12-9-2009

Comments on expanding civic participation in voting by expanded use of the Internet

Candice Hoke
Cleveland State University, s.hoke@csuohio.edu

Cleveland State University
Cleveland-Marshall College of Law

TO: Federal Communications Commission

FROM: Professor Candice Hoke, Founding Director, Center for Election Integrity
(Election security & constitutional federalism specialist; Team Leader for portion of California Top to Bottom Review of voting systems; co-author of election forensics monograph; Election Law professor; Ohio spokesperson for Election Protection Coalition, 2008; Yale Law J.D.; *Yale Law Journal* editor.

DATE: December 9. 2009

RE: FCC 09-47, 09-51, 09-137; NPB Pub Not #20

Thank you for requesting comments on expanding civic participation in voting by expanded use of the Internet.

As a law professor teaching Regulatory Law and Election Law, I have closely followed, analyzed and taught the FCC's approach to maintaining Internet neutrality, which has been an outstanding success thus far. I hope, however, the FCC will not become involved in election regulatory issues concerning the Internet, but will support a different federal regulatory agency with national security and technical-cybersecurity expertise receiving primary jurisdiction over election cybersecurity.

This memo briefly responds to the questions you posed (Part A), provides some bullet points of my professional expertise relatd to election and technical security issues (Part B), and attaches a paper delivered at an international, interdisciplinary conference in Prague to discuss formulating better Internet governance. The paper addresses for Internet voting governance issues.

A. Issues and Summary Answers

a. With existing technology, is it possible to enable and ensure safe and secure voting online today?

Mailing Address: 2121 Euclid Avenue LB 138 • Cleveland, Ohio 44115-2214
Campus Location: Law Building Room 138 • 1801 Euclid Avenue • Cleveland, Ohio
http://www.law.csuohio.edu • (216) 687-2344 • Fax (216) 687-6881

A: No, it is not. Please see the SERVE Report and the attached paper delivered this past summer on Internet voting governance issues, which cites the SERVE Report; the Technologists' Statement on Internet Voting, and the submission to the FCC from Dr. David Jefferson.

b. What can we learn from other nations that have considered or implemented online voting?

A: This is too large a question for short comments. Suffice it to say that neither Estonia nor Switzerland are comparable to the US in relevant factors, especially the payoff for a successful disruption or manipulation of federal elections.

c. What can we learn from pilot projects that have tested online voting?

A: If you are speaking of domestic pilot projects, none of these pilots have been properly structured to test for and approximate the risks that would be posed to domestic US elections. They are especially remiss in conceptualizing the risks for elections to Federal and Statewide office, where the fiscal control over billions of dollars is concerned, and the direction of military powers and foreign policy/aid.

The Internet voting pilot programs were structured by for-profit vendors, who also reported on their "success" without any independent evaluation and transparency on some critical dimensions. In Hawai'i, the project did report a dramatic drop in the reported rate of voter participation. The pilot, however, did not include any structures by which an assessment could be conducted of whether technical attacks had occurred to intercept, modify or otherwise block voted ballots from reaching the election processing location. Nor did it offer any auditing assessments that the ballots as tabulated matched the ballots as cast by voters. Thus, no conclusions can be drawn about the pilot's success, and it bears little relation to a Federal or Statewide election context.

Over the past year, those of us involved in election security and legitimacy have observed newly expanded governmental efforts at the State and Federal levels to use the Internet for voting ("IV"), including for the most sensitive cargo of all -- return of voted (marked) ballots for tabulation. This pressure is occurring despite computer and network security scientists' pointed criticism of the extraordinary risks they would generate to the legitimacy of our elections, and especially for the foreign intrusions into our election voting records and results. The regulators have generally then replied: then tell us how to reduce the risks in Internet voting, so we can vote over the Internet.

