UNITED STATES COPYRIGHT OFFICE

Long Comment Regarding a Proposed Exemption Under 17 U.S.C. § 1201

[ ] Check here if multimedia evidence is being provided in connection with this comment

ITEM A. COMMENTER INFORMATION

These comments are provided by Dominion Election Systems ("Dominion"), Election Systems & Software ("ES&S"), and Hart InterCivic ("Hart"), the three largest providers of voting machine and election technology in the United States (the "Election System Providers") through their counsel:

Steven R. Englund
Emily L. Chapuis
JENNER & BLOCK LLP
1099 New York Avenue NW, Suite 900
Washington, D.C. 20016
senglund@jenner.com
echapuis@jenner.com
(202) 639-6000

Dominion is a global provider of end-to-end election tabulation solutions and services. Its history spans more than 100 years – with roots going all the way back to the invention of direct-recording lever machines in 1895. Over the course of the last century, Dominion has developed and deployed numerous generations of election system technology. Dominion's technology is currently used in 33 U.S. states, including more than 2,000 customer jurisdictions. The company also has over 100 municipal customers in Canada, and additional offices and facilities in both the U.S. and Europe.

ES&S is the world's largest elections-only company. For over 40 years, ES&S has provided election equipment, software and services that are used by U.S. municipalities and counties to help them run fair and accurate elections. ES&S's products are used in over 4,500 localities, 42 states and 2 U.S. territories. ES&S's core mission is maintaining voter confidence and enhancing the voting experience. Its ever-evolving technology and systems are designed to fit multiple voter and election law needs, and to help maintain democracy in the jurisdictions it serves.

Hart is a full-service election solutions innovator, which partners with state and local governments to conduct secure, accurate, and reliable elections. For over 100 years, Hart has pursued its mission of advancing democracy one election at a time. The company is dedicated to technological innovation that makes voting more straightforward, more equitable and more accessible – and makes managing elections more transparent, more efficient and easier. Hart products are in use in 18 states, hundreds of counties and thousands of local jurisdictions across the U.S.

The Election System Providers all share a commitment to ensuring democracy by helping state and local election officials run fair and accurate elections. Toward that end, they all share a commitment to providing reliable and secure election systems for use in elections. Each Election System Provider offers products that have been certified as meeting the U.S. Election Assistance Commission's ("EAC") Voluntary Voting System Guidelines ("VVSG"). The EAC is the independent federal agency established under the Help America Vote Act of 2002 ("HAVA")[1] to, among other things, operate the federal government's election system testing and certification program. Certified products are independently tested through a transparent process to ensure that they meet high standards of functionality, accessibility and security.

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 10: Computer Programs—Security Research

ITEM C. OVERVIEW

Providing election software is both a copyright-based business and a public trust. Like other creators of copyrighted works, providers of election software are able to justify their huge investments in technological innovation, as well as in independent testing and certification of their products, because of the protections provided under the Copyright Act. They also rely on those protections, including the prohibition on circumvention in Section 1201, to carefully control access to their products to ensure their security.

Election software serves important public purposes by promoting efficient, accurate and fair elections. Because software is used to manage every aspect of voting, voter registration, and vote tabulation, the security of this software is critical to national security. It is also critical to voters' confidence in the electoral process and to democratic functioning at local, state and federal levels.

During the 2015 triennial proceeding, the Register recommended a new exemption allowing for the circumvention, in certain limited circumstances, of technological protection measures ("TPMs") controlling access to software on three types of devices: medical devices, motorized land vehicles, and – of relevance here – "device[s] or machine[s] primarily designed for use by individual consumers (including voting machines)."[2] Even in recommending this exemption, however, the Register also "recommend[ed] that the Librarian exercise a degree of caution in adopting" it.[3]

[1] Pub. L. No. 107-252, 116 Stat. 1666.
[2] 37 C.F.R. § 201.40(7)(b)(i)(A).
[3] U.S. Copyright Office, Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights 317 (Oct. 2015), https://www.copyright.gov/1201/2015/registers-recommendation.pdf ("Register's 2015 Recommendation").

As both the regulatory language and the underlying record indicate, the Register's consideration of this exemption focused on a broad class of consumer products, and mostly medical devices and motor vehicles. Voting machines fall within the exemption only to the extent that they are "primarily designed for use by individual consumers," and the existing exemption implicates no other election software.[4] This narrow class definition was by design.[5] Cognizant of the significant security risks involved in allowing circumvention with respect to a broader range of software, and based on concerns expressed by several federal agencies, the Office carefully imposed limitations that the proponents now seek to eliminate.

The Register also explicitly distinguished between ordinary consumer products (which fall within the exemption) and critical infrastructure (which does not). In excluding the latter from the exemption, the Register recognized that critical infrastructure – including "highly sensitive systems such as nuclear power plants and air traffic control" – implicates concerns that differ significantly from those raised by consumer-oriented products.[6] Including voting machines in the former category rather than the latter was, from the perspective of the Election System Providers, a curious choice. Voting machines are "use[d] by individual consumers" only in the sense that some consumers vote. Voting machines are procured and owned by state and local governments, which (1) determine the functionality they want in their voting machines based on applicable law, their experience conducting elections, and sometimes testing at the state or local level; (2) maintain, configure, secure and operate those machines; and (3) make them available for voting by eligible voters only on election days (including days of early voting), and only under tightly controlled conditions, including the close supervision of local election judges and poll watchers. Voting machines are not consumer products under any typical conception of that term.[7]

Importantly, while in 2015 the Register specifically sought out advice from the Department of Transportation ("DOT"), the Environmental Protection Agency ("EPA"), and the Food & Drug Administration ("FDA") concerning products under their jurisdiction, it does not appear that she solicited or obtained input from the EAC or state or local election officials.[8] Although the Election

[4] Register's 2015 Recommendation at 317; *see also id.* at 317 n.2170 (explaining that where certain software is used on both consumer devices and industrial ones, "security research into such software would be permitted where it is conducted on a consumer device, but not when it is conducted on an industrial one").

[5] Register's 2015 Recommendation at 317 (narrow class definition is consistent with Congress's intention that the "particular class of works" addressed in § 1201 "be a *narrow and focused subset* of the broad categories of works identified in section 102 of the Copyright Act") (emphasis in original; internal quotation marks and alteration omitted).

[6] Register's 2015 Recommendation at 317.

[7] *See, e.g.*, 15 U.S.C. § 2052(a)(5) ("article . . . produced or distributed (i) for sale to a consumer for use in or around a permanent or temporary household or residence, a school, in recreation, or otherwise, or (ii) for the personal use, consumption or enjoyment of a consumer in or around a permanent or temporary household or residence, a school, in recreation, or otherwise"); 15 U.S.C. § 2301(1) ("tangible personal property which is distributed in commerce and which is normally used for personal, family, or household purposes").

[8] Register's 2015 Recommendation at 312-13.

System Providers question whether the 2015 record, which was largely directed toward typical consumer products, adequately supported creating an exemption for circumvention of voting machine software, they did not oppose renewal of the existing exemptions in the current proceeding.[9] However, the Election System Providers oppose broadening the exemption to encompass any other election software, or by removing reasonable limits on circumvention of voting machine software that the Register found necessary and appropriate in 2015.

The extremely broad class of works to which the proposed expansion would apply is inconsistent with the justification for the initial exemption and the Register's careful effort to construct a focused class and mitigate risks. Indeed, sweeping the full range of election software into the exemption would jeopardize national security. Recognizing the significant national security issues associated with protecting election technology, the Department of Homeland Security ("DHS") designated election systems as "critical infrastructure" in 2017, making protection of such systems "a priority within the National Infrastructure Protection Plan."[10]

The proponents are wrong and misguided in their argument that the Register's allowing independent hackers unfettered access to election software is a necessary – or even appropriate – way to address the national security issues raised by election system security. The federal government already has ways of ensuring election system security through programs conducted by the EAC and DHS. These programs, in combination with testing done in partnership between system providers, independent voting system test labs and election officials, provide a high degree of confidence that election systems are secure and can be used to run fair and accurate elections. Giving anonymous hackers a license to attack critical infrastructure would not serve the public interest. To the contrary, it would create a potential new threat vector for federal, state and local government officials to defend against.

As in the 2015 proceeding, the record in this proceeding is exceedingly thin as to election software, the particular security issues it raises, and the assertedly legitimate activities that the proponents would like to take with respect to election software that are not already permitted under the current exemption. The proponents have failed to meet their burden of proof. As described below, access to election software is tightly controlled by a variety of physical and legal measures. This means that there are practical limitations on hacking of election software that are beyond the scope of this

[9] *See* Exemptions To Permit Circumvention of Access Controls on Copyrighted Works, 82 Fed. Reg. 49,550, 49,555 (Oct. 26, 2017) ("NPRM") ("recommend[ing] renewal of [the good-faith security research] exemption" in its current form); *see also* 37 C.F.R. § 201.40(b)(7). The Election System Providers reserve the right to oppose continuation of the exemption in a future proceeding.

[10] Press Release, U.S. Department of Homeland Security, Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical; *see also* 6 U.S.C. § 132 (authorizing DHS to make critical infrastructure designations); Press Release, White House, Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil ("Secretary of Homeland Security shall . . . coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure").

proceeding, and it is doubtful that there are additional legitimate activities that could be undertaken without infringing the copyrights in election software. Because the proposed exemption is significantly directed to activities that would be infringing with respect to election software, and the statutory factors do not support an expanded exemption, the expansion should be denied as to election software.

ITEM D. TECHNOLOGICAL PROTECTION MEASURE(S) AND METHOD(S) OF CIRCUMVENTION

To promote a functioning democracy and maintain national security, elections and election systems are secured by many layers of protection. These safeguards include protections that copyright owners like the Election System Providers build into their systems and contracts, protections employed by secretaries of state and local election officials, and important DHS and EAC programs.

Election systems include many components. The Election System Providers' products include voting machines, election management software, voter registration software, ballot assembly software, electronic poll book software, tabulation solutions, and absentee voting software. Documentary evidence describing selected components of the Dominion, ES&S and Hart product lines is attached to this comment as Exhibits 1A-1I.

Election system hardware and software is designed to secure such products against threats presented in an election environment. While the details vary from provider to provider and product to product, the Election System Providers' products employ numerous security measures, including ones directed to security of hardware, software and data, as well as logging of relevant activities to make them auditable. Some of those measures constitute technological protection measures ("TPMs") securing access to software within the meaning of Section 1201. These TPMs include measures such as user account and network access authentication, security authentication keys, encryption and authentication of software, encryption and special formatting of data for use in election software, secure media, measures to prevent modification of data outside the intended flow of applications, and intrusion detection monitoring.

The EAC administers an elaborate certification process to ensure that election systems meet high standards of functionality, accessibility and security. Under the auspices of the EAC and the National Institute of Standards and Technology ("NIST"), multiple volumes of the VVSG have been developed through a multi-stakeholder process that has included some of the individuals who are proponents of the exemption.[11] The EAC also runs a transparent certification process that involves rigorous testing of election systems by federally-accredited independent testing

[11] Copies of the standards and information about their development is available at U.S. Election Assistance Commission, Voluntary Voting System Guidelines, https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/ (last visited Feb. 8, 2018).

laboratories.[12] The Election System Providers all offer products that have been certified by the EAC. The independent testing reports regarding these products are publically available.[13]

Like providers of other critical infrastructure software, the Election System Providers control access to election systems through restricted distribution of their products. Unlike consumer products that are readily available for individual consumer purchase, election systems are distributed only to state and local governments for official use in elections. Software is licensed in executable code form only, not sold, and is subject to significant limits on use and redistribution. While the details of the license agreements vary to some extent from company to company, product to product and customer to customer, such licenses are generally limited to use by employees of the relevant governmental entity for limited purposes such as conducting elections in its jurisdiction. Such licenses generally prohibit reverse engineering, redistribution of the software, and transfer or sublicensing of the license.

The foregoing provides only the foundation for election security. Elections in the U.S. are conducted at the state and local levels. State and local officials across some 10,000 U.S. jurisdictions implement comprehensive safeguards to protect their election systems, and those measures reinforce those built into election hardware and software. These measures include physical security for election hardware and computers running election software; network security; procedural safeguards; comprehensive and transparent pre-election testing of ballots, voting machines and tabulation equipment; close supervision of voting by local election officials and poll watchers; paper-based audit trails; strong chain-of-custody requirements for ballots, memory cards and tabulation devices; and legal standards for auditing tabulated results.[14] Voting machines and election management systems are never connected to the Internet, which prevents any attack from a remote location. Access to voting machines and other voting equipment is strictly controlled by local election officials, and at least 33 states have statutes that

[12] Additional information about EAC's certification process is available in the agency's Election System Testing and Certification Program Manual (eff. May 31, 2015), https://www.eac.gov/assets/1/28/Cert.Manual.4.1.15.FINAL.pdf.

[13] U.S. Election Assistance Commission, Certified Voting Systems, https://www.eac.gov/voting-equipment/certified-voting-systems/ (last visited Feb. 8, 2018) ("U.S. Election Assistance Commission, Certified Voting Systems").

[14] *See, e.g.*, National Conference of State Legislatures, Election Security: State Policies, Overview (Dec. 11, 2017), http://www.ncsl.org/research/elections-and-campaigns/election-security-state-policies.aspx (discussing security measures state election officials implement before an election, during an election, after an election and on an ongoing basis to ensure the integrity of the voting process); *see also, e.g.*, Secretary of State of Washington, Elections & Voting: System Security, https://www.sos.wa.gov/elections/system-security.aspx (last visited Feb. 8, 2018); Secretary of State of California, Elections & Voter Information: Voting System Security, http://www.sos.ca.gov/elections/voting-systems/voting-system-approval/ (last visited Feb. 8, 2018).

prohibit tampering with election systems.[15] The proponents and others often overlook these layers of additional security measures that protect election systems.[16]

Finally, DHS and the EAC work with state and local officials to assess vulnerabilities in their election systems, respond to any incidents, mitigate threats, and share information.[17] DHS' efforts in this regard are addressed in further detail in recent congressional testimony by Christopher Krebs of DHS' National Protection and Programs Directorate, which is attached as Exhibit 2.[18] These activities follow from DHS' designation of election systems as part of our nation's critical infrastructure. That designation is given to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[19] The designation of election systems as critical infrastructure means, among other things, that DHS gives requests for assistance within this sector priority over requests regarding non-critical infrastructure.[20] It also means that election-related information shared with DHS is not subject to the same public disclosure requirements as those found in the Freedom of Information Act and similar state statutes.[21] The impact of designating U.S. election systems as critical infrastructure is addressed in further detail in an EAC white paper, which is attached as Exhibit 3.

The DEF CON Voting Machine Hacking Village discussed in the comments of the Center for Democracy & Technology ("CDT") illustrates how tightly voting systems are controlled. DEF

---

[15] National Conference of State Legislatures, State Statutes Prohibiting Tampering with Voting Systems (Dec. 18, 2017), http://www.ncsl.org/research/elections-and-campaigns/state-statutes-prohibiting-tampering-with-voting-systems.aspx.

[16] *See, e.g.*, Matt Blaze et al., *DEF CON 25 Voting Machine Hacking Village, Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure* (Sept. 2017), https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf (failing to account for presence of election officials and other safeguards present in live election context).

[17] *See* U.S. Election Assistance Commission, Starting Point: U.S. Election Systems as Critical Infrastructure, https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf; DHS Cybersecurity Catalog for Election Infrastructure, https://www.eac.gov/assets/1/6/DHS_Cybersecurity_Services_Catalog_for_Election_Infrastructure.pdf

[18] Written Testimony of Christopher Krebs, National Protection and Programs Directorate, U.S. Department of Homeland Security, Before the U.S. House of Representatives, Cybersecurity of Voting Machines (Nov. 29, 2017), https://oversight.house.gov/wp-content/uploads/2017/11/Krebs-NPPD-Statement-Voting-Machines-11-29.pdf.

[19] 42 U.S.C. § 5195c(e).

[20] *See* EAC, Starting Point: U.S. Election Systems as Critical Infrastructure, *supra* note 17.

[21] 6 U.S.C. § 133 (Critical Infrastructure Information Act of 2002, exempting critical infrastructure information from FOIA and other disclosure requirements); *see also* DHS Protected Critical Infrastructure Information (PCII) Program webpage, www.dhs.gov/pcii-program.

CON proclaimed that its voting hackathon was "the first occasion where mainstream hackers were granted unrestricted access to explore and share any discovered vulnerabilities" in the voting machines they examined.[22] The report generated from that event credited the 2015 adoption of the current software security research exemption as enabling the Hacking Village.[23]

But even after adoption of the exemption, DEF CON's ability to obtain voting machines was extremely limited. Organizers were able to acquire only obsolete machines that had been decommissioned, and participants were apparently unable to obtain election software other than firmware on voting machines and one instance of electronic poll book software that had been improperly decommissioned.[24] At a conference, the founder of DEF CON explained that it was able to acquire these products only because of a storm-caused roof collapse at a facility where a county stored its voting machines. The machines were declared a total loss by the county's insurance carrier, which provided them to an electronics recycler (apparently without removing the licensed software), and the recycler then sold them to DEF CON.[25] Such redistribution of election software would violate the terms of the Election System Providers' licenses for their software.

While the organizers of the DEF CON event claim that it involved "good-faith security research" subject to the existing exemption, that characterization is belied by DEF CON's Hacking Village report. The report highlights that the event was a hacker free-for-all in Las Vegas that was open to the public and attended by 25,000 people. Far from serious research, the report specifically distinguishes the event from "academic or industrial settings."[26] The hacking at this event was not conducted in a realistic simulation of a real-world election environment – with its physical security, election judges and poll watchers, audit processes, and chain of custody standards – and so presented a threat environment totally different from the one for which the machines were designed. Hackers attending the conference (many of them anonymous) could examine and attack the displayed voting machines at will and at leisure. Despite the proponents' evident enthusiasm for the event, it confirmed that even in an unrealistic scenario, the old equipment held up pretty

[22] Blaze et al., *supra* note 16, at 4.
[23] Blaze et al., *supra* note 16, at 4.
[24] Blaze et al., *supra* note 16, at 7 ("Most of the equipment in the Village was purchased by DEF CON on secondary market, such as eBay); *id.* at 8 (acknowledging that Voting Village included "only a sample of voting technologies" and that "[o]rganizers obtained what they could get their hand on quickly, legally and affordably"). The "most recently used system" DEF CON organizers were able to acquire was a decommissioned voting machine, which Virginia decertified in 2014. *Id.* at 8. It is not clear, based on the information available, whether the sale of this machine with software on it was in violation of AVS's licensing agreement, although the Voting System Providers expect that it would have been.
[25] Statement of Jeff Moss, Voting Machine Security, C-SPAN (Oct. 10, 2017), https://www.c-span.org/video/?435437-1/def-con-hacking-report-warns-voting-machines-vulnerability (approximately minute 15:50).
[26] Blaze et al., *supra* note 16, at 4.

well against hacking efforts.[27] Because the event involved only obsolete machines, the exercise ultimately proved little more than that old voting machines used old technology. It did not reveal any new vulnerabilities of voting machines or systems, and is not relevant to election systems that are designed using today's technology and for the current threat environment.

