protection, with 10 known vulnerabilities in CVE. d. Uses OpenSSL, with over 50 known vulnerabilities in CVE. e. Uses Dell Latitude E6430 with one known vulnerability in CVE which allows local users to bypass the Secure Boot protection and gain privileges to write to physical memory. f. Uses Dell Optiplex 5040, 5050, and 7020, with one known vulnerability in CVE which allows local users to conduct EFI flash attacks bypassing BIOS security.
Unisyn OVS 2.2	a. Uses CentOS open source Linux distribution, with over 1,000 known vulnerabilities in the Linux kernel in the last five years in CVE. b. Uses Java JRE, with over 200 known vulnerabilities in the last five years in CVE.

c. Uses Android 4.4.4., with over 100 known vulnerabilities in CVE.

d. Uses Apache-Tomcat, with over 100 known vulnerabilities in CVE.

e. Uses MySQL, with over 100 known vulnerabilities in CVE.

f. Uses OpenSSL, with over 100 known vulnerabilities in CVE.

g. Uses OpenVPN, with over 30 known vulnerabilities in CVE.

Appendix 4 – Country of Manufacture or Origin for Voting System Components

This list is a non-comprehensive, representative sample; the full list of hardware components is hundreds of items long per voting system and requires not only serial numbers, but physical inspection, to verify precise configuration. In many cases, the country of manufacture can be confidently asserted without serial numbers or physical inspection because those components or systems are only manufactured in that location.

System	Component	Notes
DVS D-Suite 5.5B	Dell Optiplex 7440 All-in-One HVNRFB2	- Assembled in Brazil - Motherboard manufactured in China – includes internal mini PCIe slot for wireless card and "Password Jumper" that allows removal or reset of BIOS password - Incorporates Intel Management Engine for out-of-band (non-user/non-local-controlled, remote management) in chipset; labeled as "MEBX, disabled," but Dell confirms that "the ME is not really disabled," and the configuration is controlled by whomever has BIOS access[106]

[106] https://downloads.dell.com/manuals/all-products/esuprt_laptop/esuprt_latitude_laptop/latitude-d630_user%27s%20guide%204_en-us.pdf

DVS D-Suite 5.5B	Dell PowerEdge R630 4Z07T52[107],[108]	- Final assembly in the PRC, Mexico, Brazil, India, or Malaysia[109] - Intel Xeon E5-2623 v3 processor manufactured at Ocotillo plant, Chandler, AZ, which employed over 200 foreign engineers on H1B Visas, including BIOS engineers from PRC[110] - Dell part 4TD8G – DVD+/-RW SATA Internal Drive manufactured in Huizhou, PRC - Dell part 2T9KH – Broadcom 5720 Quad Port 1 GbE Base-T, network interface card – manufactured in PRC

[107] The configuration for 4Z07T52, Dell PowerEdge R630, used as a test article for D-Suite 5.5-B EAC 2005 VVSG Certification Testing, did not incorporate an integrated Dell Remote Access Controller (iDRAC), or UEFI BIOS Boot Mode, or Avocent royalty (enables remove keyboard-video-mouse (KVM)) as part of the vendor (Dell) configuration, but the deployed (in use by U.S. states and counties) D-Suite R630s used for EMS servers frequently are configured with iDRAC, UEFI BIOS Boot Mode, and Avocent royalties (e.g. Dell R630 HMVCVD3, deployed by Dominion Voting Systems in Mesa County, Colorado).

[108] Dell's support site page for 4Z07T52 shows 25 "URGENT" severity driver and firmware updates available for this R630 model.

[109] https://i.dell.com/sites/csdocuments/Corporate_corp-Comm_Documents/en/dell-suppliers.pdf

[110] https://www.myvisajobs.com/GreenCard/SearchLCA.aspx?E=Intel%20Corporation&WC=chandler&CT=China&Y=2015&PN=2

DVD D-Suite 5.5B	Dell PowerEdge R640 JMP9CM2	- Dell part KMCCD – PERC H730 Integrated RAID Controller – manufactured in PRC[111] - Dell part 1R8CR – 16GB RDIMM memory modules, manufactured in either PRC or in South Korea - Dell part R1XFC – Intel i350 Quad Port network interface card – manufactured in Malaysia, with on-board components manufactured in PRC - Dell part 1MW70 – Trusted Platform Module 2.0, manufactured in PRC - Dell part 4TD8G – DVD+/-RW SATA Internal Drive manufactured in Huizhou, PRC.