A preeminent MIT computer scientist who also has served on the Federal Technical Guidelines Development Committee for the US Election Assistance Commission, Dr. Ron Rivest, has noted that asking how to reduce the risks in Internet voting by formulating "best practices" so Internet voting can be broadly and quickly launched, is analogous to

inquiring how to drive drunk more safely. The risks of drunk driving and Internet voting (especially the risks attending the Internet transmission of voted ballots) are so incontrovertible to those who are knowledgeable in these fields that asking these questions is obvious, palpable nonsense. Unfortunately, the regulators thus far interested in promoting the expanded use of the Internet in voting/elections have lacked a sufficient understanding of network and computer security, election security, and their relation to this nation's national security interests, that a bandwagon is beginning to develop for Internet voting in the US. The FCC should assist in arresting this development, literally *pro bono publico* and perhaps even the survival of the US as an independent nation.

For-profit Internet voting vendors have underestimated the risks and overstated the reliability and other performance features of their Internet voting software. It appears we may be facing a redux of the electronic voting system debacles that wasted public monies and lost votes over the past decade.

d. Have localities or states enabled online voting either domestically or for citizens abroad (such as military personnel stationed overseas)?

A: Several States and localities, and the US EAC are moving in this direction now. The attached paper (presented at the international Internet governance conference in 2008) calls for a nuanced approach to IV.

e. Do government jurisdictions at any level, domestic or foreign, allow online voting for any citizen? Have there been quantifiable impacts tied to oiline voting, including impacts on the number of citizens that voted? Have there been qualitative impacts tied to online voting, either positive or negative?

A: I defer to others to provide data here.

f. What are the security and privacy risks that government jurisdictions must consider when considering the implementation of online voting?

A: See the attached article and its citations, including to the SERVE Report, the NIST Report on Internet voting risks, the statement submitted to the FCC by the Verified Voting Foundation and VVOrganization, and the statement from Dr. David Jefferson.

g. What are the history and current state of play of online voting technologies?

A: Far too broad a question to answer here.

h. What are best practice processes concerning online voting?

A: See the attached article; also, recall that asking for "best practices in internet voting" is akin to asking for "best practices for drunk driving." (per Dr. Ron Rivest, as noted supra). If we are attentive to the risks of the Internet, and the critical importance of honest, transparent, and auditable elections for legitimacy of our government, we don't want to move into Internet voting.

i. How would enabling online voting impact overseas military personnel, overseas diplomatic personnel or other Americans living overseas?

Undoubtedly, these Americans would believe they are participating in a convenient and safe manner in US elections. But the Internet cannot provide at a high degree of assurance that the votes as cast will reach the election offices.

Use of the Internet for transmitting ballot materials, and for providing a range of other election information and services may offer far better risk-benefit ratios, and should be the focus of any Federal or State efforts to use the Internet in voting.

Part B. Brief Overview of the Author's Expertise

Credentials (excerpt) of Professor Candice Hoke

- J.D., Yale Law School; Senior Editor, *Yale Law Journal*
- Professor of Election Law, Regulatory Federalism, and Employment Law; previously taught Federal Jurisdiction, Constitutional Federalism.

- Research Team Leader in the California Secretary of State's *Top to Bottom Review* (TTBR) of Voting Systems (for the Diebold Election System Documentation Team); participated in open-ended vulnerability "red team" testing with the TTBR's preeminent computer security scientists; discussed findings regarding the security, reliability, and accuracy of three major voting systems.

- Consultant assisting in formation of Ohio's EVEREST study of voting system vulnerabilities; planned Election Day 2007 on-site security evaluations for 11 counties (ultimately not funded).

- Co-author (with prominent national security computer scientists) monograph on election forensics for digital elections and other election security reports and academic papers.

- Member of the American Bar Association's *Standing Committee on Election Law, Advisory Commission*, recruited to serve as the voting technology expert. (Three terms, 2007-present)

- Project Director of the *Public Monitor of Cuyahoga Election Reform*, as part of the Center for Election Integrity, in which we conducted unprecedented election security technical and operational assessments for an urban election office (Cleveland, Ohio).