The Office should not be misled by the proponents of an expanded exemption into thinking that democracy depends on unbridled hacking of election software. To the contrary, if the Office were to approve of hacking election software in the manner proposed, the integrity of elections could be threatened.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

Section 1201, as modified by the current exemption, does not adversely affect the ability of users of election software to make noninfringing uses of those works, and will not do so over the next three years. However, the proposed expansion of the exemption would promote infringement and could have a substantial adverse effect on the value of election software and the integrity of elections. The proposed expansion should be denied.

Limitations On The Existing Exemption Do Not Cause The Requisite Adverse Effects

As the Register has consistently reiterated, the proponents "bear the burden of establishing that the requirements for granting an exemption have been satisfied."[28] This means that the proponents must prove both that (1) "uses affected by the prohibition on circumvention are or are likely to be noninfringing,"[29] and (2) "as a result of a technological measure controlling access to a copyrighted work, the prohibition is causing, or in the next three years is likely to cause, an adverse impact on those uses."[30] The proponents fail to demonstrate that Section 1201, as modified by the current exemption, is causing sufficient adverse effects with respect to election systems.

(i) Constraints beyond the scope of Section 1201 prevent the activities in which the proponents wish to engage

As an initial matter, limitations on independent efforts to attack election software are *not* primarily caused by Section 1201. Rather, such efforts are primarily limited by physical and legal control over the availability of copies of that software (as opposed to circumvention to access a work in the possession of the user). Those limitations are not effects of Section 1201, and they cannot be addressed in this proceeding.

---

[27] Blaze et al., *supra* note 16, at 11 ("nothing of value was obtained"); *id.* at 12 ("it was difficult to figure out what the contents were"; "no voter identities or similar personal voter data was viable"; "could not get it to boot") ; *id.* at 13 ("this only slowed the device, instead of crashing the main application and potentially allowing further access"; "unit's networking seemed to be well-locked down"; "that was not possible to test").

[28] Register's 2015 Recommendation at 13.

[29] Register's 2015 Recommendation at 15.

[30] Register's 2015 Recommendation at 15.

In this way, election software differs significantly from other classes of works subject to current and proposed exemptions, where copies are readily available through lawful means to persons who might wish to circumvent the access controls on those copies. As described above, election software is distributed *only* to state and local governments, and it is distributed *only* pursuant to licenses designed to maintain the security of this critical infrastructure. The reasons for these limitations are self-evident: making the software used to run U.S. elections more broadly accessible would make it easier for foreign hackers and other bad actors who might want to violate the integrity of the electoral process to plan attacks. These serious national security concerns underscore both the closeness with which this technology is guarded and DHS's designation of election systems as critical infrastructure.

Because of these layers of protection that a would-be hacker would need to overcome before Section 1201 became relevant, it is not surprising that the proponents acknowledge that – even after the adoption of the 2015 exemption – they have had little success in acquiring election software. As the DEF CON report indicates, organizers of that event were only able to purchase a handful of obsolete voting machines. With the exception of some software that apparently was not properly removed from the equipment when it was decommissioned, likely in violation of applicable license agreements, DEF CON was not able to obtain election software. Limitations on distribution are even tighter for election software that does not reside within voting machines.

Outside the system provider's facility, the only place where software such as election management software, voter registration software, ballot assembly software or absentee voting software resides is on computers where local jurisdictions maintain live instances of that software for use in running their elections. Accessing a local government's computer systems without authorization to tamper with or obtain a copy of such software would not only violate the Copyright Act, but in many cases state and federal computer crimes laws like the Computer Fraud and Abuse Act[31] as well.

Similarly, many of the findings that emerged from the DEF CON Voting Machine Hacking Village do not appear to have involved circumvention of TPMs protecting access to copyrighted software. For instance, the report's observations regarding physical security,[32] hardware configuration,[33] old software (hardly a surprise on an old voting machine),[34] and the failure of former owners of the equipment to wipe data when decommissioning the equipment[35] do not appear to have required circumvention of TPMs within the meaning of Section 1201. Thus, the ability to make such observations is not limited by Section 1201 and would not be affected by a broader exemption.

The proponents have failed to identify *any* specific example of good-faith election-related research that both (1) they could obtain the software to perform if their expanded exemption were adopted, and (2) they need the expanded exemption to perform. That failure does not meet proponents' burden of showing an adverse effect caused by Section 1201.

---

[31] 18 U.S.C. § 1030.

[32] Blaze et al., *supra* note 16, at 9 (lock picking, compromising a hinge, uncovered USB ports), 10 (removal of computer chips); *id.* at 13 (use of screwdriver to remove media).

[33] Blaze et al., *supra* note 16, at 11 (configuration of chip); *id.* at 14-15 (foreign-made parts).

[34] Blaze et al., *supra* note 16, at 12, 13.

[35] Blaze et al., *supra* note 16, at 4-5, 12.

(ii) The security of election systems is amply tested under current law

Well before the 2015 triennial proceeding, which created a narrowly tailored exemption for products "primarily designed for use by individual consumers (including voting machines)," election systems were subject to rigorous security testing. The Election System Providers themselves subject their products to stringent security testing at independent, federally-accredited labs under the auspices of the EAC's certification program.[36] Indeed, the Election System Providers' commercial success depends on the security of their products, because that is what their state and local government customers have always demanded, even as technology and the threat environment have changed. Only by providing secure products can the Election System Providers maintain their position in a competitive market for election systems.[37]

The creation of the EAC in 2002 led to additional testing and transparency surrounding election systems. HAVA requires that the EAC certify and decertify election systems, and gives the EAC sole authority to grant certification or withdraw certification at the federal level.[38] The EAC accredits independent testing laboratories that are authorized to test and provide transparent, publically available reports regarding election systems. Providers of election products, including the Election System Providers, allow their products to be tested by these federally-accredited laboratories. Products that meet EAC's stringent security standards are "EAC certified," and state and local election officials normally require products with this certification, along with additional state-level certification testing, in order to ensure the integrity of their elections.[39]

Academic and independent researchers have also conducted research into election systems prior to the 2015 exemption for security research. As CDT admits, "election-related computer and network vulnerabilities have been studied for decades."[40] CDT's comments highlight some of this research, including a 2004 study, two separate 2007 studies commissioned by the states of California and Ohio, a 2009 study, and a 2012 study.[41] Indeed, CDT's comments suggest that the

---

[36] Test reports are available at U.S. Election Assistance Commission, Certified Voting Systems, *supra* note 13.

[37] The proponents' suggestion that "software developers and copyright holders lack adequate incentives to conduct the necessary security research themselves" and may even work to "*conceal* security vulnerabilities rather than fixing them" is both unsupported and untrue, at least as to the Election System Providers. The Election System Providers have every incentive to conduct security research: market demands, the credibility of their organizations, and federal, state and local law all demand sustained attention to preventing, finding and fixing security flaws.

[38] 52 U.S.C. § 20971(a)(1) (EAC to "provide for the testing, certification, de-certification and re-certification of voting system hardware and software by accredited laboratories").

[39] *See* U.S. Election Assistance Commission, Certified Voting Systems, *supra* note 13.

[40] Center for Democracy & Technology, *The Importance of Security Research: Four Case Studies* § 4 (Dec. 2017) § 4, attached to the CDT Comments (hereinafter "CDT Case Studies").

[41] CDT Case Studies § 4.1.

academic world may view past election system research as having largely exhausted the potential to contribute to "fundamental knowledge" through this kind of work.[42]

Waning academic interest in hacking old voting machines raises a substantial question about what noninfringing research purpose is being affected by Section 1201. Entertaining the public at an event billed as a "hacker convention[]"[43] does not seem like the "scholarship[] or research"[44] that Congress meant when it enacted Section 107 of the Copyright Act. Nonetheless, the current Section 1201 exemptions do leave the door open to good-faith security research. Instances of investigation into election systems like the DEF CON event have happened under current law, and the proponents and others have asserted that the current exemption permitted these actions.[45] The permanent security testing exemption in Section 1201(j) also would allow testing of election systems in certain circumstances.[46] Abundant security testing under current law indicates that a broader exemption is not warranted.

(iii) The limitations that the proponents wish to eliminate are not having an adverse effect on legitimate activities

The proponents' proposals to expand the existing exemption fall into two broad categories. First, proponents ask the Office to reconsider its decision to restrict the relevant exemption to enumerated types of devices.[47] As to election systems, that proposal implicates a whole new range of infringing activity, so it is addressed below in the context of infringement. The proponents also urge the Register to eliminate all of the other important limitations she included when recommending the existing security research exemption in 2015.[48] Those limitations reflected a

---

[42] CDT Case Studies § 4.1 (referring to "questions about whether any additional analysis of a voting system above and beyond previous academic treatments would contribute to fundamental knowledge"; noting that "[i]t is difficult to fund and publish academic work without serious contributions to fundamental knowledge").

[43] Frequently asked questions about DEF CON, https://www.defcon.org/html/links/dc-faq/dc-faq.html (last visited Feb. 8, 2018).

[44] 17 U.S.C. § 107.

[45] CDT Case Studies § 4.1; Blaze et al., *supra* note 16, at 7. The CDT comments also discuss two independent security researchers, unaffiliated with any educational institution, who hacked Georgia Kennesaw State's voting infrastructure and were able to download a database with voter registration records, passwords, and software for electronic poll books used on election day. CDT Case Studies § 4.1.

[46] *See* 17 U.S.C. § 1201(j); Register's 2015 Recommendation at 307-09 (finding that permanent exception for security testing in 1201(j) overlaps, in part, with scope of proposed exemption). For example, and setting aside any questions as to whether the particular activities involved might be consistent with applicable license agreements, a researcher working in cooperation with a local government to test the vulnerability of its election-related systems might qualify for Section 1201(j).

[47] *See, e.g.*, Felten and Halderman Comments at 5 (challenging "Device Limitation"); *see also* 37 C.F.R. § 201.40(7)(i)(A)-(C) (limiting exemption to these three categories).

[48] *See, e.g.*, Felten & Halderman Comments at 18-26.

reasoned approach, crafted to account for the concerns of multiple federal agencies as well as those of opponents to the exemption.[49] Applied to election systems, eliminating these limitations would raise serious national security concerns without actually enabling any additional research that should be viewed as legitimate. There are four such limitations that the proponents suggest eliminating. We address each in turn.

Controlled Environment Limitation

First, the proponents oppose the requirement that security research be conducted "in a controlled environment."[50] That proposal is directly at odds with the position *all* participants took in the last proceeding, including some of the same individuals providing comments in this proceeding.[51] As the Register observed in 2015, there was "universal agreement among proponents that testing in 'live' conditions . . . is wholly inappropriate."[52] In light of the views of other agencies and in order to avoid risk to the public, the Register agreed with participants that testing could not be done on "cars being driven on public roads" or on medical devices that might be used by patients. Likewise, the current exemption permits testing on voting machines only to the extent that such devices "are not and will not be used" in elections.[53] Maintaining this limitation – which operates to prevent security testing on election systems, including voting machines, during an election or in advance of their use in an election – is critical to safeguarding the security of voters and the democratic process, and to promoting confidence in the electoral process.

Nothing in the proponents' comments addresses the obvious risks that "live" testing of election systems would create. Rather, proponents simply ask the Register to throw to the wind the caution exercised in the last proceeding, and allow uses such as hacking avionic control systems of aircraft in flight.[54] However, tampering with election systems during an election would undermine the

[49] Register's 2015 Recommendation at 317 (recommending that Librarian exercise "a degree of caution" in adopting exemption); *id.* at 318 ("tak[ing] seriously the concern expressed by other agencies" and imposing limitations on exemption for this reason); *see also* U.S. Copyright Office, Section 1201 of Title 17, A Report of the Register of Copyrights 74 (June 2017), https://www.copyright.gov/policy/1201/section-1201-full-report.pdf ("Section 1201 Report") (noting that "most of the security researchers who petitioned for the [security research] exemption" adopted in 2015 agree that exemption is a useful starting point in striking balance between "better accommodate[ing] a broader range of legitimate security research without compromising copyright's core objectives").

[50] Felten & Halderman Comments at 2, 5; *see id.* at 21-23, 38-39.

[51] *See, e.g.*, Tr, at 139:01-08, 140:12-141:25 (May 26, 2015) (Green) ("I think I speak for all of the security researchers here when I say that [testing on live critical systems] is not something that we endorse"); *id.* 150:16-29 (Blaze) ("[L]et me add my voice to the chorus that condemns tampering with live safety, critical systems. I think nobody—nobody advocates that here."); *see generally* 2015 Bellovin et al. Comments (filed on behalf of proponents Felten & Halderman).

[52] Register's 2015 Recommendation at 318 (noting "consensus" as to this "common-sense" limitation).

[53] Register's 2015 Recommendation at 318.

[54] Felten & Halderman Comments at 22.

democratic principles the proponents profess to uphold and violate the law in many states.[55] Preventing such activity cannot be considered an adverse effect of Section 1201. The controlled environment requirement should not be eliminated.

Existing Laws Limitation

Second, the proponents oppose the requirement that security research "not violate any applicable law."[56] That limitation was a direct response to "concerns raised by opponents [in the 2015 proceeding], as well as DOT, EPA, and FDA."[57] The proponents do not address these concerns or offer any new basis for departing from this position. Elections are highly regulated, and a deeply-rooted principal of U.S. federalism is that "The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof . . . ."[58] As a result, state laws *prescribe* numerous details of how elections are conducted, including in many cases requirements for election systems, and state laws *proscribe* various acts that may interfere with the conduct of fair elections. Accessing election software where it can be found, on the computers of local elections officials, would also in many cases violate computer crimes laws as well. Section 1201's prohibition on circumvention of election system TPMs that would violate these laws is not an adverse effect that should be recognized in this proceeding, and the Register should not place the federal government in the position of appearing to countenance election interference that the states have seen fit to proscribe.[59]

[55] National Conference of State Legislatures, State Statutes Prohibiting Tampering with Voting Systems (Dec. 18, 2017), http://www.ncsl.org/research/elections-and-campaigns/state-statutes-prohibiting-tampering-with-voting-systems.aspx.

[56] Felten & Halderman Comments at 23-24 (quotation marks omitted).

[57] Register's 2015 Recommendation at 318; *see* 37 C.F.R. § 201.40(7)(i) (exemption applies to "[c]omputer programs, whether the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates solely for the purpose of good-faith security research and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986").

[58] U.S. Const., art. 1, § 4.

[59] This conclusion comports with the findings of the recent comprehensive study of the operation of section 1201, which the Copyright Office performed at the Congress's request. *See* Section 1201 Report at 80 (finding that study does not show that "the requirement to comply with other laws impedes legitimate security research" because "other laws still apply even if the activity is permitted under section 1201").

Good-Faith Research Limitation

Third, the proponents oppose the requirement that security research be undertaken "solely for the purpose of good-faith security research," where such research is limited to accessing a computer program "solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability."[60] They say their concern is with limiting "security researchers' broader aims, including teaching, scholarship, and research."[61] But the "scholarship[] and research" the proponents say they want to do sounds an awful lot like the "research" that the current exemption permits. Nothing in the current regulation seems to prohibit teaching based on the results of what was in the first instance good-faith security research, scientific dialogue concerning such research or its results, or academic peer review of such results.

Nonetheless, the proponents propose expanding the exemption to allow circumvention almost without regard to its purpose. For example, in the case of election systems, it would not be in the interests of the United States to open this exemption to a researcher motivated to some extent by a "research" interest but also motivated by a desire to help a foreign adversary interfere in U.S. elections. Because the proponents have not meaningfully identified the uses to which they would open the exemption or explained how those purposes are being unreasonably limited by Section 1201, they have not met their burden of proof with respect to establishing that this requirement causes a sufficient adverse effect.

Coordinated Disclosure Limitation

Finally, the proponents' criticize the requirement that "the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, . . . and is not used or maintained in a manner that facilitates copyright infringement."[62] The principal basis for this criticism seems to be that the word "primarily" might be misread "to mean 'only,'" and thereby limit disclosure of the results of good-faith security research.[63] However, rather than asking the Register to clarify that the word "primarily" means what it says, the proponents ask that this limitation be eliminated entirely.

With respect to election systems, disclosure that is primarily for purposes other than promoting security cannot be justified. The negative consequences of an uncoordinated disclosure of an election-related security vulnerability could be great. In addition to posing significant security risks (including national security risks), disclosure of information regarding vulnerabilities in election software could undermine voter confidence in the accuracy and fairness of the underlying

[60] Felten & Halderman Comments at 2 (quotation marks omitted).
[61] Felten & Halderman Comments at 24.
[62] Felten & Halderman Comments at 25 (quotation marks omitted).
[63] Felten & Halderman Comments at 25-26 ("[A]mbiguity [in the Use Limitation] chills research because researchers know that there is a possibility of liability if the term is read narrowly to exclude related activities like publication of results. This limitation accordingly chills researchers from addressing and publicizing particularly egregious vulnerabilities that are most in need of public disclosure.").

election system and potentially depress voter turnout, affecting the outcome of elections. Limiting disclosures made primarily for purposes of voter suppression is not an adverse effect of Section 1201 that should be recognized in this proceeding.[64]

* * *

Accordingly, the proponents have not met their burden of proving that Section 1201, as modified by the current exemption for software security research, is having a material adverse effect on research with respect to election systems. To the extent that the Register may nonetheless believe that some changes to the current exemption's limitations could be justified with respect to election systems, the Election System Providers encourage the Register to consult with the EAC, DHS and relevant state and local election officials concerning their views on the matter.

The Proposed Additional Uses Are Significantly Infringing

The proposed expansion of the existing software security exemption contemplates uses of copyrighted election software that are in significant respects infringing. The proponents' claims to the contrary largely rehash their arguments in favor of adopting the existing exemption. However, those arguments are beside the point now that the Register has determined to continue the existing exemption.[65] Given that decision, the current stage of this proceeding is focused on whether or not to expand the existing exemption. The Register must now focus on the propriety of the proposed additional uses that would be enabled by an expanded exemption, rather than the propriety of software security research in general.[66]

As explained above, the proposals to expand the existing exemption fall into two broad categories: (1) removing the device limitation to enable circumvention of TPMs with respect to all software, rather than just software used on certain types of devices (e.g. voting machines),[67] and (2) eliminating essentially all of the current exemption's constraints on the circumstances in which

[64] Justifications for free disclosure of security vulnerabilities that focus on alerting consumers to product dangers are not relevant to election systems, because voters do not get a choice of what technology to use at their local polling place.

[65] NPRM, 82 Fed. Reg. at 49555.

[66] NPRM, 82 Fed. Reg. at 49,558 ("In cases where a class proposes to expand an existing exemption, commenters should focus their comments on the legal and evidentiary bases for modifying the exemption, rather than the underlying exemption."); U.S. Copyright Office, Long Form Comment Template ("When commenting on a proposed expansion to an existing exemption, you should focus your comments only on those issues relevant to the proposed expansion."); *see also* Register's 2015 Recommendation at 77 ("agree[ing] with opponents that the record lacks evidence demonstrating a need to expand the current exemption to include uses in fictional e-books or for purposes beyond close analysis of the underlying work, as no examples of such uses were submitted"); *id.* at 99-105 (analyzing proposed expansion of exemption for non-commercial videos).