[111] Dell's FY18 Supply Chain Sustainability Progress Report states that Dell has "nearly 750" Tier 1 suppliers, of which it "has worked with nearly 150...to make certain they use industry best practices to mitigate counterfeit components, tainted software, and intellectual property theft and improve their firmware and software engineering practices and physical site security," and that "the average score for suppliers that completed our program last year improved from 57% with their initial evaluation to 98%." So, 57% of 150 of roughly 750 Dell suppliers (just over 10% of Dell's suppliers) scored well on a supply chain security self-audit in 2017. I.e., nearly 90% of Dell, used almost exclusively by U.S. voting system vendors for U.S. voting systems, suppliers scored poorly on supply chain security self-audit in 2017. https://i.dell.com/sites/doccontent/corporate/corp-comm/en/Documents/ser-report-fy18.pdf?newtab=true

		- Dell part 7H4CN – PERC H730P RAID Controller – manufactured in PRC[112] - Dell part V2KWT – 1.2TB 10K Self-Encrypting Hard-Drive – manufactured in Suzhou, PRC - Dell part 385-BBKS – integrated Dell Remote Access Controller(iDRAC9) – embedded in R640 server motherboard, manufactured in PRC - Dell part VM51C – 16GB RDIMM memory, manufactured in PRC - Dell part CRT1G – R640 motherboard, manufactured in PRC
DVS D-Suite 5.5B	Dell Precision T3420 4TB3MN2	- Dell part 210-AFLH – chassis includes LGA1151 motherboard, manufactured in PRC - Dell part M0VW4 – RDIMM memory, manufactured in Malaysia - Dell part C7F2G – SATA hard drive, manufactured in PRC or Philippines - Dell part PNDVV – DVD/+/-RW optical drive, manufactured in PRC

[112] The PERC H730P RAID Controller incorporates a lithium battery and integrates with iDRAC to allow remote management of equipped servers, including server hard drives, even while the server appears to be powered off. https://i.dell.com/sites/doccontent/shared-content/data-sheets/en/Documents/PowerEdge-RAID-Controller-H730P-Spec-Sheet.pdfCD

DVS D-Suite 5.5B	Dell Optiplex 9030 All-in-One CF73S52	- Dell part GPFNK – Intel Dual-Band 7260 Wi-Fi/Bluetooth wireless networking card, manufactured in PRC - Dell part TKK79 – wireless antenna cable, manufactured in PRC - Dell part 9M9FK – DVD +/-RW optical drive, manufactured in PRC - Dell part C7F2G – SATA hard drive, manufactured in PRC or Philippines - Dell part NWMX1 – RDIMM memory, manufactured in PRC or South Korea
DVS D-Suite 5.5B	Dell PowerConnect 2808 Network Switch 3S2P971	- Manufactured in PRC
ES&S EVS 6.0.4.0.	EMS Standalone Dell 5580 Or E6430	- Manufactured in PRC - Motherboard manufactured in PRC - AC power adapters manufactured in PRC - TPM manufactured in PRC
ES&S EVS 6.0.4.0.	EMS Networked Client Optiplex 5040, 5050, 7020	- Assembled in PRC, Mexico, or Brazil - Motherboard manufactured in PRC
ES&S EVS 6.0.4.0.	EMS Networked Server PowerEdge T420	- Assembled in either PRC or Mexico - Motherboard manufactured in PRC

	PowerEdge T630	- Hard drives, memory modules, I/O ports, power supply all manufactured in PRC - If equipped w/ iDRAC7, manufactured in PRC - If equipped with TPM, manufactured in PRC
ES&S EVS 6.0.4.0.	OpenElect Voting Optical Scan (OVO) system Jetway Motherboard JNF9D-2550	- Manufactured in PRC - Uses NM10 chipset, manufactured in PRC under contract for Intel - Uses Realtek RTL8111EVL[113] PCI-E Gigabit Ethernet ports, manufactured in PRC under contract for Realtek, a Taiwanese company - Uses Fintek F71869A Super IO input/output controller chip, manufactured in PRC under contract for Fintek, a Taiwanese company - Uses PowerVR SGX 545 integrated graphics processor; PowerVR is manufactured in PRC under

[113] The driver files that were employed in the Stuxnet supply-chain attack against Iranian centrifuges at Natanz used a certificate belonging to Realtek Semiconductor: https://web.archive.org/web/20120708081604/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

		contract for Imagination Tech, a UK firm owned by Canyon Bridge Capital, a private equity firm headquartered in the U.S. but funded by PRC government-controlled China State Council.
Unisyn OVS 2.2	OpenElect Voting Central Scan (OVS) Dell Precision laptop or Dell Optiplex desktop computer	- Precision laptop manufactured in PRC - Optiplex desktop manufactured in PRC or Mexico with motherboard manufactured in PRC

Appendix 5 – Comparison of Risk-Limiting Audit and Full, Independent Forensic Audit

Ability of each type of audit to affirm and provide a basis for public confidence that election results accurately reflect the sum of votes cast by eligible voters in a given contest, race, or ballot issue, with respect to the "Four Statements."