- Member, *Cuyahoga Election Review Panel*, which investigated and published a lengthy report on the nationally notorious 2006 Federal primary in Ohio's most populous urban county; documented many grave failures in election security.

- Testified before Congress (House Administration) on election verification, and also the U.S. Election Assistance Commission on election technology and election accountability issues, including *Tracking Voting System Performance* (Dec. 2008). http://www.eac.gov/News/meetings/12-08-08-public-meeting-washington-d-c

Part C. Election Cybersecurity Memorandum Submission by Professor Hoke to the Executive Office of the President, June 2008 *(slightly revised but not updated or substantively modified)*

"***Election cybersecurity***" here refers to the security of the computers and networks used to record, process, and report the votes, which includes all electronic and electromagnetic communications, including telephony, fax, and Internet, in each case whether wired or wireless, analog or digital.

A. Essential Questions and Answers regarding Election Cybersecurity

1. Are Federal elections currently vulnerable to attacks similar to those that generated the President's cybersecurity review and initiative?

- Yes. Election systems have been among the victims of known, widespread malware attacks, and at least two examples of targeted attacks. Further, election administrators lack the information security expertise to harden their systems and to protect vulnerable information and systems that range from voter registration databases to remote transmissions of election results.

2. Are the information and information systems underlying Federal elections currently within Federal cybersecurity planning and oversight, under the Department of Homeland Security coordination or subject to the Federal Information Security Management Act (FISMA)?

- No, thus far Federal statutory law and administrative provisions implementing the statutes remain silent, and thus exclude, information systems used to conduct Federal elections. Federal elections information security is not specifically listed in prior Executive Orders or in other documents recording administrative implementation of Federal Homeland security. President Obama's cybersecurity Report helpfully mentions "e-voting" as within the scope of Federal concerns, but goes no further. The Help America Vote Act (HAVA) mandates deployment of certain digital information systems without providing Federal authority for:

    - mandatory minimum security or reliability standards;

    - other oversight of the procurement, use, and maintenance of Federal elections information systems;

    - performance data regarding voter registration systems and voting systems, from local or State administrators; or

    - auditing voter registration and voting systems for deterring "mischief," and identifying software bugs and design issues that undermine voter access (eligibility to vote), election results accuracy, and overall election transparency.

- The U.S. Election Assistance Commission, which HAVA charges to facilitate improvements in State management of elections, has not developed a respected track record on election security issues and should not be entrusted with Federal election security coordination.

3. Are there sound reasons that warrant the exclusion of information systems underlying Federal elections from overall Federal cybersecurity planning and protections?

- No. Other areas of shared Federal-State regulatory authority and of private sector commercial activities have been designated as "critical infrastructure" or as a "strategic asset" warranting Federal cybersecurity coordination.

- Constitutional federalism and the traditional role of the State governments in administering Federal elections do not justify the exclusion of vulnerable elections information systems from Federal minimum standards and ongoing monitoring.

    - Federal deference to State governments to protect these information systems is especially unwarranted given the critical importance of democratic elections, the high level of expertise and resources needed to evaluate the risks and properly manage them, and the highly problematic record State election officers (county and State) have amassed thus far on election information security issues.

    - Federal elections infrastructure should be considered as part of U.S. national security infrastructure (though with transparency and public accountability), and as such would seem to be manifestly a federal regulatory responsibility.

B: Evidence of Election Information and Information System Vulnerabilities

1. Voter Registration Systems, including HAVA-mandated Statewide Voter Registration Databases

These databases are not subject to any federal certification or testing, and States have not interposed standards. The local databases range from MS Access, with lax security and significant reliability issues to specially designed and marketed Voter Registration databases (e.g., Diebold/Premier's GEMS) with documented serious design and functional flaws.