[67] *See, e.g.*, Felten & Halderman Comments at 5 (challenging "Device Limitation"); *see also* 37 C.F.R. § 201.40(7)(i)(A)-(C) (limiting exemption to these three categories).

security research qualifies for the exemption. Both of these changes contemplate uses of copyrighted election software that are in significant respects infringing.

The first of those changes would extend the exemption to all forms of election software, including election management software, voter registration software, ballot assembly software, electronic poll book software, tabulation software, and absentee voting software – rather than just software controlling voting machines. The Register has previously rejected this type of "open-ended exemption" which would "encompass[] all computer programs on all systems and devices, including highly sensitive systems such as nuclear power plants and air traffic control systems."[68] The Register found that "proponents' arguments . . . focused largely on consumer-oriented software and products" and made no showing that would "justify access to other types of software or systems or explain how such an exemption would work."[69] The proponents in this proceeding do no better than the 2015 proponents. Now, as then, the "particular class of copyrighted works" subject to a Section 1201 exemption should "be a *narrow and focused subset* of the broad categories" of copyrighted works.[70] That principle is important not only because it is what Section 1201 requires, but because focused classes allow the Register to consider in a particularized way the possible adverse effects of Section 1201 with respect to, and the infringing (or noninfringing) status of, a discrete set of works and activities.

With respect to election software, the limits on the current exemption protect national security without unreasonably restraining noninfringing activities. Among other things, the proponents want to eliminate the requirement that security research be conducted on a "lawfully acquired device or machine" without substituting any requirement that the research be conducted with lawfully acquired software.[71] Broadening the exemption to cover all software or copies of software that are not lawfully obtained would result in more infringement. This is because election software is distributed only to state and local governments and only pursuant to licenses that restrict further distribution of the software. The Election System Providers believe that independent security researchers who are not working collaboratively with the provider of the applicable product could not acquire a copy of election software without violating the applicable license.

While the proponents try to minimize their need to make copies of software to carry out security research,[72] their argument rings hollow in the case of election software. Typical license agreements for election software restrict third-party access to the licensed software. Thus, it seems all but certain that someone would have to make an unlicensed copy for a security researcher to be

[68] Register's 2015 Recommendation at 317.
[69] Register's 2015 Recommendation at 317.
[70] Register's 2015 Recommendation at 317 (quoting DMCA legislative history) (emphasis in Register's 2015 Recommendation).
[71] Felten & Halderman Comments at 23-24. Requirements that exemptions be used only with respect to lawfully-acquired copyrighted works have been a staple of past exemptions. *See, e.g.*, 37 C.F.R. § 201.40(b)(1)(i)(A), (ii)(A), (iii)(A), (iv)(A), (v)(A), (vi)(A), (vii), (viii), (2)(i), (4), (5), (6), (8)(i).
[72] Felten & Halderman Comments at 11.

able to work, since it is difficult to imagine a local government permitting a researcher to conduct research on a live system. In the unlikely event that a state or local government would agree to reproduce and distribute such a copy for a researcher in violation of its license, doing so would be a *prima facie* violation of Section 106(1) and (3). Were a researcher himself to download a copy of election software after intruding into a state or local government's computer,[73] that would be a *prima facie* violation of Section 106(1). Running an unauthorized copy of computer software would also implicate the exclusive rights of the copyright owner,[74] as would making any other unauthorized copies of software for purposes of analyzing or testing it.

Section 117 does not immunize such activity. Section 117 requires that the person acting pursuant to it be "the owner of a copy" of the software.[75] Not even the state and local governments that acquire licenses to election software qualify as owners of copies of the software. Unlike providers of software embedded in many garden variety consumer goods, providers of election systems do not sell copies of their software, whether for use on a voting machine or not. Instead Election System Providers license their software pursuant to agreements that "restrict[] the user's ability to transfer the software" and "impose[] notable use restrictions."[76] Often such licenses are time-limited. Thus, even if a state or local government purported to sell *its* copy of election software to a researcher, the researcher could not rely on Section 117 to cover that activity.[77] Moreover, a researcher receiving an infringing copy from a state or local government, or helping itself to one, certainly does not qualify for Section 117.

The uses that would result from circumvention of the TPMs protecting a broader range of election software, or that may be built into infringing copies of election software, are also not fair use. As the Office knows well, a fair use determination requires considering four nonexclusive statutory factors.[78] The first fair use factor, the purpose and character of the use, weighs against the additional uses here. While the Register's 2015 Recommendation viewed favorably the nature of security research involving legitimate copies of consumer products in general, noting that it may involve "academic inquiry," "criticism or comment" or education,[79] there is reason to question that conclusion in the context of a broader exemption. As CDT's comments suggest, the potential to contribute to "fundamental knowledge" through hacking of particular election-related products

[73] Some election software is not used on computers connected to the internet, so copies of that software would have to be removed physically from a local government's facility.
[74] *E.g.*, *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F. 2d 511, 518-19 (9th Cir. 1993).
[75] 17 U.S.C. § 117(a)(1); *see also* Register's 2015 Recommendation at 160.
[76] *Vernor v. Autodesk, Inc.*, 621 F.3d 1102, 1110-11 (9th Cir. 2010). The court's decision in *Krause v. Titleserve, Inc.*, 402 F.3d 119, 124-25 (2d Cir. 2005) is not to the contrary, because the user found there to be the owner of a copy enjoyed considerably broader rights with respect to the software than a local government typically would with respect to licensed election software.
[77] Unless the local government was prepared to part with its copy of the software, the government could not rely on Section 117, because that provision permits distribution only with the owner's original copy and the transfer of all rights in the program. 17 U.S.C. § 117(b). Such transfer would violate the terms of typical election software licenses.
[78] *See* 17 U.S.C. § 107.
[79] Register's 2015 Recommendation at 300.

may be close to exhausted.[80] And without limitations on the environment in which the research is conducted, the lawfulness of the activity (apart from copyright), the purposes of the research, and the use of the research results, the additional activity proposed here is much less connected to these salutary ends. It is difficult to see how copying to advance the interests of a foreign adversary or interfere in a U.S. election could possibly be favored uses under U.S. copyright law, even if the results were publicly disclosed.

It is not transformative for a state or local election official to reproduce and provide to a researcher a complete and unmodified copy of election software in violation of the applicable license. Nor is it transformative for a researcher to download such a copy from a state or local government computer, or to run such a copy in an environment where it performs exactly its intended function. Such activities also are considered commercial uses within the meaning of Section 107, because they involve making copies to obtain a work without paying the customary price.[81] Reproduction and distribution to provide a copy outside the small circle of state and local election officials able to obtain election software in the ordinary course also weighs against a finding of fair use.[82]

The second factor, the nature of the copyrighted work, also runs counter to a finding of fair use. Analysis of an expansion of an existing exemption requires consideration of only the *new* uses proposed. Here, the new uses include circumvention with respect to essentially all software, not just the embedded software in consumer products that was the focus of the Register's 2015 recommendation.[83] That recommendation focused on a finding that such software was "likely to be largely functional in nature."[84] Because the prior analysis of election-related products was limited to "consumer products (including voting machines)," the only election software at play in 2015 was firmware embedded in voting machines.

Here, the relevant class of software is much broader and more varied. Software products such as election management software, voter registration software, ballot assembly software, electronic poll book software, tabulation solutions, and absentee voting software are user-oriented applications with significant functionality, user interfaces and business workflows, and hence much higher expressive content than "software contained in a vehicle's ECU, or software used to control a medical device."[85] Such highly expressive works are entitled to a full measure of copyright protection.

---

[80] CDT Case Studies § 4.1 (referring to "questions about whether any additional analysis of a voting system above and beyond previous academic treatments would contribute to fundamental knowledge"; noting that "[i]t is difficult to fund and publish academic work without serious contributions to fundamental knowledge").

[81] *Sega Enters. Ltd. v. MAPHIA*, 857 F. Supp. 679, 687 (N.D. Cal. 1994).

[82] *See Harper & Row, Inc. v. Nation Enterprises*, 471 U.S. 539, 553-55 (1985) (addressing first publication).

[83] Proponents are wrong that the "nature of the works impacted by this modification petition is the same as the nature of the works proposed in 2015." Felten & Halderman Comments at 15.

[84] Register's 2015 Recommendation at 301.

[85] Register's 2015 Recommendation at 301.

In 2015, the Register found that the third factor, the amount and substantiality of the use, weighed slightly against a finding of fair use because "proposed uses would involve reproduction of copyrighted computer programs in their entirety."[86] This observation is true as to the proposed additional uses as well.

The fourth factor, the effect on the potential market for or value of the work, weighs strongly against a finding a fair use. The proponents acknowledge, as they must, that the Register's analysis of this factor in 2015 hinged on the fact that security research would only be performed on lawfully acquired copies.[87] At the same time, they urge the Register that this requirement need not be codified in the regulations.[88] Obviously, acquiring infringing software without paying the customary price is classic market harm. And removing copyrighted software from the closely-controlled confines of state and local government election offices so that it is accessible to persons unknown to the copyright owner would greatly increase the risk of piracy of such software.

In a similarly contradictory fashion, proponents argue that any market harm "will likely be avoided through coordinated disclosure" with copyright owners, but they also *oppose* regulatory requirements surrounding disclosure. The proponents cannot have it both ways. In the absence of any assurance that the results of "research" will be used for socially-beneficial purposes such as strengthening the security of elections through disclosure to the software provider timed so as to enable correction of any issues found, it must be assumed that such research could be used in ways that would threaten the integrity of elections as well as the market for election software. And while incorporating excerpts of a copyrighted work into a new work of responsible criticism may not be cognizable harm under the fourth factor,[89] obtaining infringing copies to hack copyrighted software and sell information about vulnerabilities to a foreign adversary, or to disrupt an election, or to stir up public fears about the integrity of elections, presents a very different situation. These uses could not excuse obtaining an infringing copy in the first instance, or making an infringing copy in the course of the hacking activities, and could well scare local election officials away from particular products or providers, or even back to hand count systems, to the detriment of the market for election software.

Because all of the statutory fair use factors weigh against a finding of fair use, the additional uses at issue here are infringing.

---

[86] Register's 2015 Recommendation at 301 (noting that proponents conceded that proposed uses would involve reproducing computer programs in their entirety).

[87] Register's 2015 Recommendation at 300-01 (finding that proponents' "security research will not usurp the market for any original works subject to that research, *as they will be lawfully obtaining copies of those works* for analysis") (emphasis added)).

[88] Felten & Halderman Comments at 17 (arguing that reliance on the other law limitation "does not need to be codified by including the 'lawfully acquired' wording that exists in the current exemption").

[89] Register's 2015 Recommendation at 302.

The Statutory Factors Weigh Against An Exemption

The statutory factors set forth in Section 1201(a)(1)(C) require denying the proposed expansion of the security research exemption.

(i) The availability for use of copyrighted works

The proponents provide no reason to think that a broadened exemption would result in greater availability of copyrighted works. To the extent that they address the first statutory factor at all, they simply point to the existing exemption adopted in 2015.[90] But the fact that the Register found that the first statutory factor "slightly favor[ed]" the creation of a limited exemption in 2015 does not mean that this factor favors wholesale expansion of the exemption to allow unfettered access to all election software.[91] In 2015, the Register rejected the conclusory assertion that allowing greater circumvention will necessarily "permit greater 'use' of the TMP-protected works at issue."[92] The "more salient consideration," the Register explained, "is whether there will be greater availability of copyrighted works in general if an exemption" – or here an expansion – "is granted."[93]

Here, there is nothing in the record that indicates that the availability of copyrighted works would somehow increase by allowing testing of election software outside of controlled settings (such as in live elections), or allowing circumvention of such software in contravention of other laws, or for purposes other than good-faith security research and to promote security or safety. However, allowing independent hackers greater access to election software would have a negative effect on the availability of copyrighted works. To the extent that independent research results in

[90] Green Comments at 7 (arguing that the "evidence submitted in support of the Register's conclusions in 2015 remains valid and relevant and the factors continue to favor an exemption"); *see also* Felten & Halderman Comments at 26-27 (noting that "[i]n 2015, the Register found this first statutory factor favors proponents" and reasoning the same must be true with regard to the proposed expansion of this exemption); CDT Comments at 2-4 (no discussion of statutory factors); Consumers Union Comments at 2-4 (no discussion of statutory factors or election systems); Free Software Foundation at 1-2 (same); Rapid7 et al. Comments (same); U.S. Public Policy Council of the Association for Computing Machinery (same).

[91] Significantly, this aspect of the Register's Recommendation was based, in large part, on the finding that opponents in that proceeding had "not established that an exemption would have a negative impact on the availability of copyrighted works." Register's 2015 Recommendation at 310. True as this may be, the Election System Providers note that the 2015 Recommendation was made without the benefit of input from members of the election community, such as the owners of copyrighted products, the government entities that use these products, or the federal agencies involved in their oversight. Commenters respectfully suggest that input from these constituents may have lead the Register to a different conclusion with respect to voting machines. Election systems and software differ meaningfully from the range of other consumer products on which the 2015 record focused. *See* pp. 2-3, 15-16 *supra.*

[92] Register's 2015 Recommendation at 310 (finding that this argument "would seem to prove too much, as presumably the same could be said of any requested exemption").

[93] Register's 2015 Recommendation at 310.

compromised security of any particular election software product, that is likely to affect negatively the market for that particular product and election software in general, particularly if the results are used to compromise or disrupt elections rather than to remedy any issues that may be found. As discussed above, the expansion that the proponents seek needlessly threatens the market for election software, and could ultimately drive officials back to hand count systems.

(ii) The availability for use of works for nonprofit archival, preservation, and educational purposes

The broadened exemption would not increase the availability of election systems for archival, preservation or educational purposes. Class 10 does not target archival or preservation uses. And the proponents fail to connect the proposed expansion to any educational purpose. For instance, the DEF CON Voting Machine Hacking Village was a hacker-free-for-all, untethered to any academic institution or instructional program. Participants were allowed to come and go, and do what they wanted with the available products, in some cases under the cover of anonymity. Regardless of what information may have been uncovered, this exercise has none of the indicia of an educational purpose relevant to this statutory factor.

CDT discusses the history of research into election system security, including work by academics within educational institutions. However, it suggests a decline in academic attention to election systems, because after the publication of initial landmark studies, subsequent studies faced "resistance in academic venues due to questions about whether any additional analysis of a voting system above and beyond previous academic treatments would contribute to fundamental knowledge (the merit criteria for academic work)."[94] And no proponent suggests that any vulnerabilities that a hacker may find in a particular software product are at all likely to find their way into a genuine program of instruction. Thus, there is a significant question whether more hacking of election systems has a material academic component at all. Nonetheless, to the extent it might, there is an existing exemption to enable certain such uses under certain circumstances.

There is certainly no connection between the proposed elimination of the limits on the exemption and use of results in an educational setting. To the contrary, allowing circumvention of election software in contravention of other laws, or for purposes other than good-faith security research and to promote security or safety, seems to reduce any linkage between the circumvention and academic purposes.

(iii) The impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research

The third statutory factor weighs against an expanded exemption for the same reasons the second factor does: the proponents fail to connect the request for a broadened exemption (or the additional uses such an expansion would allow) to criticism, comment, news reporting, teaching, scholarship, or research. To the extent that proponents are worried about ambiguities in the current

[94] CDT Case Studies at 4.1.

exemption,[95] that concern is not justified. The Election System Providers believe the words of the current exemption are reasonably clear, but to the extent the Register may agree that greater clarity would be beneficial, this proceeding provides an opportunity for her to opine on the scope of the exception and its limitations in greater detail. The solution is not to simply throw open the gates to any type of circumvention that a hacker might wish to undertake in the name of "research."

(iv) The effect of circumvention of technological measures on the market for or value of copyrighted works

As discussed in Part E *supra* (with regard to the fourth fair use factor), elimination of limitations on the current exemption would harm the market for election software.

(v) Such other factors the Librarian considers appropriate

Interests in promoting national security, maintaining local control of elections, and safeguarding the democratic process weigh strongly against an expanded exemption as to election software. Congress created the EAC, and DHS designated election systems as critical infrastructure, because American democracy depends on maintaining the security of such systems. The programs conducted by those agencies, in combination with testing done in partnership between system providers and election officials, provide a high degree of confidence that election systems are secure and can be used to run accurate and fair elections.

Moreover, election security is significantly under the control of state and local election officials, who provide multiple layers of election security beyond that built into the election systems they buy and use. Exhibit 4, an issue briefing on cybersecurity by the National Association of Secretaries of States, addresses some of the steps that officials have taken to ensure the security of elections.[96] The Copyright Office should be reluctant to undermine state and local officials' roles in determining controlled use and access to enhance voting system security, particularly now that these systems have been declared critical infrastructure.

While the proponents agree that election systems have national security implications,[97] their vision of how to promote national security is very different from that of the Election System Providers. They ask the Register to give a green light to circumvention of TPMs controlling access to election software and simply trust that individuals with an interest in "research[]" will operate in "good-faith" based on the "norms and customs" of their field, without any meaningful regulatory limits on what they might do or their purposes for doing so.[98] What is more, they do so without identifying *any* specific type of legitimate election system research an expanded exemption would

---

[95] *E.g.*, Felten & Halderman Comments at 2 (referring to "problematic ambiguities"); *id.* at 4 (asking "to remove the ambiguity"); *id.* at 5 ("it is ambiguous"); *id.* at 28 (arguing that "ambiguities in the current exemption" result in "chilling effects [that] inhibit key security research").
[96] National Association of Secretaries of States, Issue Briefing: Securing Future Elections Against Cyber Threats (July 21, 2017).
[97] *E.g.*, Felten & Halderman Comments at 32.
[98] Felten & Halderman Comments at 31-32.

allow them to conduct. The Office should reject the invitation to abandon its well-reasoned approach in favor of the proponents' assurances.

Moreover, the proponents' First Amendment arguments are without merit.[99] Professors Felten and Halderman argue that "the conduct and publication of security research is protected by the First Amendment."[100] To the extent that proponents' suggest that hacking itself is First Amendment protected conduct, such a claim strains credulity. No court has found a First Amendment right to hack election software.[101] Insofar as proponents complain about limits on the disclosure of election security vulnerabilities, these arguments fail as well. Given the strong governmental interest in election integrity and national security more broadly, and in light of the fact that the regulations do not include an outright prohibition on publication, a First Amendment challenge on these grounds would clearly fail under any standard of review.[102] Proponents are wrong that the First Amendment demands that the Register expand the security research exception exactly as they demand and that any lesser accommodation renders Section 1201 unconstitutional.

Just as the Register in 2015 refused to grant an "open-ended exemption . . . encompassing all computer programs on all systems and devices," and specifically referred to "highly sensitive systems such as nuclear power plants and air traffic control systems" as being excluded,[103] the Register should decline to include election system critical infrastructure in any expanded exemption.

