CENTER FOR
DEMOCRACY
& TECHNOLOGY

August 14, 2019

U.S. Election Assistance Commission
1335 East West Highway
Silver Spring, MD 20910

Re: Written Comment for Election Security Forum

The current certification model for identifying and addressing software vulnerabilities throughout the lifecycle of election equipment is woefully outdated and needs to be changed immediately. Election system vendors and election administrators are struggling to defend their equipment against substantial threats that exploit the ever-growing number of software vulnerabilities being discovered in *every* product. For example, 1191 vulnerabilities[1] have been reported in the Windows 7 operating system since Microsoft released it in 2009; the most common vulnerabilities allow attackers to run malicious code or access restricted data. Modern cybersecurity models have evolved to depend on the coordinated disclosure of vulnerabilities by researchers, development of security updates by software developers, testing by system vendors, and deployment by system operators. The integrity of election systems will be in an inevitable, yet avoidable, state of insecurity while the status quo of disincentivizing regular software updates remains stuck in 2005.

The EAC requires "manufacturers who wish to implement a proposed *de minimis* change must submit it for VSTL review and endorsement and EAC approval...Software and firmware modifications are not *de minimis* changes.[2]" The reasoning behind the requirement is sound. It is designed to prevent unintended consequences from seemingly innocuous changes. In practice however, this heavily incentivizes vendors to avoid the expensive, time-consuming certification process for what would otherwise be critical updates for other computing products. This is no longer compatible with today's software industry as a result of a dramatic shift in how features and security updates are developed and deployed, where software updates are seen as a regular and important part of defending the cybersecurity of computerized and networked information systems. The consequences are profound for elections operations: for example, election administrators in Pennsylvania have recently procured new equipment with software that will stop receiving security updates shortly after delivery.[3] This should have come as a surprise to *no one*, but should concern *everyone*.

[1] Serkan Özkan, "CVE Details," (August 13, 2019), available at: https://www.cvedetails.com/product/17153/Microsoft-Windows-7.html?vendor_id=26

[2] Election Assistance Commission, "NOC 09-003: Clarification of De Minimis Change Determination Requirements," (September 18, 2009), available at: https://www.eac.gov/assets/1/1/De%20Minimis%20Change%20Determination%20Requirements.pdf

[3] Tami Abdollah, "AP Exclusive: New election systems use vulnerable software", AP News, (July 13, 2019), available at: https://apnews.com/e5e070c31f3c497fa9e6875f426ccde1

All products have a useful lifetime – software is no different. The total cost of software development must take into account that intended useful lifetime. Typically, a business decision is made to stop supporting a product when the cost of support is too high. An example of this is the Microsoft operating system Windows. Versions of Windows have been deployed in numerous sectors, including elections, for decades. The company has taken a systematic approach to supporting its operating system software in a manner that brings new features and security patches to existing versions according to the product's lifecycle policy[4]. Windows 7 has two distinct support periods: mainstream (features & security updates) and extended (security only updates). Each period lasts 5 years, making the total support period 10 years long. Windows 7 mainstream support ended 5 years ago and extended support is scheduled to end January 2020. Despite Microsoft publishing these dates years in advance the election community is struggling to adapt to this reality when security patches are needed most. Keep in mind that even this policy is outdated because Windows 7 is actually 3 versions old and Microsoft has evolved its lifecycle policy to reflect the current, more aggressive, threat environment.

Security patches are the updates that developers use to fix or mitigate vulnerabilities that have been discovered or reported. Sporadic delivery of security updates make it difficult for IT staff to test and deploy the updated software. Microsoft formalized a predictable security update schedule in 2003 that is colloquially known as Patch Tuesday. Updates are released on the second Tuesday of every month in order to give IT staff the opportunity to make an update plan that minimizes system downtime. Malicious actors also know about Microsoft's monthly release cycle, which is why the day *after* Patch Tuesday is informally known as Exploit Wednesday[5]. It speaks to how quickly malicious actors are able to reverse-engineer the security patches in order to uncover and exploit the underlying vulnerabilities that the patch fixes. August 13th was the most recent Patch Tuesday. The update addresses 90 vulnerabilities, which were all classified as either important or critical in severity[6]! Four vulnerabilities related specifically to Remote Desktop Services like those potentially used by vendors and election administrators to remotely access election management systems and voter registration databases[7].