- Ohio's Statewide Voter Registration Database (SVRD) sustained an attack in October 2008 that caused the database to be shut down for a period of days; no information was released.

Reuters: http://www.reuters.com/article/domesticNews/idUSTRE49K96820081021
October 21, 2008 "The Web site of the Ohio state agency that handles voter registration and other election information was shut down briefly after it was hacked, an official said on Tuesday, vowing to guard against fraud in the key battleground state in the November 4 presidential contest.

"Ohio Secretary of State Jennifer Brunner said the agency temporarily took the Secretary of State Web site at www.sos.state.oh.us down on Monday after "one or more" security breaches were detected."

- The EAC completed a report on "voter information" websites. The author mentioned in press reports but not in the official report that:
    - Some States placed their statewide voter registration database live on-line, accessible via the Internet, rather than place an image on line.
    - Some States' management of their SVRD gravely endanger voters' personal information, expanding opportunities for identity theft.
- No independent study of the security and reliability of these SVRD has been conducted. These gateways to voting have been shrouded in secrecy.
- The Ohio Secretary of State is planning to use in house technical staff to design and build a new SVRD. No information as been released on his expertise, but it is highly unlikely that this staff member has the security expertise needed, or the other expertise, to design a complex, critical interoperable database such as is needed for SVRD purposes. No Federal standards exist, however, and no "best technical design and practices" guidance.
- Vast numbers of Cuyahoga County voters mysteriously "disappeared" from the GEMS database and were unable to vote in the Ohio 2004 general election. "Updates" were installed to the voter registration database during the fall. No review or assessment occurred as to the contents of the uploaded code.

For documentation and further development of these many of these voter registration points, see AMERICA VOTES! SUPPLEMENT, Chapter 3, *Voting and Registration Technology Issues: Lessons from 2008* by Candice Hoke and David Jefferson (national security cybersecurity scientist at Lawrence Livermore National Labs)

2. Election Tabulation-Management Systems

- Virtually all voting systems use MS Windows operating systems, with their well-documented and continuing severe security problems.
- Few States forbid connection of election tabulation servers to networks; malware has been uploaded.
- Not only have States not issued baseline, technically defensible election information security standards but those that have some standards do not have compliance and monitoring programs to determine and correct compliance.
- At least 7 States currently permit emailed ballots in certain circumstances, and several more are currently considering various forms of Internet or telephonic voting.
- Examples of documented problems follow.

Worms found on the central tabulation system.

Pinellas County, Florida. June 2008. **Two malicious software programs (worms) were found on the central tabulation system.**
http://www.tampabay.com/news/localgovernment/article605711.ece
"The two bugs, known as Flush.G and W32.SillyDC, work in tandem and go from computer to computer redirecting **Internet** browsers to sites the user hasn't selected, officials said. The worm is carried through removable media like USB drives, is easily detected and, officials say, rather harmless." The worms have been removed, and the Secretary of State has released a memo (pdf) urging election supervisors across Florida to take steps, including the use of antivirus software, to protect their voting systems from corruption." Notably, the memo is no longer posted on the Internet.

Virus in Sarasota Database

October 2006. Sarasota County, Florida. An Internet service outage lasting approximately two hours occurred on Monday, 10/23/2006. The outage was caused by an unpatched database server that was compromised by a variant of the SQL Slammer worm. Once the server was infected, it sent traffic to other database severs on the Internet, and the traffic generated by the infected server rendered the firewall unavailable.
This happened on the first day of early voting, and left voters unable to cast their ballots for about two hours. This was the Jennings/Buchanan race, later litigated, and the state court declined to permit forensics reviews requested by the Electronic Frontier Foundation (attorneys).

Blog coverage: http://www.bradblog.com/?p=4480
Register coverage:
http://www.theregister.co.uk/2007/05/17/sarasota_county_network_breached/
Problem report:
http://www.bradblog.com/Docs/SarasotaCounty_SQLSlammerWorm_IncidentReport_102407.pdf

Modem Problems over telephonic networks.