DOCUMENTARY EVIDENCE

Exhibit 1 Selected Election System Provider Product Information
- A. Dominion Democracy Suite
- B. Dominion ImageCast Evolution
- C. ES&S Electionware Election Management Software
- D. ES&S Centralpoint Poll Management Software
- E. ES&S PowerProfile Voter Registration System
- F. ES&S Unity 3400 Election Management Software
- G. Hart Verity Election Software

---

[99] *See* Felten & Halderman Comments at 33-34; *see also* Green Comments at 7 (characterizing rulemaking process as a "speech-licensing regime" and arguing that the First Amendment does not permit the Librarian to consider other factors in her discretion).

[100] Felten & Halderman Comments at 33.

[101] The passage from the Register's 2015 Recommendation, which proponents cite, does not support their position. In that Recommendation, the Register explicitly declined to resolve First Amendment claims. *See* Register's 2015 Recommendation at 311. To the extent that she noted that regulations related to security research "may implicate First Amendment concerns," the Register was clear that this concern was limited to regulations of "disclosure of vulnerabilities," not the conduct of hacking. *Id.*

[102] *See Holder v. Humanitarian Law Project*, 561 U.S. 1 (2010) (even under First Amendment strict scrutiny, national security interests justify prohibition on speech).

[103] Register's 2015 Recommendation at 317.

H. Hart Verity Scan
I. Hart Verity Touch Writer

Exhibit 2 Written Testimony of Christopher Krebs, National Protection and Programs Directorate, U.S. Department of Homeland Security, Before the U.S. House of Representatives, Cybersecurity of Voting Machines (Nov. 29, 2017)

Exhibit 3 U.S. Election Assistance Commission, Starting Point: U.S. Election Systems as Critical Infrastructure

Exhibit 4 National Association of Secretaries of States, Issue Briefing: Securing Future Elections Against Cyber Threats (July 21, 2017)

Exhibit 1A

DEMOCRACY SUITE®

Democracy Suite is Dominion's fully integrated voting system solution, and the engine that powers your entire election. This technology platform delivers an improved experience for the voter, long-term sustainability, operational efficiencies, transparency, and cost savings.

EFFICIENT

Dominion developed Democracy Suite with efficiency in mind. From election programming and ballot creation to results consolidation and reporting, your entire election takes place end-to-end out of a single database, making additional third-party tools optional. Democracy Suite has been built to help you streamline your process, increase productivity, and save you time and money.

FLEXIBLE & SCALABLE

Democracy Suite is a highly scalable, flexible system, making it ideal for elections of any size and in any environment. It has been deployed in jurisdictions with as few as 5,000 voters, and in national-level elections with over 50 million voters. Democracy Suite offers a diverse range of voting terminal devices with flexible configurations to meet jurisdictional needs.

SIMPLE

With easy-to-use, intuitive user interfaces across the entire Democracy Suite product line, your staff and poll workers are able to confidently carry out the tasks in their workflow, and your voters have a user-friendly experience. Democracy Suite reduces complexity for your election officials as election event definition and results reporting all take place out of a single, unified database.

SECURE

Security is a big factor when you choose an election solutions provider. Democracy Suite is designed to ensure a high level of security that meets the latest EAC VVSG requirements while maintaining ease of use. The Democracy Suite system also features Dominion's patented, exclusive ballot-level audit trail, AuditMark®, which not only creates a digital image of every ballot cast, but also appends to that image a record of how the voter's intent was interpreted by the voting system. You can rest assured that the integrity of your election data is fully maintained at all times.

SUSTAINABLE

Dominion is committed to producing the highest quality election automation tools and to listening to our customers. Developed from the ground-up as an integrated system, Democracy Suite was created with present and future customer needs in mind. Dominion is listening to the market and focusing on innovative software solutions to deliver secure elections that are sustainable and cost-efficient. As modern technologies evolve, we will continue to innovate.

Exhibit 1B

IMAGECAST® EVOLUTION

THE FIRST ALL-IN-ONE OPTICAL SCAN TABULATOR AND BALLOT MARKING DEVICE

*Dominion's **ImageCast® Evolution** provides both ballot scanning and accessible ballot marking solutions in one universal integrated device.*

VVSG 2005 VER. 1
EAC
CERTIFIED

ImageCast® Evolution Optical Scan Tabulator & Ballot Marking Device: Redefining the Standard for Poll-Based Voting

- Integrated accessible voting - everyone uses the same ballot on the same machine
- Designed for simple, hassle-free election preparation
- 19" touchscreen display for an intuitive user experience
- Can mark and scan ballots up to 22 inches

TO LEARN MORE ABOUT OUR TECHNOLOGY, PEOPLE AND SERVICES
VISIT **DOMINIONVOTING.COM** TODAY

DOMINION VOTING
Our customers come first

STANDARD FEATURES & ADVANTAGES

Easy to use for all

- Intuitive touch screen interface for:
  - Visual ballot review and ballot casting
  - Navigating poll worker and administrative menus
- Accessible, audio-visual ballot marking interface, supporting a range of assistive input devices, including an ATI (Audio-Tactile Interface), sip & puff, or paddles

STANDARD FEATURES

- High resolution scanning technology
- Automatic detection of fraudulent ballots
- Ultrasonic multi-feed detector that prevents the device from accepting more than one ballot at a time
- Ballot scanning and tabulation, ballot review and second chance voting, as well as ballot marking functionality - all in one device to allow "no-touch" accessible voting
- Dual, removable commercial memory cards for redundancy
- Internal diverter for simplified ballot sorting
- Patented AuditMark® image technology

VVSG 2005 VER. 1 EAC CERTIFIED

DOMINION IMAGECAST® VOTING EVOLUTION

DEMOCRACY SUITE®

BENEFITS

Dominion has invested in the development of proprietary technology that truly sets its products apart from the competition. Focusing on two key aspects of the electoral process **– risk-limiting auditing and voter intent –** *Dominion's technology improves the transparency and integrity of the election process.*

- **AuditMark® technology:** Each digital ballot image has an AuditMark® appended at the bottom, showing a record of how that ballot was interpreted by the tabulator on Election Day. Why bother purchasing a scanner if it can't tell you what it read?
- **Marginal Mark detection:** This feature makes it possible for voters to clarify their intent when they cast their ballot. Thresholds can be configured to jurisdictional requirements.
- **Complete end-to-end system auditability:** Every action taken on the tabulator and the election management system is recorded in a permanent, unalterable digital log.
- **Engineered simplicity:** Dominion's voting systems are designed to be easy-to-use for voters, poll workers and election officials.

STATE OF THE ART INNOVATION & INTEGRATION

VVSG 2005 + TABULATOR + BMD

WHAT YOU NEED, WE DELIVER

EXPERTISE

Dominion team members are leaders in the industry in project management services and support for voting system implementations. With nearly 200 professional staff - including 60 individuals dedicated to Customer Service & Delivery - **and over 2,000 years in combined elections experience,** Dominion has the expertise to deliver on all your election needs.

EXPERIENCE

Dominion staff leverage their broad implementation experience with Dominion, Sequoia as well as Premier/Diebold product lines to deliver the best professional services in the industry. This cornerstone in project management has been the key to the success of voting system implementations ranging in scale from large statewide projects to small scale election events. **As a Dominion customer, you know you can rely on Dominion's state-of-the-art technology, vast engineering resources and expertise** - all of which are mobilized to ensure that your needs, and those of your voters, are fully met.

DOMINION CUSTOMER SERVICE & SUPPORT

- Planning & Scheduling
- Overall Change Control Process
- Project Scope Management
- Resource Planning
- Quality Control
- Risk Management
- Resource Management
- Equipment Procurement & Deployment
- Customer Interface & Communications
- Training Management

STATE-OF-THE-ART TECHNOLOGY, EXPERTISE & EXPERIENCE.
DEDICATED TO MAKING YOUR ELECTION A SUCCESS.

Newest Members of the ImageCast® Evolution Family:

- Monroe County, *Florida*
- Baker County, *Florida*
- City of Ottawa, *Ontario*
- Guernsey County, *Ohio*
- State of *New Mexico*
- Hamilton County, *Tennessee*

SECURE

STATE-OF-THE-ART SECURITY TO SATISFY THE NEEDS AND EXPECTATIONS OF VOTERS, AND FOR YOUR ADDED PEACE OF MIND

EAC VVSG 2005 certified, featuring the highest security standards - with symmetric and asymmetric encryption - while preserving transparency through end-to-end system auditability.

Integrated ballot security features.

Encryption and security protocols are designed to meet the drafted Next Iteration requirements of the VVSG.

Extensive internal security monitoring to ensure data integrity and maintain public confidence.

EFFICIENT

SPECIFICALLY DESIGNED TO HELP YOUR ELECTION RUN EFFICIENTLY

All in one tabulator and accessible ballot marking device.

AuditMark® ballot image auditing capability retains a secure digital image of every ballot cast in your election.

Meets EAC VVSG 2005 standards with superior accessibility for all voters; designed to meet the drafted Next Iteration requirements of the VVSG.

ACCESSIBLE

PRESERVING THE INTEGRITY, PRIVACY AND DIGNITY OF VOTERS WITH ACCESSIBILITY NEEDS

A single unit to service all voters, featuring an integrated printer for ballot marking.

Randomized oval marking patterns and writing make the machine-marked ballots indistinguishable from hand-marked ballots, ensuring voter privacy.

Integrated privacy shield and screen cover.

Multi-lingual audio-visual support for all voters.

Please contact us for more information:
sales@dominionvoting.com
1.866.654.VOTE

Exhibit 1C

Electionware®

Election Management System

User Friendly

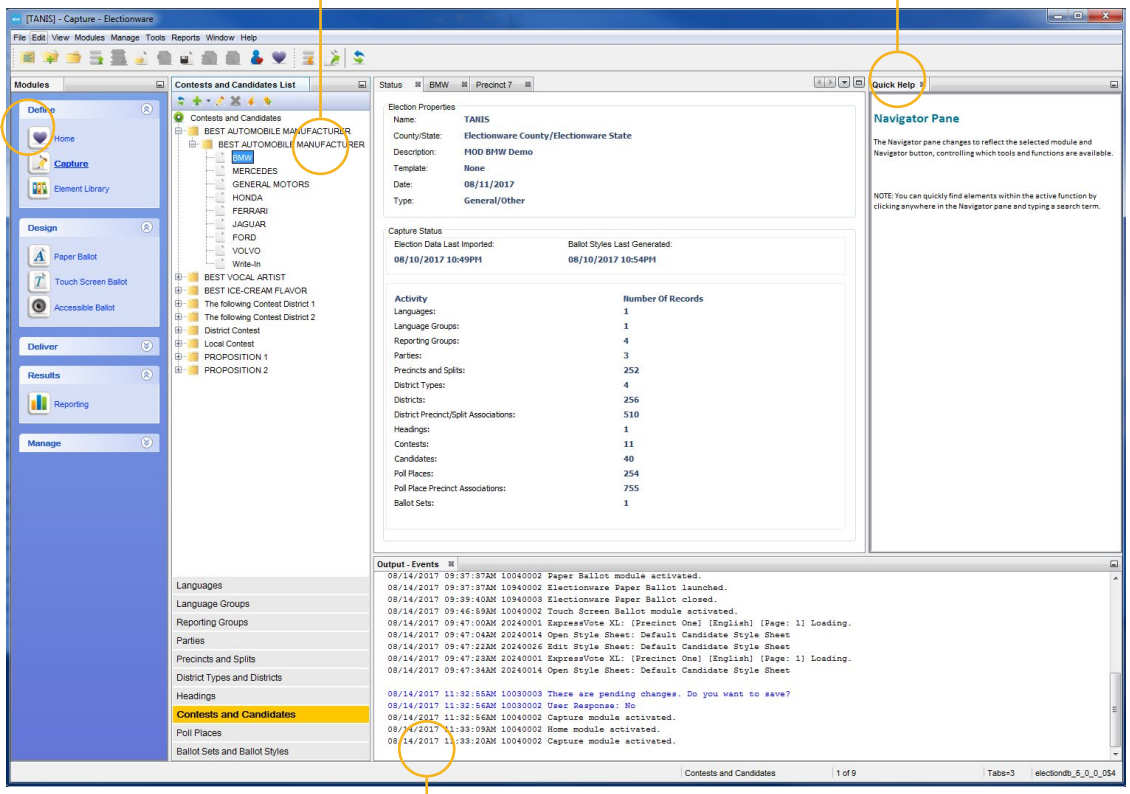
Navigator helps users access exactly what is needed in the current module.

Quick Help

Context-sensitive Quick Help is available in all areas of Electionware.

Easy End-to-End Workflow

Enables end-to-end election management, from data capture, ballot layout, and configuring equipment to loading and reporting results.



Feedback

Flexible, yet powerful election management software guides user through the creation of the election, ensuring that all election data, security codes, and machine settings are added correctly to the election definition.

ELECTION INTELLIGENCE

- Timely election data inquiries and reports
- Workflow management and error alerts
- Enforced data accuracy
- User customization
- Tracking of election media
- Live status indicators for incoming results

PRODUCTIVITY

- Fast data import
- Reusable election and ballot layout templates
- Simple translation and audio file management
- Multiple simultaneous users
- Ballot image filtering, viewing and printing

Electionware Key Features

Electionware is designed to accommodate the latest election trends, including early and overseas voting, ADA compliance, ballot adjudication, and Election Night reporting. Use Electionware to create an election information database, format ballots, program voting and ballot scanning equipment, count ballots, review ballot images, and report results. This agile election management system is the result of our nearly 40 years of election product research and development.

SIMULTANEOUS MULTIUSER ACCESS

Multi-user Electionware functionality enables large jurisdictions to use authorized election personnel on a closed-network system simultaneously creating precinct media flash drives and entering information for the ES&S equipment and Electionware. Additionally, the multi-user functionality in Electionware allows multiple teams of election officials to work simultaneously on different elections.

DATA SECURITY

Electionware incorporates the latest in election security, including built-in audit controls, encrypted election data, and access level user credentials designed to keep election data safe and secure. Electionware is fully compliant with EAC guidelines for usability, accessibility and security requirements. The Equipment Security feature creates security codes that control access to voting equipment. All election media USB flash drives contain encryption specific to the current election and equipment type.

ROBUST

Electionware manages nearly 10,000 ballot styles and precincts; supports myriad languages; manages and deploys multiple levels of security. One database for multiple equipment types provides election-wide uniformity and compliance, as well as less room for human error.

Exhibit 1D

POLL MANAGEMENT SOFTWARE

centralp•int®

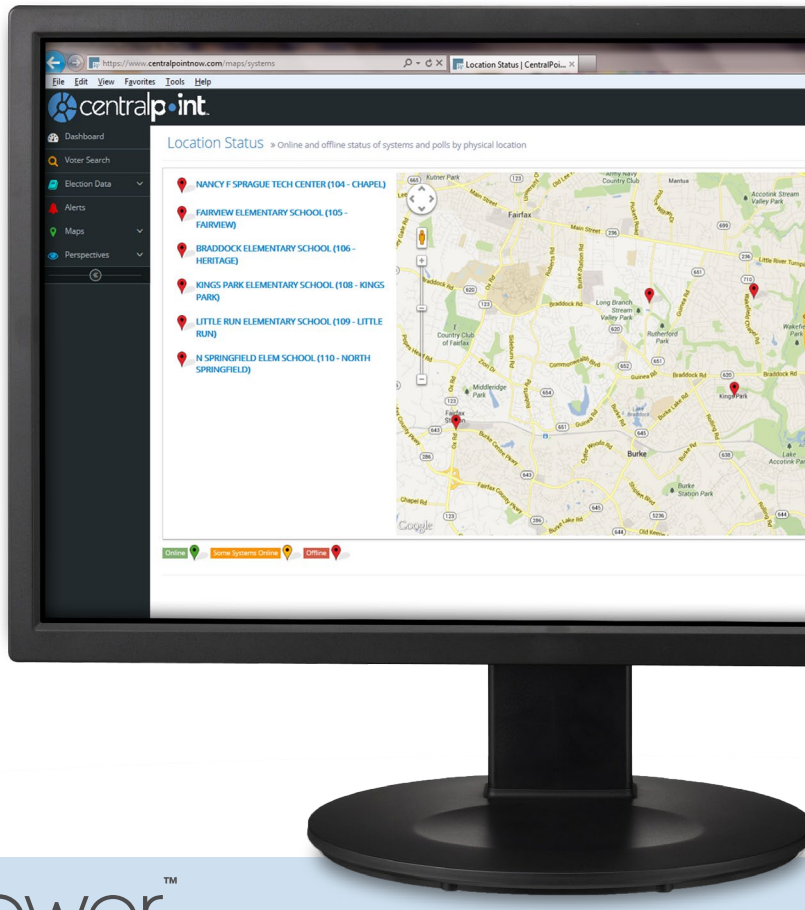
EVER WISH YOU COULD MANAGE YOUR POLL PLACES FROM THE CONVENIENCE OF YOUR PC OR SMARTPHONE?

CentralPoint is a web-based application that displays, monitors and tracks poll place information in real-time, allowing election administrators to mitigate issues before they becomes serious problems. All of this information is presented in graphical charts, maps and reports on an easily monitored dashboard display. This dynamic, real-time insight allows Election Administrators to manage their poll locations like never before.

Real-time Insight

PREVENT PROBLEMS WITH INTERACTIVE ALERTING AND AUTOMATED NOTIFICATIONS.

- Who voted by party, precinct, polling place, or hour
- Ballot quantities
- Poll opening and closing status
- Poll location traffic
- Equipment issues such as battery status, systems, software versions, connectivity



SECURE HOSTING BY empower™

CentralPoint's application design and controls are in place to protect sensitive data, monitor access and address regulatory compliance. ES&S developed Empower to support our customers with data storage and management. CentralPoint is hosted on Empower allowing, jurisdictions to not sacrifice the time, staff, or money required to maintain hardware and software.

- SAS-70 Certified and PCI compliant facilities
- Physical and virtual firewalls
- Monitored and managed server for guaranteed uptime
- Anti-virus and anti-malware
- Intrusion detection, intrusion prevention, and data integrity checking
- Data backups and disaster recovery

EARLY VOTING AND VOTE CENTERS

Are you worried about voter fraud if your voters can now vote anywhere? CentralPoint is a hub of voter information that allowsthe ExpressPoll's voter list to stay dynamic throughout the election. You always know who voted as soon as they vote at the polls.