Critical security updates on election systems have been delayed for months or years as a result of the current certification process. As the EAC considers updates to the Voluntary Voting System Guidelines

[4] Microsoft, "Windows lifecycle fact sheet," (August 13, 2019), last updated: June 2019, available at: https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet

[5] Frank Burton, "Simple Tips for Network Sanity: Patch Tuesday, Exploit Wednesday and Uninstall Thursday," Sonicwall, (January 30, 2017), available at: https://blog.sonicwall.com/en-us/2017/01/simple-tips-for-network-sanity/

[6] Greg Wiseman, "Patch Tuesday – August 2019," Rapid7, (August 13, 2019), available at: https://blog.rapid7.com/2019/08/13/patch-tuesday-august-2019/

[7] Benjamin Freed, "Hundreds of Wisconsin elections offices use expired operating systems, official says", StateScoop, (August 12, 2019), available at: https://statescoop.com/hundreds-of-wisconsin-elections-offices-use-expired-operating-systems-election-security-official-says/

(VVSG) the certification process should reflect the modern state of the cybersecurity models that depend on rapidly developing, testing, and deploying security patches. An example of this is Microsoft's updated lifecycle policy for Windows 10 that continues security updates every month, consolidates feature releases to twice a year, and ends support 18 months after release date[8]. This aggressive release and support cycle encourages customers to stay as up-to-date and secure as possible. This is incompatible with the certification process and will result in a much larger cause for concern if VVSG 2.0 expands in scope to apply to additional election system components such as election reporting systems and electronic pollbooks. These components will be at a greater risk of exploitation due to the likelihood that they will have persistent network connections making them susceptible to remote access and service disruption by malicious actors[9]. Election system vendors themselves may face the same threats because their businesses operate using the same software containing the same vulnerabilities.

Vulnerabilities can only be patched if they are discovered and reported. Researchers should be encouraged to participate in securing election systems without fear of going to jail[10]. The only opportunity for independent researchers to examine voting systems is in the Voting Machine Hacking Village at the annual DEF CON security conference[11]. Electronic pollbooks and tabulators were among the equipment compromised in each of the past three years of this event. Researchers were able to install non-election software as a demonstration of their successful unauthorized access[12]. The EAC should facilitate good-faith communication between researchers and election system vendors through vulnerability disclosure programs[13]. The disclosures should also be promptly communicated directly to the jurisdictions that operate affected systems and disseminated to the appropriate Information Sharing and Analysis Centers (ISAC).

The end of support for Windows 7 was the wake-up call that the election community needed to seriously address the outmoded software update process. The EAC should immediately modernize the certification process to reflect the current software development lifecycle that deploys security patches frequently and ends support for old versions sooner. Security researchers should be

[8] Microsoft, "Windows lifecycle fact sheet," (August 13, 2019), last updated: June 2019, available at: https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet

[9] Kim Zetter, "Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials", Vice, (August 8, 2019), available at: https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials

[10] Joseph Lorenzo Hall, "Taking the Pulse of Security Research", (April 10, 2018), available at: https://cdt.org/blog/taking-the-pulse-of-security-research/

[11] Taylor Telford, "Hackers were told to break into U.S. voting machines. They didn't have much trouble.", Washington Post, (August 12, 2019), available at: https://www.washingtonpost.com/business/2019/08/12/def-con-hackers-lawmakers-came-together-tackle-holes-election-security/

[12] https://twitter.com/techvendetta/status/1160605310957973504

[13] United States Justice Department Criminal Division's Cybersecurity Unit, "A Framework for a Vulnerability Disclosure Program for Online Systems", (July 2017), available at: https://www.justice.gov/criminal-ccips/page/file/983996/download

recognized for their important role in securing the election ecosystem by establishing vulnerability disclosure programs that reward good-faith participation. Time is running short to make the changes necessary to upgrade election equipment for the 2020 elections.

Sincerely,

Maurice Turner
Senior Technologist, CDT

Joseph Lorenzo Hall, PhD
Chief Technologist, CDT