	Risk-Limiting Audit (RLA)	Full, Independent Forensic Audit (FIFA)
No ineligible voters' ballots or ineligible ballots counted	Not Answered. 1. Voters are never canvassed to either confirm that voters listed by State as having voted actually voted, or to identify voters whose ballots were cast but not counted. 2. Voter registration rolls demonstrably inaccurate (e.g. hundreds of thousands of mailed-out ballots returned as "undeliverable" by the U.S. Postal Service).	Partially or Fully Answered (depending on extent of canvassing). 1. Voter verification (canvass) of registered voters and of voters listed as having voted in a given election on State records, based upon statistical sampling technique of precincts and counties can provide estimate of roll and voter history accuracy to a selected confidence level, but to eliminate the risk of counting ineligible voters' ballots and the risk of uncounted ballots from eligible voters, a jurisdiction must either vote only in-person with government photo ID and accurate rolls to confirm

		eligibility and identity, or conduct a complete canvass of all registered voters to compare with voting records. 2. Hand-count and forensic examination of ballot envelopes to verify that each counted mail-in ballot has a corresponding human-signed ballot envelope, with signatures verified as authentic by qualified questioned document examiners.
Each eligible cast ballot counted once	Not Answered. 1. RLA has no ability to detect ballots counted multiple times, because so few (as a proportion of total cast and counted) physical ballots are compared to the machine-generated CVRs and to ballot images, and the ballot images and ballots are not compared to one another to identify duplicates.	Fully-answered. 1. Hand-count of 100% of paper ballots with batch tally artifacts. 2. Comparison of hand-count tallies to machine-generated tallies. 3. If hand-count tallies and machine tallies differ, then batch-by-batch comparison to find mismatched batches. Then

2. No conduct of full hand-count to provide basis of comparison.

(RLA perversely becomes less adequate with larger margins of victory, because the statistical approach assumes that fewer ballots need be sampled, rather than recognizing the obvious risk that, if a margin of victory is larger, it may be a function of greater, more-extensive fraud or error.)

hand-recount of mismatched batches. If still mismatched, then comparison of paper ballots to ballot images. Then comparison of ballot images to CVR, and CVRs to reported results.

4. Forensic examination of paper ballots to verify that all counted ballots were marked by a human, vs. machine-marked, and that ballots indicated as mail-in show artifacts of folding. Verification of ballot security measures (watermark, discrete numbering, etc.), for each ballot, if applicable.

(Dependent on validity of either full canvass of registered voters in the audit jurisdiction, or on statistical validity of sampling approach to identify eligible voters whose cast

		ballots were not counted.) Note: some voting system vendors offer a re-tabulation of ballot images produced by their own or other voting system vendors' optical scan tabulation systems; these are inadequate because they never incorporate forensic examination of the paper ballots or comparison of the entirety of paper ballots to the ballot images. It would be like counting potentially counterfeit bills to determine how much authentic currency one held.
All legitimate ballots counted accurately	Partially Answered (being charitable). 1. Secretaries of State establish risk-limit (statistical theory-based percentage likelihood that RLA will not detect that machine-count of ballots was inaccurate, based upon very small sample).	Fully-answered. 1. As described above. 2. In addition, cyber forensic audit of voting machines to verify that only authorized users took only authorized actions on the voting systems, and that no penetration,

2. Secretaries of State tout involvement of "bipartisan election judges" in RLA but, in fact, all the audit boards do is check that the very, very small sample of paper ballots selected by the black-box of Secretary of State-run RLA software/hardware match the CVR. They also allegedly verify the chain-of-custody, but chain-of-custody is lost for both mail-in and drop-box ballots before the counties receive the ballots.

Election officials frequently assert that RLAs "ensure to a high degree of certainty that election outcomes are correct." In fact, at best, an RLA can confirm that an electronic voting machine correctly tabulated the votes on ballots examined, and to some degree of statistical certainty/probability, that the electronic voting machine correctly tabulated the votes on compromise, misuse or error occurred in the voting systems.

	ballots not examined. To the degree that the selection of ballots to be examined is truly random, and to the extent that all types of ballots pose equivalent risk of error or fraud (e.g. from different precincts, scanned on different scanners, or with different settings), and to the extent that there are no mechanisms to circumvent or frustrate random selection of certain ballots, then the statistical assertion may be valid.	
Tallies accurately reflect the sum of votes on eligible voters' cast ballots	Only Partially Answered, as described above.	Fully Answered, as described above.
Auditor Independence	None.	Full.
Auditor Freedom	None. All rules prescribed by Secretaries of State.	Full (dependent on court order, contract, or authorization from governing body of jurisdiction).

Auditor Skill	Variable, but low. Audit boards and election judges involved are trained by Secretaries of State, which are mostly attorneys with no auditing expertise or credentialling; audit boards are effectively under control of election officials in jurisdiction.	Both highly-skilled and insufficiently-skilled are available.
Auditor Standards	None. EAC promulgates no standards and no accreditation for auditing. Among institutions which promote or offer credentialing and continuing education for election officials, RLA is promoted and the issues of conflict of interest, expertise and skill in the audit methods, tools, and evidence, and independence are never raised.	Professional licensure, certification, and credentialing.