May 2006, Cuyahoga County, Ohio: modem tests over the weekend prior to the election conducted by numerous poll workers and other staff before the election left the tabulation server highly vulnerable for over 72 hours; on election day, numerous modem transmissions failed.
See Cuyahoga Election Review Panel Final Report, www.urban.csuohio.edu/cei

August, 2008. Sarasota County, Florida. When workers tried to count absentee ballots on election night, the ES&S optical scan machines would not communicate with the server. So more than 10,000 absentee ballots had to be hand-counted. "We could not get the absentee ballots totals to upload into the main server to combine all of the totals together for absentee early voting," says Supervisor of Elections Kathy Dent.
http://www.mysuncoast.com/Global/story.asp?S=8911224

"Low Turnout" in Hawaii Internet Election

May, 2009. Hawaii. "For the first time, Oahu voters had to use computers or the telephone to vote for their neighborhood board candidates and many people did not bother." Report of 80% fewer votes in this election.
http://www.kitv.com/politics/19573770/detail.html
Query whether all the votes attempted to be cast arrived at the destination. The vendor did not set up systems to monitor transmission difficulties.

States allowing completed ballots to be returned by email

Eight states allow military voters to return their completed ballots by email. Pew says:
"Unsecured e-mail can expose voters to identity theft, or their ballots could be tampered with. And states cannot be certain that the ballot they are receiving via email is the ballot sent by the military voter."
http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Election_reform/NTTV_Report_Web.pdf

States using/considering Internet voting

Michigan used Internet Voting in a 2004 Democratic primary.
Hawaii used Internet Voting in a 2009 "Neighborhood" election.
Washington State used Internet Voting in a 2009 King Conservation District election.
http://www.prweb.com/releases/2009/04/prweb2292514.htm
Kansas – a bill allowing email return of ballots for military is waiting for the Governor to sign.
Illinois – introduced a bill to set up a commission to recommend Internet voting.

Alabama, Connecticut, Maryland, and Washington – considered email ballots for military, but the bills

Part D. Internet Voting paper delivered in Prague, 2008 (slightly revised)

Internet Voting:

Formulating Structural Governance Principles for Elections Cybersecurity

Candice Hoke

Cleveland State University, USA
{shoke@me.com}

Abstract: *In Europe, the U.S., and Asia, political and market forces seek regulatory approval for Internet-based voting and electoral administrative tasks. Governmental responses have differed, but commonly governments omit Internet and computer security experts from exercising decisive weight in such policy decisions. Given its current architecture and engineering, the Internet provides neither high assurance data security and integrity, nor reliable information transmission protected from denial of service and other attacks. Nevertheless, pressures to expand Internet-based election functions continue. This paper proceeds from the premise that democratic nations have not yet posed the question of what foundational features should be required in an elections governance system that is using (or is pressured to deploy) computer and network technologies. The paper submits that election administrative policy decisions are gravely affected by an information gap regarding both Internet security risks and the availability of effective mitigations for these risks. The paper recommends disaggregating election tasks so that nuanced policy decisions can issue approving the Internet and other computer technologies for specific electoral tasks. It presents seven core understandings that election policymakers must master for capacity to evaluate the relative risks and benefits of proposed computer-based election technologies, including the Internet. It reviews exemplar vendor claims and marketing strategies that misinform policymakers, leading to porous balloting and the possibility of skewed or fraudulent election results. The risks to and profound need to safeguard democratic legitimacy where critical functions are conducted on computers or the Internet thus warrant transnational elections regulatory reassessment. The paper concludes by recommending that revised governance structures incorporate three fundamental principles:* ***expertise*** *in computer and network engineering and security, as well as election administration;* ***transparency and public accountability,*** *in order that the election system and reported results have legitimacy; and* ***transnational cooperation*** *among democratic republics, to facilitate prompt mitigations and criminal prosecution for attacks on election information systems.*

Key Words: Internet, voting, elections, governance, transparency, security, assurance, integrity, cybersecurity, mitigations, threats.