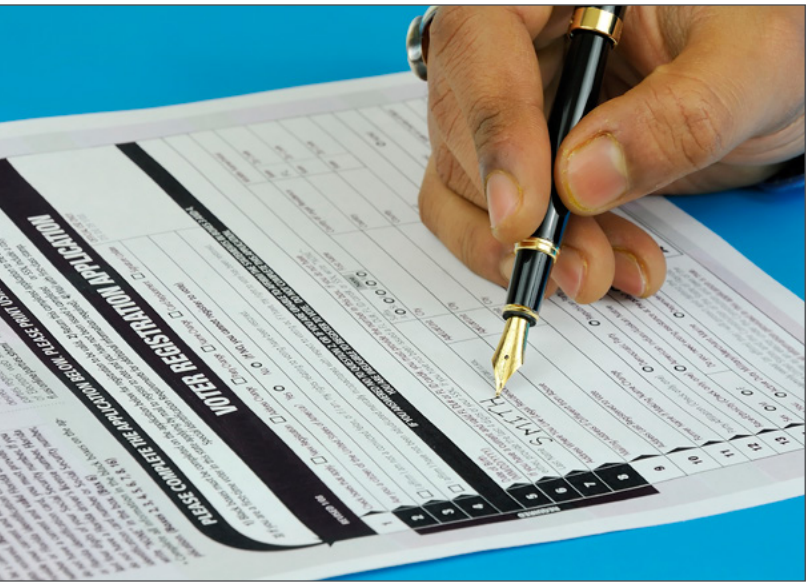
Exhibit 1E

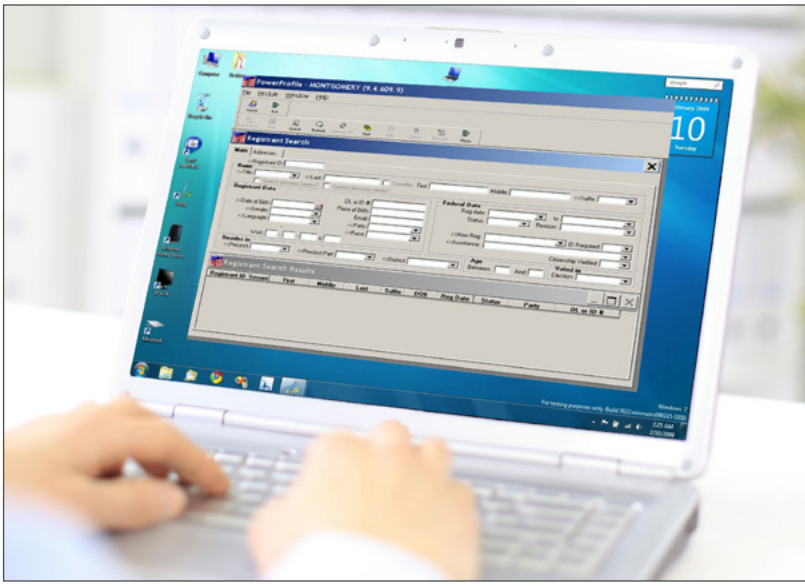
PowerProfile®
VOTER REGISTRATION SYSTEM

TURN-KEY ELECTION MANAGEMENT

PowerProfile is a voter registration and election management application that enables election officials to register voters and conduct elections from a central data store. This system allows for both single jurisdictions and states to manage elections from the same interface. Election officials are able to register voters, check eligibility, conduct election activities such as prepare absentee and early voting, recruit election workers, create poll books and rosters, verify petitions, and maintain voter records using a single software solution.

Because PowerProfile is HAVA compliant, it provides unique statewide identifiers to voter records, allows for statewide duplicate checking, and is customizable to meet specific requirements of the customer. PowerProfile also provides individual jurisdictions within a state total control over their voter registration data through role-based access controls. PowerProfile is also scalable and can be deployed for a single county, as well as for an entire state and all counties within that state.





WWW.ESSVOTE.COM

KEY FEATURES & BENEFITS

- User-friendly interface designed to facilitate quick and accurate data entry
- Real-time comparisons of new and existing registrations against external agencies such as Department of Motor Vehicles, Department of Corrections, and others
- HAVA and NVRA compliant
- Seamless voter record transfers between counties in the same state
- Integrated scanning functionality to attach additional image data to voter records, polling places, and petitions
- Audit / Activity / Notice logging and reporting
- Numerous interfaces for external products such as electronic poll books, ballot-on-demand printing, and electronic ballot delivery
- NCOA (National Change of Address) support
- Full absentee tracking from application request through ballot return (including all mail elections)
- Robust reporting, with the ability to produce notices/labels/reports and data exports
- Generation of notices such as ID cards, poll worker notices, and others
- Coding Accuracy Support System (CASS) interface allows jurisdictions using it to take advantage of postal discounts for CASS-certified mail
- GIS interface allowing bi-directional data exchange between GIS applications and PowerProfile
- Granular security utilizing role-based access controls as well as encryption of data at rest and in-transit
- A mobile-friendly web interface allowing voters to look up provisional and absentee ballot status, view sample ballots, and look up precinct and polling location information

WHY CHOOSE POWERPROFILE AND ES&S?

OUR PEOPLE! ES&S' experience working with government reaches back over four decades. Through the continual development and introduction of innovative elections products, our company has emerged as the leading provider of end-to-end, fully integrated voting solutions serving four countries and 39 states in the USA. Our team is composed of seasoned experts whose mission is to support our customers' election processes from start to finish. Access to this experience is a critical component in ensuring your elections run smoothly.

Because elections are all we do, ES&S provides 24/7 support by elections experts located in the United States, dedicated exclusively to voter registration. In addition to customer support, ES&S also provides comprehensive training programs and tools, software enhancements and upgrades, systems and procedures documentation, and user group meeting facilitation and coordination.

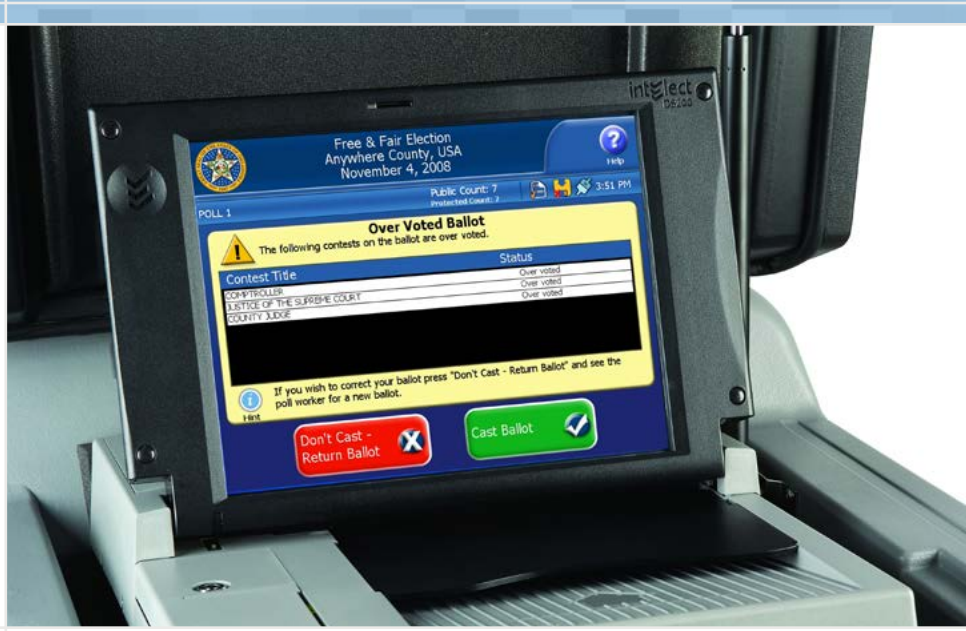
Exhibit 1F

Unity 3.4.0.0

ES&S Unity 3.4.0.0 is the latest election management software that combines your current voting system with the industry's best digital scanning solutions.

The DS200® is an intelligent, advanced, and integrated solution that features the latest digital image technology available on the market.

The DS850™ is unrivaled in speed and accuracy. Its high-speed digital imaging solution allows for smooth, continuous ballot scanning from start to finish – saving valuable time during the election process.



experience.
reliability.
security.
innovation.

DS200

Precinct Tabulator

- Handles over 450 precincts for Early Voting needs
- Large LCD touch screen for clear instructions at the poll
- Thermal paper roll with EZ-Load technology
- Results stored on USB drives—no batteries
- Easy transport with rolling case

DS850

High-speed Tabulator

- Scans more than 9,000 folded ballots per hour
- Automatic sorting allows for continuous scanning
- 3 outstack bins for write-ins, over-votes and blank ballots
- Large LCD touch screen for clear instructions at the poll
- High-speed camera captures every ballot image

Bridging the Gap

- Pairs your M100, M650 and AutoMARK with the latest digital scan technology
- Allows you to upgrade your tabulators at your own pace
- Bridges the gap between your current system and the next generation of voting equipment

Unity 3.4.0.0 gives you freedom to transition at your own pace to the DS200 and DS850

As a Premier customer, you don't have to leave behind your investment in the AutoMARK®.

As a customer of ES&S, you can continue to use the M100 and M650 while you upgrade.

+ =

unity 3.4.0.0

Certification of Unity 3.4.0.0

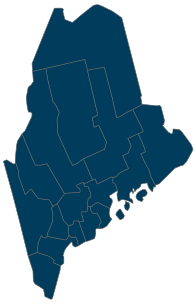
ES&S is proud to introduce our pairing of the DS200 with the world's fastest, most precise digital central scanner -- DS850. The suite enhances the DS200 and the AutoMARK for voters with special needs.

This latest suite of software has set a new standard of usability for voters and election officials.

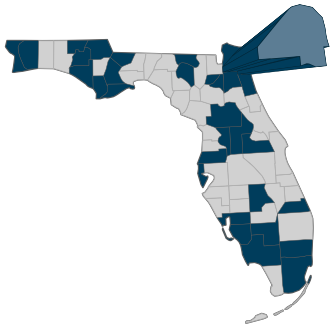
CERTIFIED EAC CERTIFIED

Newest Members of the ES&S Family

State of Maine
DS200® and AutoMARK®



Duval County, FL
DS850®, DS200®, AutoMARK®



maintaining voter confidence. enhancing the voter experience.

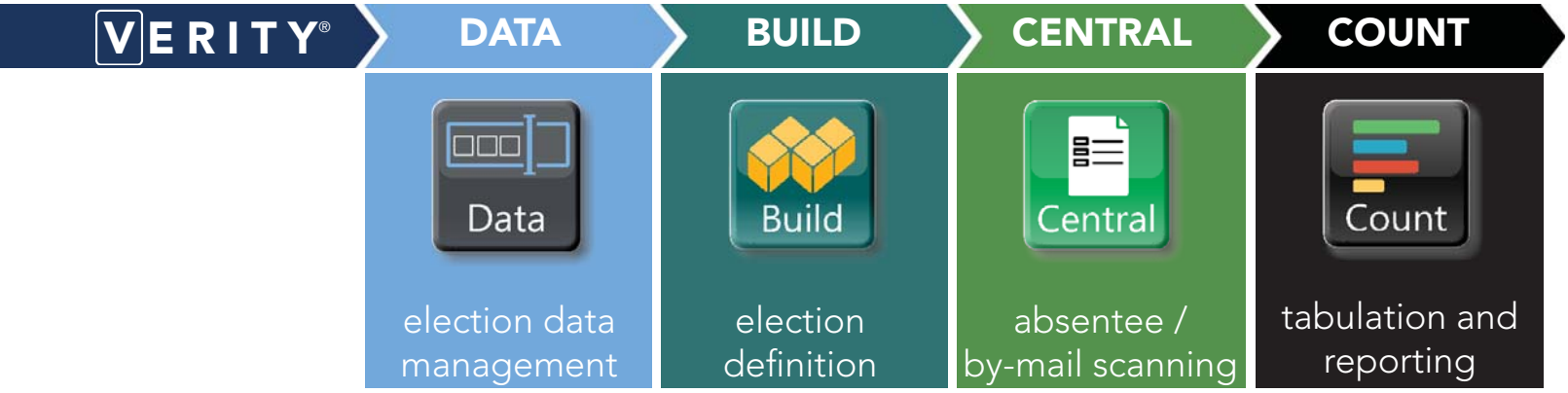
11208 John Galt Boulevard | Omaha, NE 68137 USA | P: 402.593.0101 | TF: 1.800.ESS.VOTE | F: 402.593.8107

www.essvote.com | hardware@essvote.com | software@essvote.com

Exhibit 1G

Verity

election software like no other

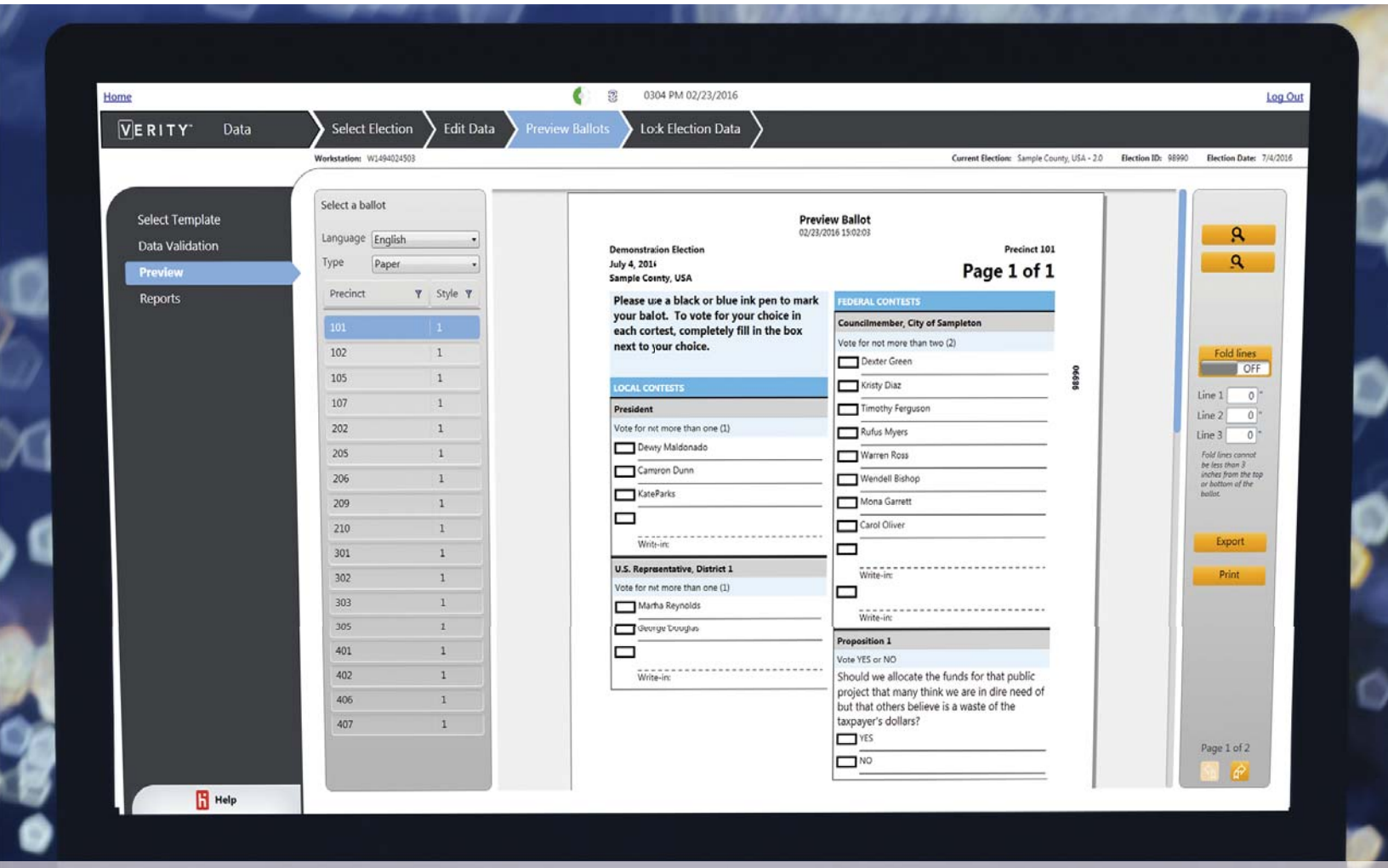


integrated end-to-end election management

HART intercivic™

Because software matters

Intuitive, plain language interfaces make it simple for elections staff to quickly get up to speed and efficiently run every aspect of every election.



The easiest election software you'll ever use

With a common look and feel across the whole system, Verity software suite is holistic and integrated.

Long-lasting ROI

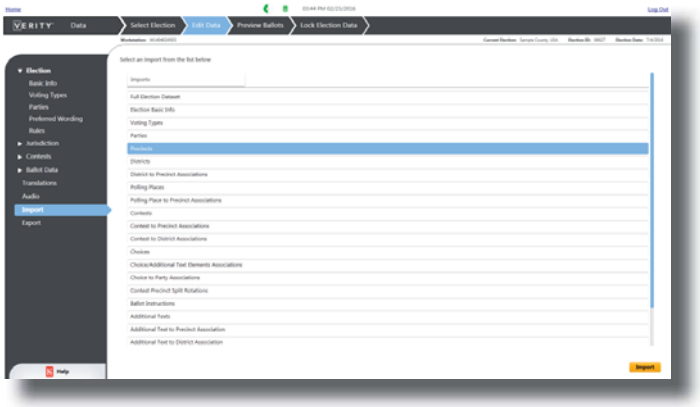
Verity software is designed for today's election needs – and tomorrow's. It accommodates flexible ballot layout, Vote centers, precinct voting, convenience voting, ranked choice voting and more. So today's investment pays off for years to come.

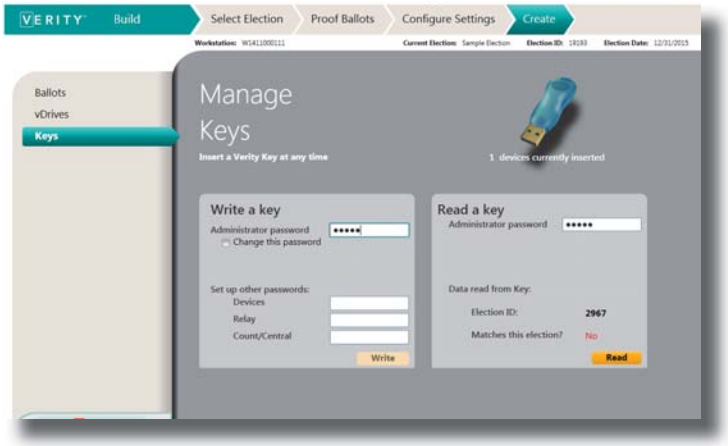
Choose only the components you need

Versatile, "one-path" election management

With Verity, you create the election just once for all devices and all methods of voting – whether you're preparing for Election Day, early voting, central scanning, vote centers, or another scenario. No workarounds, no duplicated effort.