1 Introduction

The citizens of democratic republics select their core representatives through periodic public elections. While the specific offices subject to election and the frequency of holding elections varies among nation-states, electing new governmental officers often impacts business opportunities, individual and business wealth, the use of military power, and a broad range of other governmental policies. A national election in the most populous nations worldwide can affect vast wealth and the course of domestic and international events.

The potentially high stakes of elections, and the history of intentional electoral disruptions and fraud in numerous countries worldwide, counsel governmental officials to engage in careful planning in order to protect election information and processes from deliberate attacks. Security and contingency planning for elections differs among and within nations, with some significant variations in the physical contexts for conducting elections and in human factors such as poll staffing. For those nations that use computer technologies for election administrative functions, election security has become increasingly complicated.

This paper proceeds from the baseline fact that the Internet as currently architected and engineered provides neither high assurance data security and integrity, nor information transmission reliably impervious to deliberate targeted attacks and ubiquitous malware. While these factors pose dangers for many entities and activities, elections are especially vulnerable. That voting occurs using anonymized data presents major hurdles to utilizing the Internet in a secure manner for casting ballots, though careful analysis and appropriate mitigations might permit other election tasks to be securely conducted..

The paper argues that election policy decisions are affected by an information gap regarding both Internet security risks and the absence of effective mitigations and controls that can achieve assured election data and system integrity. It recommends revised national governance structures based on three fundamental principles: ***expertise*** in computer and network engineering and security, but also in election administration; ***transparency and public accountability,*** in order that the election system and reported results have legitimacy; ***transnational cooperation*** among democratic republics, to facilitate prompt mitigations and criminal prosecutions.

2 Current and Projected Uses of the Internet in Elections

The pace of election administrative computerization appears to be rapidly increasing. Manufacturers of business automation systems have accelerated development of product adaptations for elections. In the wake of the notorious U.S. presidential election of 2000, passage of the Help America Vote Act [1] stimulated vast computerization of elections. The Act has spurred an array of new options in computer-based and networked equipment. In other nations, both market and "modernization" pressures have led to wide use of computers for election

functions. Many European and Asian nations have joined the U.S. in using or planning transitions to electronic voting devices, tabulation systems, and a broad range of other equipment.

Electronic equipment is now available that permits automation of most election functions, ranging from the creation of voter registration lists to the presentation of an electronic ballot to voters, to recording votes, and to tabulation and reporting election results. Electronic databases often substitute for paper-based systems for retaining the lists of eligible voters and their personal information such as address, birth date, unique identifying number, and political party. Voters may register to vote by visiting a website or by sending a registration document by email attachment or fax. Software is increasingly used to design ballots, including automating the task of rotating candidates into the favored top position on different ballots so no one candidate holds that advantage. Many voting machines use electronic ballots that humans have created on servers using complex election management software.

Electronic voting devices may offer voters the option of ballot correction where the ballot contains marks for too many candidates in a race ("overvoting"). Vote data may be recorded on removable digital memory media as well as on internal components such as flash memory in order to produce "redundant" vote data records.[1] Voting devices may incorporate hardware and firmware for network transmission of election information, including for sending vote data electronically from remote polling locations; these transmissions may occur using the Internet, T1 or common telephone lines instead of physically transporting memory devices such as thumb drives and memory cards. From security and data integrity standpoints, arguably the most problematic electronic voting initiatives are efforts to permit remote voting from personal computers that use operating systems documented to have serious security flaws. These deficiencies are then compounded by the security issues of current Internet architecture. [2]

2.1 Absentee Ballot Transmissions Jurisdictions often allow voters to request "absentee" ballots when the voter will be physically absent on Election Day. Others permit "no-fault" or convenience voting from home, regardless of the reason. These requests or applications formerly were confined to paper documents sent through traditional mails or delivered by hand. Technological options have expanded to include, depending on the jurisdiction, applying at a website, by email, or by fax.