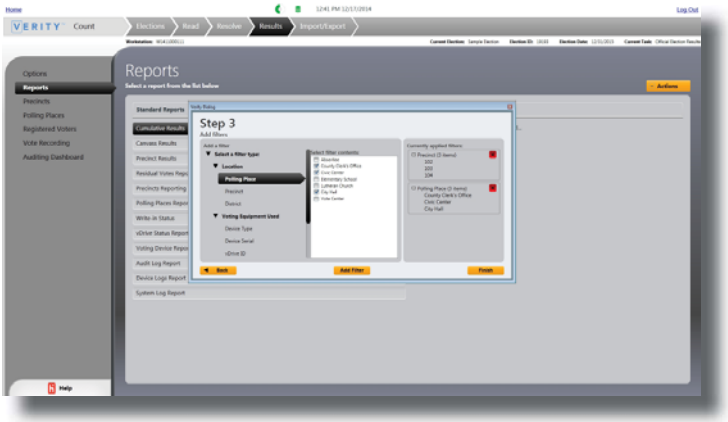
election data management | election definition | absentee / by-mail scanning | tabulation and reporting





Built-in transparency for trusted results

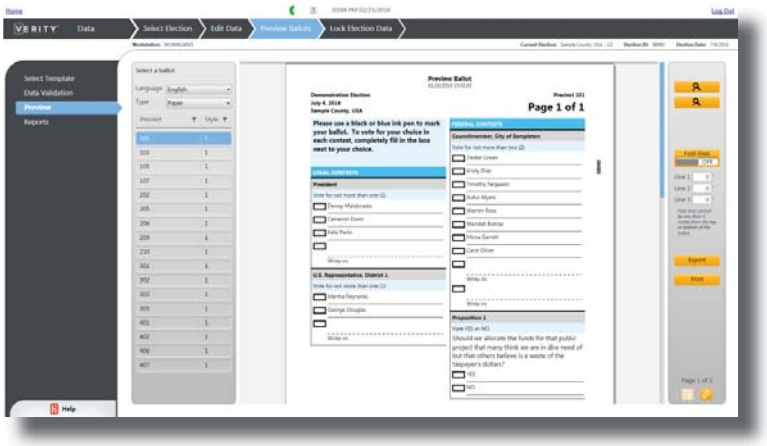
With Verity's comprehensive audit logging and robust report filters, plain-language information about all user actions is at your fingertips. And Verity safeguards your election with the latest security protocols.



Verity Data

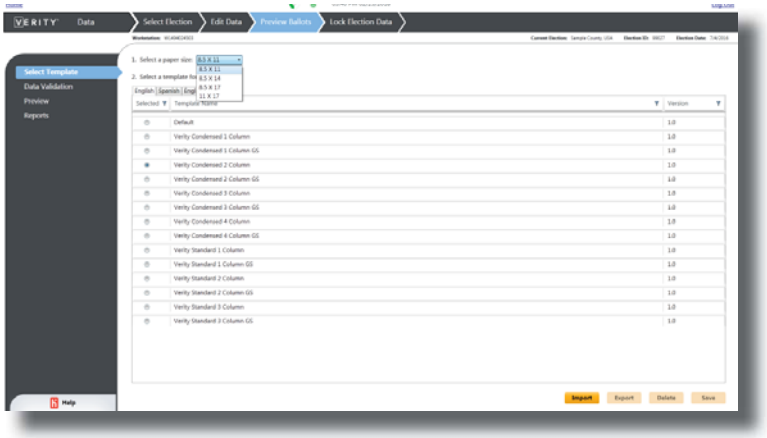
Election Data Management

Verity Data makes it easy to manage all the data that goes into every election. And Verity Data speaks to you in plain English – not in "code."



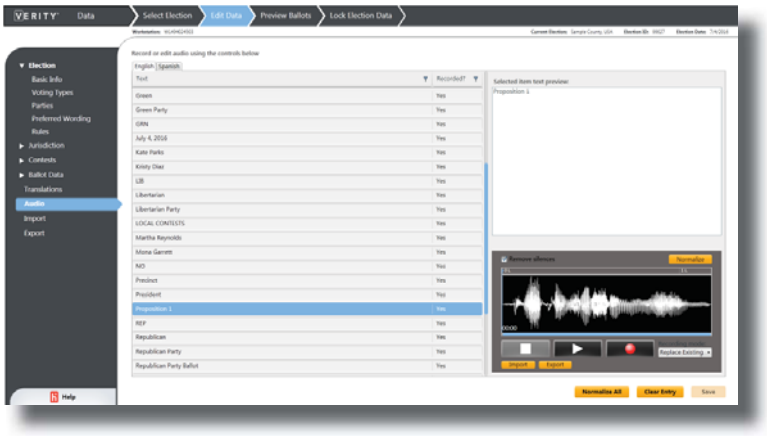
Easy, quick ballot layout

With customizable ballot templates and a modern graphical interface, ballot layout is easy and quick.



Efficient data management

You save time because you can re-use polling location names and other repeated data from previous elections, and you can import data from outside sources.



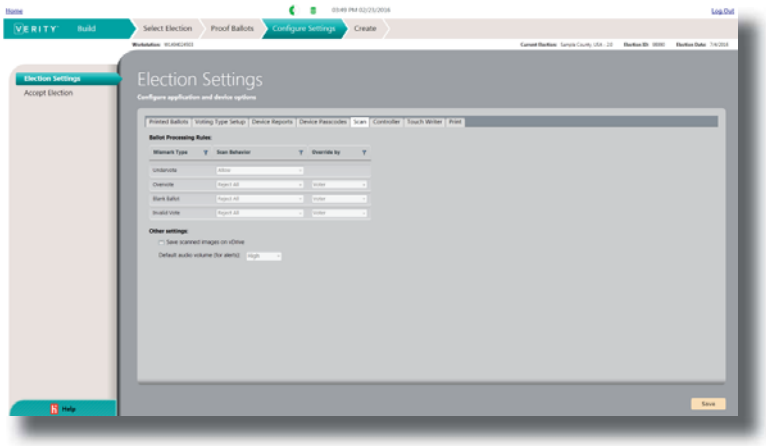
Flexible audio production

Verity Data includes live voice recording for audio creation.

Verity Build

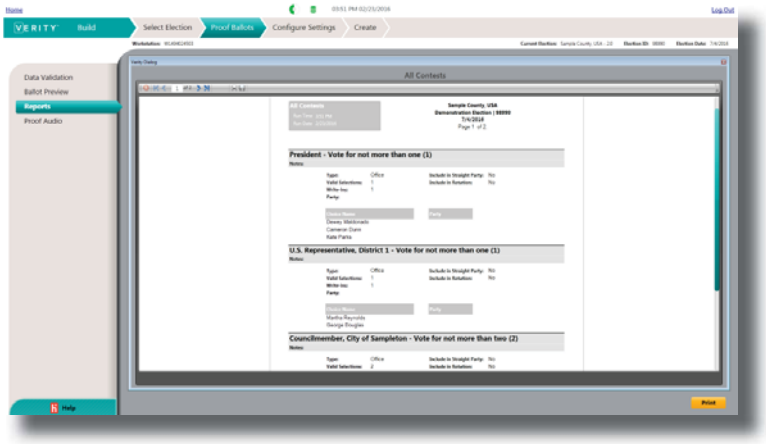
Election Definition and Deployment

Build your election once for all components – for any voting type. Program, proof and print your own ballots; no vendor help is needed.



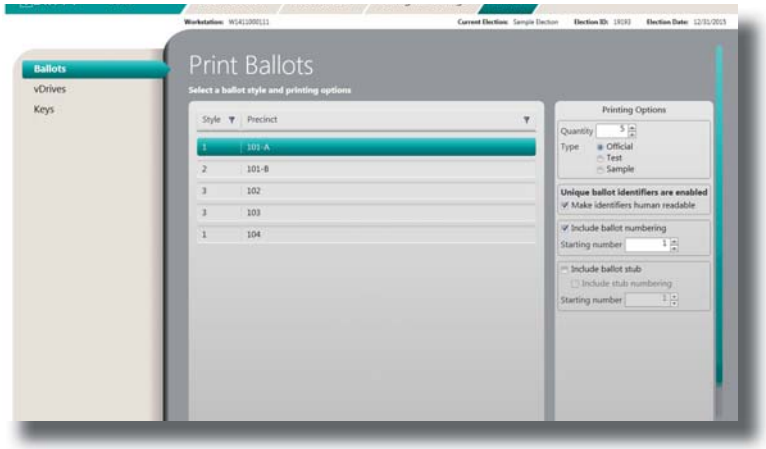
Get up to speed fast

With Verity Build's user-friendly interface, you don't have to be a programmer to define and deploy an election.



Flexible efficiency

Deploy your election with the election type, ballot sizes, device settings and many other options you choose.



Quick, accurate ballot and data proofing

Clear onscreen renderings let you preview ballots by precinct style and make corrections in real time.

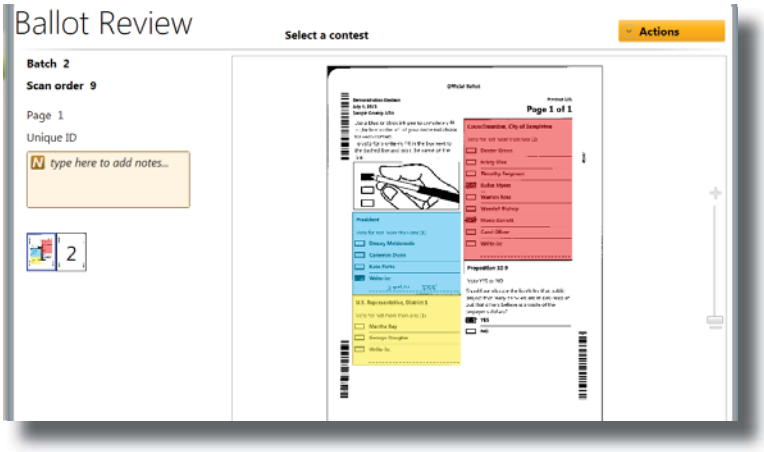
Automated test deck

With Verity Build's import of test deck marking patterns, staff no longer spends hours or days hand-marking ballots for logic and accuracy testing.

Verity Central

High-speed Central Scanning

Only Verity Central offers next-generation digital technology with the most efficient workflow, the easiest onscreen adjudication and auditing features like you've never seen.

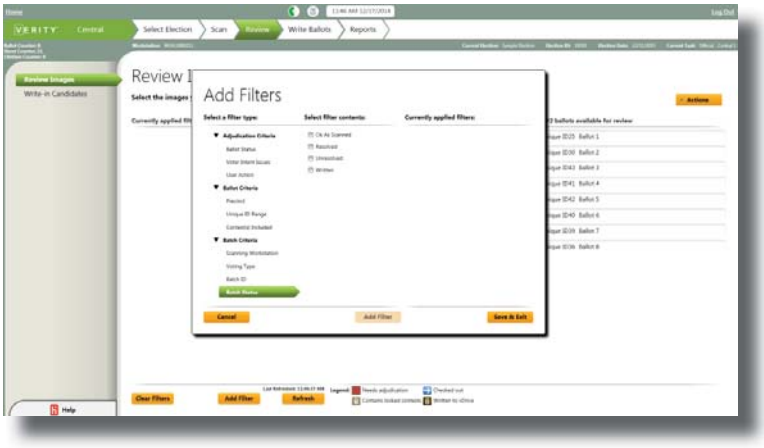


True onscreen adjudication

Verity Central provides unique contest-by-contest resolution for all voter intent issues with clear, color-coded flags and Verity's consistently easy-to-understand, plain-language instructions.

No presorting

Scan multiple precinct styles and/or multiple languages in the same batch, in any orientation.



No outstacking and rescanning

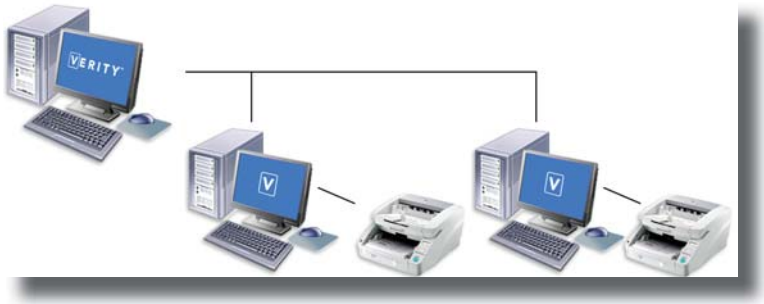
With Verity Central, there's no extra work – just an easy, efficient workflow. Preserve your ballots in their original form, with minimal handling.

No-wait scanning

Verity Central scans without tabulating, so you can start scanning weeks before polls close on Election Day. No more late nights at the scanner.

Transparency and easy auditability

With an unmatched variety of image filters, you easily locate exactly the ballot images you want. Plain-language processing notes clearly show exactly how voter selections are recorded.



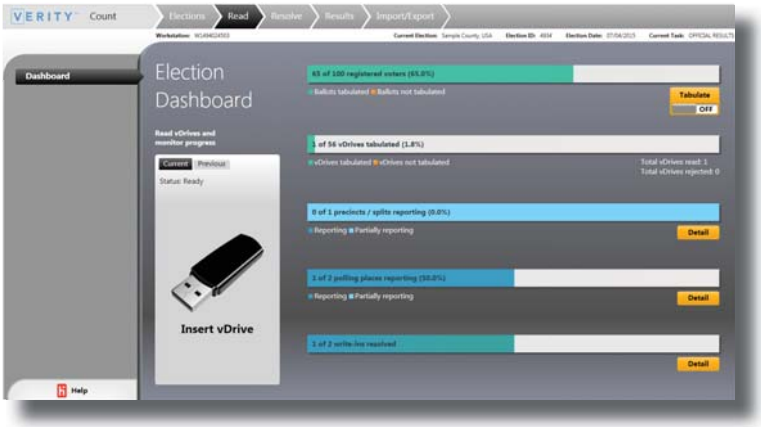
Cost-effective scalability

Choose the right Hart-integrated COTS scanner for your jurisdiction's size, budget and need for speed. You get industry-best scanning technology with the assurance of Hart support – and EAC certification.

Verity Count

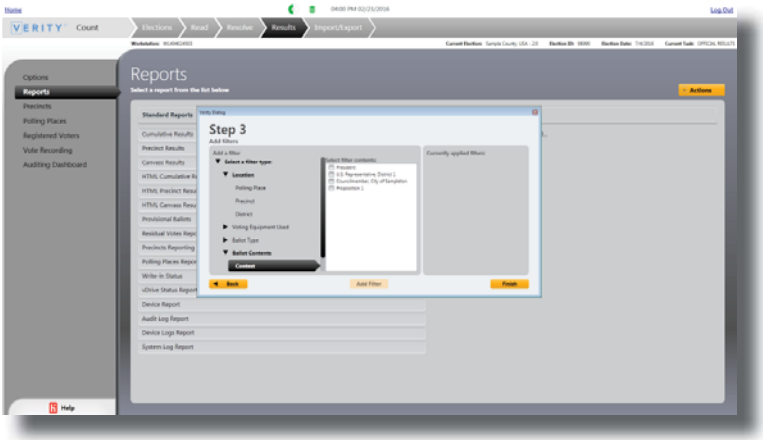
Tabulation and Reporting

With intuitive, easy-to-use dashboards and flexible, configurable reporting, Verity Count is exceptionally transparent and auditable.



At-a-Glance Election Night status monitoring

Verity Count's Election Dashboard shows progress toward completion in real time.

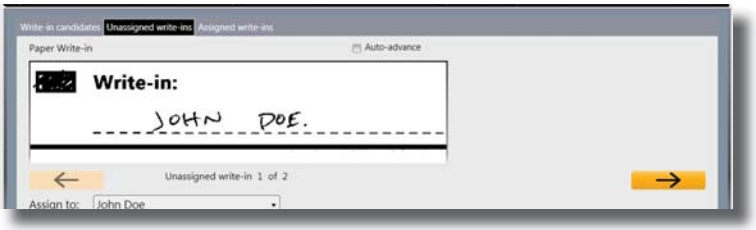


Scalable for faster tabulation

You can network Verity Count workstations for faster tabulation.

Flexible, customizable reporting

The power to decide when and how to display, combine, or group results is in your hands, through a user-friendly reporting interface. And Verity Count's rich array of reporting filters puts the data you need at your fingertips.



Efficient, adjudication of write-ins

Verity Count can display an image of each write-in for quick resolution.

Robust post-election auditing

Access exactly the cast vote record you need with Verity Count's unique Auditing Dashboard and an unmatched variety of highly customizable filters.

The Future of Elections

Exceptionally easy to use, Verity's software suite streamlines election management. It's flexible for how you vote – today and tomorrow. And transparency and security are built in.

www.hartintercivic.com | info@hartic.com | 800.223.4278

This brochure contains marketing information that describes the functional capabilities of Verity products, and is not intended to represent specific implementations for your locale. State- and/or jurisdiction-specific requirements may affect how the products are permitted to be implemented and used.

Exhibit 1H

Verity Scan

Digital Ballot Scanning

exceptionally easy and accurate scanned vote capture

Designed for: Early Voting | Election Day | Vote Centers

HART intercivic™

Voters

Quick ballot scanning
Patented, animated arrows show the voter exactly when and where to insert the ballot. There's no wrong way to insert the ballot lengthwise, and Verity Scan reads both sides of the ballot in seconds.

Easy second-chance voting
Easy-to-understand, plain language notices alert voters to possible errors, giving them a second chance to make any corrections.

Election Managers

Ensures reliable audits of voter intent and enables fast recounts
You can configure Verity Scan to digitally capture full images of scanned ballots.

Securely stores voting data
Secure, redundant, physically separate storage locations for ballot images, case vote records and audit logs assure officials that voting data is safe.

Provides polling place reports
Built-in thermal printer can print ballot count totals or results at the polling place after polls close.

Enables immediate resolution of write-ins at the polling place
Can print write-in images for on-the-spot write-in resolution.

Poll Workers

Easy to transport, set up and use
Verity Scan is easy to transport in ordinary vehicles and easy to set up at the polling place. And the collapsible ballot box folds to just 6 inches thin.

Easy to start up and shut down in minutes
Simple, plain-language, step-by-step onscreen instructions.

Fewer voter questions
Plain-language instructions, animated guide lights, and jam-free ballot feeding means easy scanning for voters – and less work for poll workers.

Only Verity uses AIGA Design for Democracy templates; its plain language interface is the easiest to use.

Ballot box folds to 6" thin

Warehouse Staff

Saves on storage space
Verity Scan is compact and stackable, so you use less storage space.

Easy delivery
A small footprint means Verity Scan requires minimal manpower and muscle to deliver.

Exceptionally easy to use

With its plain-language, Design for Democracy-based interface and easy-scanning features, Verity Scan is a breeze for voters and poll workers to use.

VERITY®

The Future of Elections

Hart InterCivic is a full service election solutions innovator, partnering with state and local governments to deliver the most secure, accurate and reliable elections.

Versatile for long-term value

Verity Scan easily manages hundreds of ballot styles, so you can use it in a large variety of voting scenarios, even if your needs change.

Cost-effective storage, transport and setup

Compact size saves storage space and reduces transportation costs. Easy setup at the polling place can lower staffing costs.

Cost-saving features

With on-board testing and calibration, Verity Scan requires very little maintenance.

Lifecycle longevity

Early in its lifecycle and with a robust new supply chain, Verity Scan promises many, many years of cost-effective service.

Exhibit 1I

Verity Touch Writer

Ballot Marking Device

ballot marking for everyone

Designed for: Early Voting | Election Day | Vote Centers | Central Election Offices

HART intercivic™

Voters

Simple
Touchscreen interface with plain-language instructions inspired by EAC/AIGA Design for democracy standards make voting simple. No ballots to load, no waiting.

Provides true equality of access
Verity Touch Writer, paired with a Hart-integrated COTS printer, produces identical full-sized paper ballots for all voters – no segregated ballots. Includes adjustable audio and contrast settings and compatibility with "sip-and-puff" and other adaptive controls.

The voting booth offers easy wheelchair access, and the tethered controller can be placed wherever it is easiest for the voter to use.

Easy second-chance voting
Voters can review the ballot summary at any time, and it's easy to change selections before printing the ballot.

Election Managers

Adaptable
Accommodates limitless ballot styles and is suitable for all voters in a variety of settings. Can print blank ballots as needed.

Reduces training time
User-friendly interface has the same look-and-feel as other Verity voting components, for shorter staff training time and lower training costs.

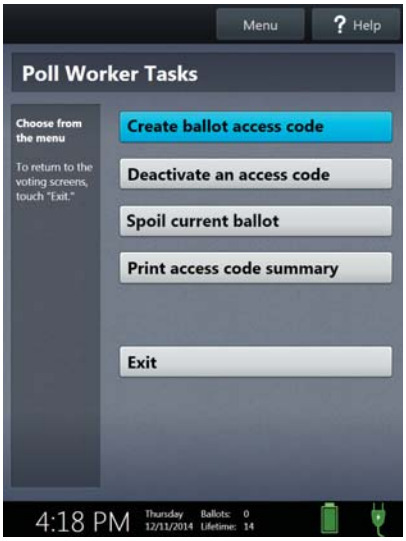
Nearly maintenance free
Verity Touch Writer is exceptionally simple to maintain; election staff easily completes most tasks independently.

Poll Workers

Easy to transport, set up, and use
Compact and lightweight, Verity Touch Writer is easy to transport in ordinary vehicles and easy to set up at the polling place.

Easy to start up and shut down in minutes
Simple, plain-language, step-by-step onscreen instructions.

Easy ballot activation
Voters can activate their own correct ballot style using a simple access code – no pre-loading of ballots or proprietary cards required.



Only Verity uses AIGA Design for Democracy templates; its plain language interface is the easiest to use.

Warehouse Staff

Saves on storage space
Verity Touch Writer is compact and stackable, so you use less storage space.

Easy delivery
A small footprint means Verity Touch Writer requires minimal manpower and muscle to deliver.

Easy, accessible ballot marking

With its user-friendly interface and comprehensive accessibility features, Verity Touch Writer makes ballot marking easy for everyone.

VERITY®

The Future of Elections

Hart InterCivic is a full service election solutions innovator, partnering with state and local governments to deliver the most secure, accurate and reliable elections.

Lower total cost of ownership
Compact size saves storage space and reduces transportation costs. Setup at the polling place is easy for anyone – reducing staffing costs. And Verity Touch Writer requires very little maintenance.

Versatile for long-term value
Accommodates almost limitless ballot styles, and is part of the holistic, scalable Verity Voting solution that can adapt as your needs change.

Lifecycle longevity
Verity Touch Writer promises many, many years of cost-effective service.

Exhibit 2

Written Testimony

of

Christopher Krebs
Senior Official Performing the Duties of the Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the
United States House of Representatives
Committee on Oversight and Government Reform
Subcommittees on Information Technology and Intergovernmental Affairs

Regarding
Cybersecurity of Voting Machines
November 29, 2017

Chairman Hurd, Chairman Palmer, Ranking Member Kelly, Ranking Member Demings and members of the Subcommittees, thank you for inviting me to participate in today's hearing on securing our elections from malicious cyber activity. This is an especially timely topic given the elections earlier this month. As you know, the Department of Homeland Security (DHS) performs a critical mission focused on reducing and eliminating threats to the nation's critical physical and cyber infrastructure, including how it relates to our elections.

Given the vital role that elections play in a free and democratic society, the Secretary of Homeland Security determined that election infrastructure should be designated as a critical infrastructure subsector. With the establishment of an Election Infrastructure Subsector (EIS), the DHS National Protection and Programs Directorate (NPPD) and federal partners have been formalizing the prioritization of ***voluntary*** cybersecurity assistance for election infrastructure similar to that which is provided to a range of other critical infrastructure entities, such as financial institutions and electric utilities.

During the 2016 election period and since that time, the federal government and election officials have been meeting regularly to share cybersecurity risk information and to determine effective means of assistance. Recently, the EIS Government Coordinating Council (GCC) met to establish goals and objectives, to develop plans for the EIS partnership, and to lay the groundwork for developing an EIS Sector Specific Plan (SSP). The GCC framework provides a well-tested mechanism across critical infrastructure sectors for sharing threat information between the federal government and council partners, advancing risk management efforts, and prioritizing services available to sector partners in a trusted environment. EIS-GCC representatives include DHS, the U.S. Election Assistance Commission (EAC), the National Institute of Standards and Technology (NIST), the Federal Buruea of Investigation (FBI), the Department of Defense (DoD), and key state and local election officials. Participation in the council is entirely voluntary and does not change the fundamental role of state and local jurisdictions in overseeing elections.

In addition to the work of the EIS-GCC, DHS continues to engage state and local elections officials – coordinating requests for assistance, risk mitigation, information sharing, and incident coordination resources and services. In order to ensure a coordinated approach across DHS, NPPD has brought together stakeholders from across the Department as part of an Election Task Force (ETF). The ETF increases the Department's efficiency and efficacy in understanding, responding to, communicating, and sharing information related to cyber threats. The ETF serves to provide actionable information to assist states in strengthening their election infrastructure against cyber threats.

Assessing the Threat

DHS continues to robustly coordinate with the EAC, the intelligence community, and law enforcement partners. Among non-federal partners, DHS has been engaging state and local officials, as well as relevant private sector entities, to assess the scale and scope of malicious cyber activity potentially targeting the U.S. election infrastructure. In addition to working directly with state and local officials, we partnered with stakeholders to analyze relevant cyber data, including the Multi-State Information Sharing and Analysis Center (MS-ISAC), the

National Association of Secretaries of State and the National Association of State Election Directors.

We also used our field personnel deployed around the country, to help further facilitate information sharing and enhance outreach. Such engagement paid off in terms of identifying suspicious and malicious cyber activity targeting the U.S. election infrastructure. A body of knowledge grew throughout the summer and fall of 2016 about suspected Russian government cyber activities, and understanding that helped drive collection, investigations, and incident response activities. On October 7, 2016, DHS and the Office of the Director of National Intelligence (ODNI) released a joint statement to the public on election security and urged state and local governments to be vigilant and seek cybersecurity assistance.

We continue to assess that mounting widespread cyber operations against U.S. voting machines at a level sufficient to affect a national election would require a multiyear effort with significant human capital and information technology (IT) resources available only to nation-states. The level of effort and scale required to significantly change a national election result, however, would make it nearly impossible to avoid detection.

Enhancing Security for Future Elections

DHS continues to focus our efforts on ensuring a coordinated response from DHS and its federal partners to plan, prepare, and mitigate risk to the election infrastructure. We recognize that working with stakeholders is the only sure way to ensure more secure elections. Based on our assessment of activity observed in the last election, DHS is engaged with stakeholders across the spectrum to increase awareness of potential vulnerabilities and enhance security of U.S. election infrastructure.

Our election process is governed and administered by state and local election officials in thousands of jurisdictions across the country. These officials manage election infrastructure and ensure its security on a day-to-day basis. State and local election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of their elections. In partnering with these officials through both new and existing, ongoing engagements, NPPD is working to enhance their efforts to secure election systems.

Improving coordination with state and local partners: Increasingly, the nation's election infrastructure leverages IT for efficiency and convenience. Similar to other IT systems, reliance on digital technologies introduces new cybersecurity risks. NPPD helps stakeholders in federal departments and agencies, state and local governments, and the private sector to manage some of these cybersecurity risks. Consistent with our long-standing partnerships with state and local governments, we have been working with election officials to share information about cybersecurity risks, and to provide voluntary resources and technical assistance.

DHS works with the MS-ISAC to provide threat and vulnerability information to state and local officials. Created by DHS over a decade ago, the MS-ISAC is partially funded by NPPD. The MS-ISAC's membership is limited to state and local government entities, and all

fifty states and US territories are members. It has representatives co-located with the NCCIC to enable regular collaboration and access to information and services for state chief information officers.

Providing technical assistance and sharing information: Through engagements with state and local election officials, including working through the Sector Coordinating Council, NPPD actively promotes a range of services to include but are not limited to the following:

Cyber hygiene service for Internet-facing systems: This voluntary service is conducted remotely, afterwards, NPPD provides state and local officials with a report identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the Internet, such as online voter registration systems, election night reporting systems, and other Internet-connected election management systems. During the 2016 election, we provided cyber hygiene services to 33 state and 36 local election jurisdictions.

Risk and vulnerability assessments: These assessments are more thorough and executed on-site by NPPD cybersecurity experts. These evaluations require two to three weeks and include a wide range of vulnerability testing services, focused on both internal and external systems. When NPPD conducts these assessments, we provide a full report of vulnerabilities and recommended mitigations following the testing. These assessments are available on a limited, first-come, first-served basis.

Incident response assistance: We encourage state and local election officials to report suspected malicious cyber activity to the NCCIC. On request, the NCCIC can provide on-site assistance in identifying and remediating a cyber incident. Information reported to the NCCIC is also critical to the federal government's ability to broadly assess malicious attempts to infiltrate election systems. This technical information will also be shared with other state officials so they have the ability to defend their own systems from similar malicious activity.

Information sharing: DHS will continue to share relevant information on cyber incidents through multiple means. The NCCIC works with the MS-ISAC, and election officials can connect with the MS-ISAC or their State Chief Information Officer directly as one way to benefit from this partnership and rapidly receive information they can use to protect their systems. State election officials may also receive incident information directly from the NCCIC. In 2016, best practices, cyber threat information, and technical indicators, some of which had been previously classified, were shared with election officials in thousands of state and local jurisdictions.

Classified information sharing: DHS provides classified briefings to cleared stakeholders upon request, as appropriate and necessary.

Field-based cybersecurity advisors and protective security advisors: DHS has more than 130 cybersecurity and protective security personnel available to provide actionable information and connect election officials to a range of tools and resources to improve the cybersecurity preparedness of election systems and to secure the physical site security of voting

machine storage and polling places. These advisors are also available to assist with planning and incident management for both cyber and physical incidents.

Physical and protective security tools, training, and resources: NPPD provides advice and tools to improve the security of polling sites and other physical election infrastructure. This guidance can be found at www.dhs.gov/hometown-security. This guidance helps to train administrative and volunteer staff on identifying and reporting suspicious activities, active shooter scenarios, and what to do if they suspect an improvised explosive device. Officials can also contact local NPPD PSAs for access to DHS resources.

2017 Elections and Beyond

This hearing is timely given the elections earlier this month. We have been working with election officials in all states to enhance the security of their elections by volunteering operations support and by establishing essential lines of communications with election infrastructure partners at all levels – public and private – for reporting both suspicious cyber activity and incidents. To quickly and effectively evaluate and triage any potential cyber-related events related to Election Day, DHS enhanced its state of readiness. Our goal was to enhance transparency and have visibility of aggregated elections-related cybersecurity efforts. These enhanced operations exercised interagency coordination, incident escalation, and incident communications to better improve guidance and planning in preparation for elections operations in 2018 and beyond.

In closing, the fundamental right of all citizens to be heard by having their vote accurately counted is at the core of our American values. Ensuring the integrity of our electoral process is a vital national interest and one of our highest priorities as citizens in a democratic society. We have confidence in the overall integrity of our electoral system. Our voting infrastructure is diverse, subject to local control, and has many checks and balances. As the threat environment evolves, the Department will continue to work with state and local partners to enhance our understanding of the threat; and to provide essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency.

Thank you for the opportunity to appear before the Subcommittees today. I look forward to your questions.

Christopher C. Krebs Biographical Summary

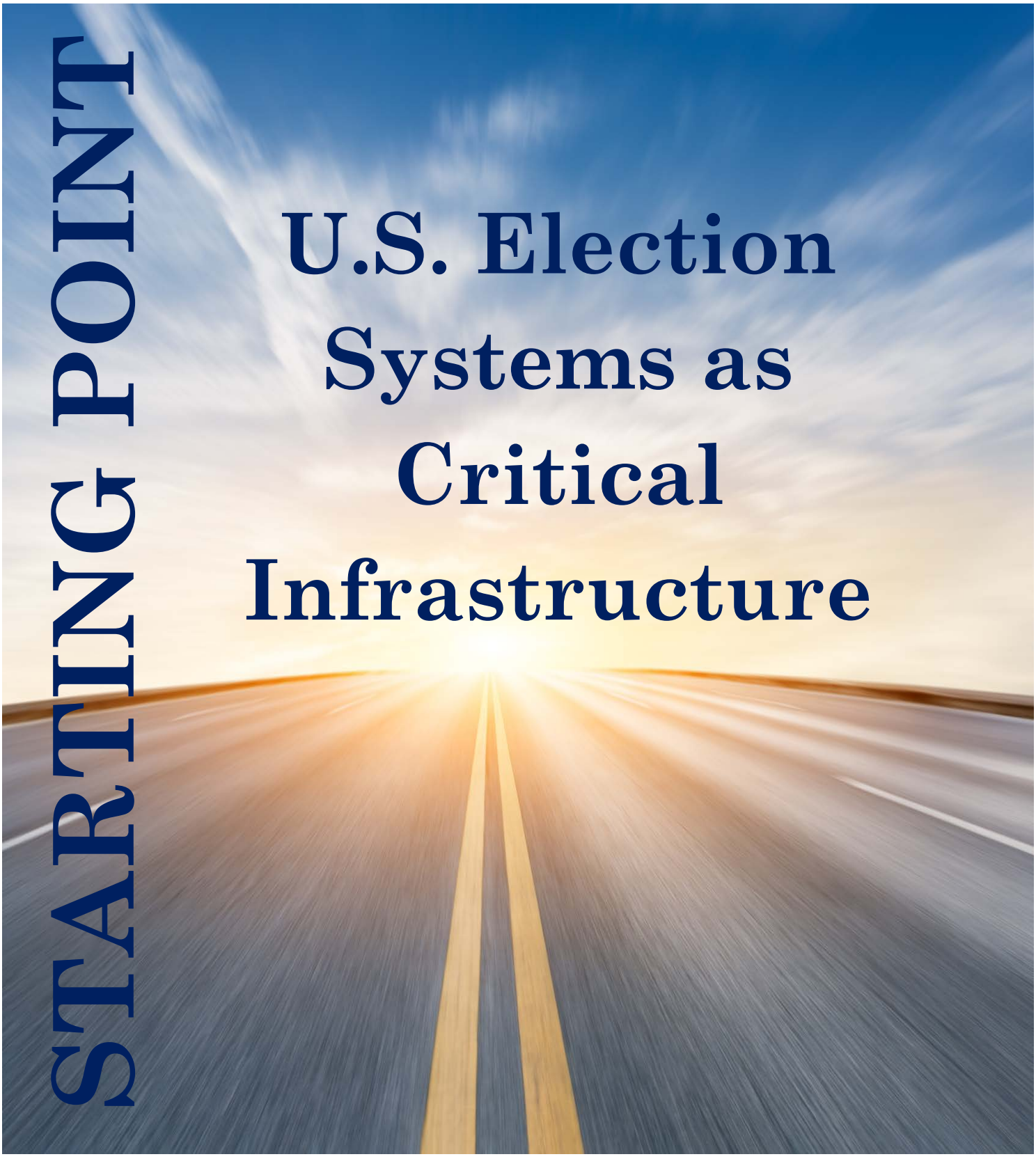
Chris Krebs is the Senior Official Performing the Duties of the Under Secretary for the National Protection and Programs Directorate in the Department of Homeland Security, where he oversees the cyber and physical infrastructure security mission for the Department. He is concurrently filling the role of Assistant Secretary for the Office of Infrastructure Protection, to which he was appointed by the President in August 2017. As Assistant Secretary, he leads NPPD's mission on issues such as preventing complex mass attacks, securing high-risk chemicals, and other areas related to cyber and physical infrastructure resilience. This includes serving as the national coordinator for the critical infrastructure security and resilience mission and directly managing 6 of the 16 critical infrastructure sectors outlined in the National Infrastructure Protection Plan. The 16 sectors cover a complex and interconnected range of infrastructure, such as commercial facilities, emergency services, chemical facilities, nuclear facilities and government facilities including the 2017 addition of an election infrastructure subsector.

Mr. Krebs joined the Department of Homeland Security in March 2017, serving as Senior Counselor to the Secretary, where he advised DHS leadership on a range of cybersecurity, critical infrastructure protection, and national resilience issues. Prior to coming to DHS, Krebs was a member of Microsoft's US Government Affairs team as Director for Cybersecurity Policy, where he led Microsoft's U.S. policy work on cybersecurity and technology issues. Before Microsoft, Krebs advised industry and Federal, State, and local government customers on range of cybersecurity and risk management issues. This the second time he has worked at the Department, previously serving as Senior Advisor to the Assistant Secretary for Infrastructure Protection and playing a formative role in a number of national and international risk management programs. He holds a Bachelors in Environmental Sciences from the University of Virginia and a J.D. from the Antonin Scalia Law School at George Mason University.

Exhibit 3

STARTING POINT

U.S. Election Systems as Critical Infrastructure



U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

Starting Point:

U.S. Election Systems as Critical Infrastructure

On January 6, 2017, Department of Homeland Security (DHS) Secretary Jeh Johnson designated U.S. election systems as part of the nation's critical infrastructure, a decision that was later affirmed by current DHS Secretary John Kelly. Since the designation was announced, state and local election officials across the country have raised questions about the day-to-day impact of the designation and how it will benefit their work to conduct accessible, accurate and secure elections. This document details DHS's critical infrastructure designation and what election administrators can expect moving forward. It also provides a glossary of terms frequently used in conjunction with correspondence and discussions about the critical infrastructure designation.

What is critical infrastructure?

Critical infrastructure is a DHS designation established by the Patriot Act and given to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." [i] DHS, the department responsible for critical infrastructure, was established by the Homeland Security Act in 2002.

In order to fulfill its responsibilities under the Patriot Act, DHS uses the National Infrastructure Protection Plan (NIPP) as the foundational document, or "rule book," for how to develop sector-specific critical infrastructure plans. The NIPP established a process roadmap by which the nation's critical infrastructure sectors can be identified and created.

In addition to the Patriot Act and NIPP, a third piece of critical infrastructure governing authority comes from Presidential Policy Directive 21 (PPD-21). Released on February 12, 2013, PPD-21 established the Federal Government's "strategic imperatives" in its approach to the nation's critical infrastructure. It established the current critical infrastructure sectors and identified each sector's Sector Specific Agency (SSA), which is the agency charged with structuring and managing the sector.

What other sectors are included in the nation's critical infrastructure?

Critical infrastructure sectors are groupings based on common function and form. There are currently 16 sectors. They are: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials and Waste; Transportation Systems; and Water and Wastewater Systems. [ii]

One critical infrastructure sector, Government Facilities, has three sub-sectors, Elections, National Monuments and Icons, and Education Facilities. Subsectors are sections of a specific sector that vary from the rest of the sector substantially enough to justify creating a plan just for the subsector.