Absentee ballots are the crucible for aggressive expansion in the election system's use of Internet data transmissions. The pressure in the U.S. arises mainly from efforts to ensure that those in overseas military service are not inadvertently disenfranchised by delays in ballot transmissions. [3] Sending blank or unvoted ballots to absent and overseas voters has traditionally occurred by mail. Some election offices are now using the Internet to transmit the blank ballot to the absentee voter. Yet other jurisdictions ranging from Estonia [4] to a U.S. pilot project in Okaloosa, Florida [5] have experimented with casting ballots -- voting in an actual election -- on a website described as "secure," by using an encrypted emailed ballot, or by using telephonic networks. These options theoretically permit almost instantaneous delivery of both balloting materials and the return voted

[1] Independent "red team" or penetration studies of voting systems have demonstrated that the supposed redundant memory systems may be subject to deliberate attacks that can cause the various locations to hold discrepant rather than redundant vote totals. [1], [2]

ballots, shortening the transmission time by at least 90% over the time required by traditional mailing of paper.

The authenticity of a voter's absentee ballot signature is increasingly verified by electronic means, using a digital or optical scanner connected to a computer that compares the signature on file with the signature on the submitted absentee ballot envelope. High volume urban election offices have often been first to adopt this technology. Originally developed for financial institutions that process bank cheques, these systems compare the voter's two signatures as part of the voter and ballot verification process. The machines must be calibrated, allowing discretionary human decision in the degree of deviation between the signatures on record and the absentee ballot materials.

2.2 Integration of Telephony and Other Networks. Networks used in elections encompass more than the Internet, however. In addition to telephonic transmissions of some electoral information, ballot tabulation systems often use components linked by Ethernet. Election software produces race results from raw database values, which officials then upload to the Internet for public access using network connections or memory media.

2.3 Other Electoral Uses of the Internet. Some vendors send election "management" software patches over the Internet for uploading into the local election equipment. The software systems that require patches are used for ballot configuration and for tabulations. Software patches are also sent via the Internet for updating the voter registration databases. Electronic poll-books can be used to connect poll workers to the voter registration database in order to verify the voter's eligibility to vote; these often communicate via the Internet. The electronic ballot files that are used for printing paper ballots may be posted on the Internet for proofing by political parties and the candidates. These ballot configurations can then be transmitted over the Internet to the ballot printer so the printer order may be fulfilled.

2.4 Disaggregating Election Tasks for Security Assessments

Established precepts of information security assessment direct that each task or function sought to be conducted using computer or network technologies must be separately evaluated in a threat assessment. [19], [20] Such disaggregation may result in identifying election administrative tasks to which the Internet presents low risks and compensating efficiencies. Examples include the Internet posting of voter information regarding the candidates, ballot issues, and location and timing of voting. Web-based additional "voter services," such as the posting of absentee ballot applications and voter registration forms, are also potentially low-risk.

3 The Election Equipment Marketplace Meets Internet Security Science

Security has become a primary focus for Internet participants and information system administrators, in both the private and public sectors. The firm or enterprise IT governance decisions must include types of access controls, authentication systems, and life cycle security. The popular press has covered major intrusions into supposedly "secure" networks that have compromised credit card and other personal financial data, telephone billing records, and the U.S. government's witness protection program. These reports underscore that the Internet generates

significant vulnerabilities at the same time as benign opportunities for broad communication. [21] The Internet places in jeopardy core human values such as personal privacy. [22] [23] [24]

In market-based nations, private sector, for-profit firms design, manufacture, and market specialized software hardware components for election administration. Many of these firms have been shown to overstate their voting system products' compliance with fundamental tenets of an Information Technology (IT) Security Program and misrepresent the scope of activities needed to achieve defense in depth.[2] In independent studies, computer and security scientists have documented profound risks to election data integrity and equipment reliability owing to insecure equipment and flawed managerial security policies. [6], [7], [11], [12], [13], [14], [15].