How are sectors organized?

Once DHS creates a sector, the SSA structures it and helps it self-organize, a requirement of the NIPP. With regard to election systems, this means that members of the election community come together to join and manage the various components that make up this sector. After the critical infrastructure sector is formally established and organized, the SSA is charged with managing it. The SSA is "responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment." [iii]

While DHS has vast national security knowledge and resources, it acknowledges that it is not an issue-area expert for some of the sectors designated as critical infrastructure. To fill this knowledge gap, DHS will often appoint another federal agency as its Co- Sector Specific Agency (Co-SSA). This is especially common when DHS creates a subsector. Co-SSAs help DHS navigate the nuances of a specific subsector and share SSA responsibilities. For example, the sub-sector Co-SSA for Education Facilities is the Office of Safe and Drug-Free Schools in the Department of Education. A complete list of the sectors, and their respective SSAs and Co-SSAs follows at the end of this document (Addendum II).

DHS has yet to designate a Federal Agency as a Co-SSA for the elections sector. The U.S. Election Assistance Commission (EAC) has publicly called on DHS to select the commission to fill this important role. The request was made in light of the working relationship between DHS and the EAC, crafted during the 2016 presidential election and continued since.

Beyond the SSA and Co-SSA roles, there are other key entities established to support a newly designated critical infrastructure sector, including:

- ✓ **Sector Coordinating Councils (SCCs)**: These are "self-organized, self-run, and self-governed private sector councils consisting of owners and operators and their representatives, who interact on a wide range of sector-specific strategies, policies, activities, and issues. SCCs serve as principal collaboration points between the government and private sector owners and operators for critical infrastructure security and resilience policy coordination and planning and a range of related sector-specific activities." [iv]
- ✓ **Government Coordinating Councils (GCCs)**: These consist of "representatives from across various levels of government (including Federal and State, local, tribal and territorial), as appropriate to the operating landscape of each individual sector, these councils enable interagency, intergovernmental,

and cross-jurisdictional coordination within and across sectors and partner with SCCs on public-private efforts." [v]

As part of its designation plan, the SSA will work to establish these councils to support the U.S. election systems designation. For the U.S. election system, these groups will likely include representatives from federal, state, and local government; election system vendors; and other stakeholders impacted by the critical infrastructure designation.

Another key component of operating a critical infrastructure sector is to ensure clear, strong lines of communication between the SSA, Co-SSA, coordinating councils, and stakeholders. This can include creation of the following:

- ✓ **Information Sharing and Analysis Centers (ISACs)**: These are "operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders." (Source: Presidential Decision Directive 63, 1998)[vi]
- ✓ **Information Sharing and Analysis Organizations (ISAOs):** Though similar to ISACs, ISAOs are "any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of: (a) Gathering and analyzing Critical Infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof; (b) Communicating or disclosing Critical Infrastructure information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to Critical Infrastructure or protected systems; and (c) Voluntarily disseminating Critical Infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (a) and (b)." [vii]

The distinction between an ISAC and an ISAO is that "[u]nlike ISACs, ISAOs are not directly tied to Critical Infrastructure sectors, as outlined in Presidential Policy Directive 21. Instead, ISAOs offer a more flexible approach to self-organized information sharing activities amongst communities of interest such as small businesses across sectors: legal, accounting, and consulting firms that support cross-sector clients, etc." [viii] Essentially, ISAOs allow for more widespread information sharing across sectors and among interested individuals regardless of clearance, knowledge level, or inclusion in a critical infrastructure sector.

What is unique about the protection of critical infrastructure communications?

Information about security and vulnerabilities that is shared under the restrictions of the Critical Infrastructure Information Act is considered Protected Critical Infrastructure Information (PCII). PCII is not subject to the many disclosure regulations, such as those found in the Freedom of Information Act and its state-level counterpart. This protection, allows the critical infrastructure community to discuss vulnerabilities and problems without publically exposing potentially sensitive information.[ix]

For those participating in election sector coordinating councils this protection means that some information communicated between DHS and the coordinating councils can be protected. This limits the potential for sensitive election security information to be made public and protects potentially sensitive material from being misconstrued or used for nefarious purposes. This protection is made possible by an exception to the Federal Advisory Committee Act created by the Critical Infrastructure Partnership Advisory Council.[x]

Are new resources available following a critical infrastructure designation?

A critical infrastructure designation provides for greater access to DHS information and security resources. It also provides a safer and more discreet exchange of information and requests for advice or assistance. While it is important to note that DHS will provide assistance to any domestic entity that requests help and not just critical infrastructure, its assistance to entities within a critical infrastructure sector is prioritized over providing assistance to non-critical infrastructure entities.

DHS resources – including on-going and current information about threats, risk and vulnerability assessments, and security best practices as well as hands-on advice – help infrastructure owners and managers better secure their systems. The department emphasizes the importance of the information assets it has available to critical infrastructure entities and understands that security clearances are a requirement for accessing some of these resources. This is why DHS works with infrastructure owners and managers to secure clearances when necessary.

Use of DHS resources and participation in sector councils is voluntary, and DHS continually states that it cannot force critical infrastructure owners and managers to interact with a sector, its components, or its resources. Entities that choose to leverage these new resources have a direct line to DHS resources via a Cyber Security and Protective Security Advisor. These advisors directly supply security assistance to the country and handle on-going assistance to CI entities.

While some within the election community remain skeptical about the critical infrastructure designation, their outstanding concerns about the designation make the case for why input from key election sector stakeholders is a vital part of setting up the needed infrastructure of councils and committees that can make this designation impactful. DHS is actively seeking participation from election stakeholders and their sector

allies, noting that there is an advantage inherent in helping to shape the critical infrastructure mechanisms election officials will use to gain resources and communicate with DHS. The department has relied on the EAC to provide the forum for much of this outreach, and the commission recommends that election officials and others in the election community take steps to becoming involved in this process either directly or through the EAC.

What role will the EAC play as DHS stands up the critical infrastructure designation?

The EAC has requested DHS name the commission as Co-SAA. This designation is important to ensure that state and local election officials and administrators have an informed federal advocate working directly with DHS as the department determines what resources and services are needed to protect U.S. election systems and how these resources will be distributed. The EAC has held and will continue to hold, hearings and meetings to give DHS a platform to discuss the designation and its potential benefits, as well as answer questions from stakeholders. The EAC prides itself on serving as a trusted intermediary between state and local election officials and federal government leaders, as well as a provider of resources needed to navigate this new space. Serving as the official Co-SSA for implementing the critical infrastructure designation would tap into this strength and provide election officials with assurance that their interests and concerns will shape the contours of DHS's plan moving forward.

Addendum I: Glossary of Key Terms and Acronyms

Critical Infrastructure Glossary

Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Source:§1016(e) of the USA Patriot Act of 2001 (42 U.S.C. §5195c(e)))
Critical Infrastructure Partnership Advisory Council (CIPAC)	Council established by DHS under 6 U.S.C. §451 to facilitate effective interaction and coordination of critical infrastructure activities among the Federal Government, the private sector, and State, local, tribal and territorial governments. (Source: CIPAC Charter) These meetings are exempt from the Federal Advisory Committee Act (FACA) requirements that they be open to the public and provide meeting materials to the public.
Critical Infrastructure Sector	A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; NIPP 2013 addresses 16 critical infrastructure sectors, as identified in PPD-21. (Source: NIPP 2013: Partnering for Critical Infrastructure Security and Resilience)
Cybersecurity	The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (Source: 2009 NIPP)
Executive Order 13636	Executive Order that calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing; develop a technology-neutral cybersecurity framework; and promote and incentivize the adoption of strong cybersecurity practices. (Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013)
Government Coordinating Council (GCC)	The government counterpart to the Sector Coordinating Council for each sector established to enable interagency and intergovernmental coordination; comprises representatives across various levels of government (Federal and State, local, tribal and territorial) as appropriate to the risk and operational landscape of each sector. (Source: 2009 NIPP)
Information Sharing and Analysis Centers (ISACs)	Operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders. (Source: Presidential Decision Directive 63, 1998) ISACs are not operated, controlled, or managed by DHS.

Information Sharing and Analysis Organization (ISAO)	"Any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of gathering and analyzing critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability there of; communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure or protected systems; and voluntarily disseminating critical infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B)." (Source: Homeland Security Act of 2002)
Infrastructure	The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole; consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements. (Source: DHS Lexicon, 2010)
National Annual Report	Each SSA is required to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CI/KR protection in their respective sectors. (National Infrastructure Protection Plan: The National CI/KR Protection Annual Report)
National Infrastructure Coordinating Center (NICC)	The National Infrastructure Coordinating Center (NICC) is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government. When an incident or event affecting critical infrastructure occurs and requires coordination between the Department of Homeland Security and the owners and operators of our nation's infrastructure, the NICC serves as that information sharing hub to support the security and resilience of these vital assets. (Source: DHS.gov/national-infrastructure-coordinating-center)
National Infrastructure Protection Plan (NIPP)	The National Infrastructure Protection Plan 2013, involving stakeholders from all 16 critical infrastructure sectors, all 50 states, and from all levels of government and industry, provides a clear call to action to leverage partnerships, innovate for risk management, and focus on outcomes, provides an updated approach to critical infrastructure security and resilience, and involves a greater focus on integration of cyber and physical security efforts. (DHS, NIPP Fact Sheet)
National Protection and Programs Directorate (NPPD) – (DHS/NPPD)	[The DHS division] that leads the DHS mission to reduce risk to the Nation's critical physical and cyber infrastructure through partnerships that foster collaboration and interoperability. (Source: DHS FY13 Budget Guidance). NPPD contains the Federal Protective Service, the Office of Identity Management, the Office of Cybersecurity and Communications, the Office of Cyber and Infrastructure Analysis, and the Office of Infrastructure Protection.

Presidential Policy Directive 21 (PPD-21)	[Presidential Directive that] Aims to clarify roles and responsibilities across the Federal Government and establish a more effective partnership with owners and operators and State, local, tribal and territorial entities to enhance the security and resilience of critical infrastructure. (Source: PPD-21, 2013)
Presidential Policy Directive 8 (PPD-8)	[Presidential Directive that] facilitates an integrated, all-of-Nation approach to national preparedness for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters; directs the Federal Government to develop a national preparedness system to build and improve the capabilities necessary to maintain national preparedness across the five mission areas covered in the PPD: prevention, protection, mitigation, response, and recovery. (Source: PPD-8, 2011)
Protected Critical Infrastructure Information (PCII)	PCII is [information and communications] protected from disclosure. All critical infrastructure information that has been properly submitted and validated pursuant to the Critical Infrastructure Information Act and implementing directive; all information submitted to the PCII Program Office or designee with an express statement is presumed to be PCII until the PCII Program Office determines otherwise. Critical infrastructure information voluntarily shared with the government and validated as PCII by the Department of Homeland Security is protected from, the Freedom of Information Act (FOIA), State, local, tribal, and territorial disclosure laws, use in regulatory actions and use in civil litigation. PCII can only be accessed in accordance with strict safeguarding and handling requirements, and only trained and certified federal, state, and local government employees or contractors may access PCII.(Source: CII Act of 2002, 6 U.S.C. § 131, and www.dhs.gov/pcii-program)
Protective Security Advisors (PSAs)	Trained critical infrastructure protection and vulnerability mitigation subject matter experts who work for DHS and are responsible for ensuring all Office of Infrastructure Protection critical infrastructure security and resilience programs and services are delivered to State, local, tribal, and territorial stakeholders and private sector owners and operator. There are three types: (1) Regional Directors, supervisory PSAs, PSAs, and geospatial analysts. s. (Source: DHS.gov/protective-security-advisors)
Sector Coordinating Council (SCC)	The private sector counterpart to the GCC, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector. They serve as principal entry points for the government to collaborate with each sector for developing and coordinating a wide range of critical infrastructure security and resilience activities and issues. (Source: Adapted from the 2009 NIPP)
Sector-Specific Agency (SSA)	A Federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise, as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. (Source: PPD-21, 2013)

Sector-Specific Plans (SSP)	Planning documents that complement and tailor application of the National Infrastructure Protection Plan to the specific characteristics and risk landscape of each critical infrastructure sector. SSPs are developed by the SSAs in close collaboration with the SCCs and other sector partners. (Source: Adapted from the 2009 NIPP)

Addendum II: Critical Infrastructure Sectors and their SSAs and Co-SSAs

Sector/ Subsector	SSA	Co-SSA
Chemical	Department of Homeland Security (DHS)	
Commercial Facilities	Department of Homeland Security (DHS)	
Communications	Department of Homeland Security (DHS)	
Critical Manufacturing	Department of Homeland Security (DHS)	
Dams	Department of Homeland Security (DHS)	
Defense Industrial Base	Department of Defense (DOD)	
Emergency Services	Department of Homeland Security (DHS)	
Energy	Department of Energy (DOE)	
Financial Services	Department of the Treasury	
Food and Agriculture	Department of Agriculture (USDA)	Department of Health and Human Services (HHS)
Government Facilities	Department of Homeland Security (DHS)	General Services Administration (GSA)
Elections (subsector)	Department of Homeland Security (DHS)	
Education Facilities (subsector)	Department of Homeland Security (DHS)	Department of Education
National Monuments (subsector)	Department of Homeland Security (DHS)	Department of the Interior (DOI)
Healthcare and Public Health	Department of Health and Human Services (HHS)	
Information Technology	Department of Homeland Security (DHS)	
Nuclear Reactors, Materials, and Waste	Department of Homeland Security (DHS)	
Transportation Systems	Department of Homeland Security (DHS)	Department of Transportation (DOT)
Water and Wastewater Systems	Environmental Protection Agency (EPA)	

[i] Patriot Act, (Sec. 1016(e))
[ii] https://www.dhs.gov/Critical-Infrastructure-sectors, accessed May 2, 2017.
[iii] Ibid.
[iv] Department of Homeland Security, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*, p. 12.
[v] *NIPP 2013*, p. 31.
[vi] Presidential Decision Directive 63, 1998.
[vii] Source: *Homeland Security Act of 2002, 6 U.S.C. § 131.*
viii Department of Homeland Security, Frequently Asked Questions About Information Sharing and Analysis Organizations (ISAOs), https://www.dhs.gov/isao-faq, accessed May 3, 2017.
[ix] Department of Homeland Security, *NIPP 2013*, p. 12.
[x] Department of Homeland Security, *United States Department of Homeland Security Charter of the Critical Infrastructure Partnership Advisory Council,* https://www.dhs.gov/sites/default/files/publications/cipac-charter-11-30-16-508.pdf, accessed June 5, 2017

Exhibit 4

Last Updated: July 21, 2017

ISSUE BRIEFING: Securing Future Elections Against Cyber Threats

What Are the Threats? Concerns have been raised about foreign attempts to compromise our nation's election systems through cyberattacks. In January 2017, the U.S. Department of Homeland Security designated state and local voting systems as ***critical infrastructure*** in order to offer a federal response to such threats. Secretaries of State are bolstering cybersecurity and resilience levels for future elections by focusing on key digital components of their state systems: voter registration databases, election management systems, election night reporting systems and electronic voting machines.

States Taking a Proactive Approach. Secretaries of State are committed to working with their federal, state and local partners on a voluntary basis, including the U.S. Election Assistance Commission (EAC) and the U.S. Department of Homeland Security, to solicit input on threats and share information on risk assessment and threat mitigation in our elections. Additional steps may be taken based upon credible or specific threats that are identified. Secretaries of State are also working in collaboration via the NASS Election Security Task Force, created for sharing resources, best practices and technical advice between states. Areas of shared state interest include:

- Establishing clear and effective structures for threat and intelligence information-sharing, victim notification processes and cyber incident response
- Identifying threat mitigation practices and state legislation/policy trends for consideration
- Conducting risk assessments and implementing continuous vulnerability assessments
- Ensuring that election offices have sufficient equipment, technical support and resources to maintain a sound security posture for their computer-based systems
- Fostering a culture of risk awareness with strong cyber hygiene practices

Areas of Shared State Interest

1) *Establishing clear and effective structures for threat and intelligence information-sharing, victim notification processes and cyber incident response, including:*

    - Obtaining federal government security clearances for Secretaries of State/Chief State Election Officials in order to access timely threat information to protect election systems.
    - Improving government processes for notifications regarding system attacks and breaches.
    - Establishing a Critical Infrastructure State Government Coordinating Council to interface with federal agencies regarding election security issues.
    - Leveraging MS-ISAC/State Fusion Centers for continuous monitoring, threat detection and incident awareness/response.
    - Developing state-specific frameworks for cyber incident response, in the event of a major attack.

2) Identifying threat mitigation practices and state policy trends for consideration, including:

- Under a risk-based model like the NIST Cybersecurity Framework, some states are trying to develop more of an enterprise mentality to improving cybersecurity coordination and response.

- Reviewing/updating policies for back-up paper ballots and equipment, paper printouts/records for polling place use, post-election audits, back-up voter lists (paper and electronic) and voter data security.

3) Conducting risk assessments and implementing continuous vulnerability assessments, including:

- Regularly monitoring election system threats and vulnerabilities to defend any related cyber networks against attacks, including phishing scams, malware, denial-of-service attacks and other common practices employed by malicious actors.
- Working with in-house IT advisors, private security partners, state CIOs/CISOs, Homeland Security Advisors, the Department of Homeland Security and others to ensure that state election systems are secured with technologies and standard operating practices that can successfully diagnose potential cyber threats, track cyberattacks, provide mitigation options and enhance the resilience of state systems.
- Documenting and reviewing all security procedures/systems, including pre- and post-election protocols and testing procedures, physical security and chain of custody policies and response to reported hardware/software issues.

4) Ensuring that election offices have sufficient equipment, technical support and resources to maintain a sound security posture for their computer-based systems, including:

- Consulting with key stakeholders (ie. Members of Congress, Governor, state legislators, state CIO/CISO) regarding current levels of investment in state and local election infrastructure. Request cybersecurity briefing from Governor/State CIO or CISO.
- Replacing aging voting equipment that is nearing end of life, no longer meets state testing and certification requirements, or will soon fail to meet such requirements due to lack of technical support/replacement parts.
- Bringing laws and policies guiding election administration into compliance with existing legal exemptions for critical infrastructure information-sharing under federal law.

5) Fostering a culture of risk awareness with strong cyber hygiene practices, including:

- Training or guidance on cyber hygiene protocols for elections officials, along with establishing clear communication protocols between state-local officials.
- Providing guidance on procedures for reporting election issues and security-related incidents (i.e. state hotlines, poll worker guidance, state task force, DHS/FBI coordination, state fusion center with law enforcement).

What Else Will Combat Foreign Threats? Keeping elections state and locally-run (decentralized), keeping voting equipment offline and leaving voting machines unnetworked, keeping voter lists clean and up-to-date and convincing more Americans to simply take part in voting and volunteering at the polls.

For additional questions on this briefing, please contact NASS: (202) 624-3525 or nass@sso.org.