Internet-based software systems for voter authentication, ballot delivery and return of votes or "voted ballots" are no longer fanciful speculations. Private sector vendors are promoting their new wares for "secure Internet voting," replete with resuscitation of the false but previously persuasive analogy of voting to banking via automatic tellers and personal computers. The new Internet voting vendors are actively soliciting election officials to purchase their software products that will enable voted ballots to be transmitted over the Internet for tabulation in elections offices. In May 2009, one Internet voting marketing executive argued:

> The introduction of technology to any process is scary. But the time has come. We have been banking online and shopping online for over a decade, and conducting important business by phone for a century. *Digital technology, while no panacea, is the best method ever invented for securely delivering information and decisions*. [25]

3.1 Vendor Claims. The vendors' marketing claims include that the Internet:

- Permits voting to be as secure and private as personal banking transactions;
- Will achieve a net reduction of the financial costs of conducting elections;
- Will expand voter participation in the electoral system by making voting more convenient and accessible; and,
- Should be accepted as part of social and technological progress, of updating systems to accommodate youthful tastes and expectations (the "cool" factor).

3.2 Two Empirical Baselines. In considering the fitness of the Internet for conducting particular election administrative tasks, and the wisdom of permitting a *caveat emptor* market for Internet voting software in lieu of governmental regulation, two constellations of empirical fact should be kept in view. First, the profound security deficiencies independent researchers documented in privately produced, for-profit digital voting equipment[3] (despite the contrary vendors' representations) should raise questions regarding the credibility of election vendors' claims that the new voting products "securely" deliver voted ballots and voting materials over the Internet. In

[2] Documentation reviews of three commercially produced voting systems formed a part of the California Secretary of State's Top to Bottom Review of Voting Systems. All evaluators reported critical omissions in security documentation and risk mitigation. [8], [9], [10]. Principles for achieving defense in depth in election information systems are not qualitatively different from those established for IT systems for other facing significant threats. [6]

[3] In the "red team" overview report on California voting systems, Dr. Matt Bishop stated: "the security mechanisms provided for all systems were inadequate to ensure accuracy and integrity of the election results and of the systems that provide those results." [6] With only minor differences, these same systems are used in many other States.

short, the electronic elections industry equipment's past security representations have misrepresented the systems' security achievements, and the industry has chosen to market equipment that presents major risks to election integrity. [8], [9], [10], [11], [13].

The second but perhaps more significant empirical baseline relates to the Internet's technical and engineering facts. The Internet lacks the capacity for high assurance information transmissions and information systems, whether for elections functions, military communications, or other transactions. Specific election objectives include packet transmissions that cannot be delayed, blocked, modified, or intercepted, because otherwise voter disenfranchisement and possibly a fraudulent election will ensue. [2] Election-related websites, for instance, that are designed for distributing voter information, for enabling voter registration, or for casting ballots, continue to be vulnerable to malware, denial-of-service (DOS) and distributed DOS attacks. Underestimating the volume demands for website access for a major election can also gravely impair election outcomes and vitiate the election's legitimacy. Mitigations that reduce these threats to minute levels of potential impact are not available or foreseeable in the near future.

3.3 Private Vendors, Market Pressures and the Internet Security Information Gap. In addition to lacking computer security training, policymakers empowered to decide which election functions to automate using IT systems may well lack sufficient knowledge to evaluate the types and impacts of risks that are endemic to such systems. At least six core insights are needed by those vested with decisional power concerning when and how the Internet shall be used in election functions.

- ***3.3.1 Pervasive software coding deficiencies and their election consequences:*** Sometimes popularly termed "bugs," coding deficiencies have been identified to pose grave security consequences for all IT systems. [16], [17], [18] These coding errors open election software to easy, high impact attacks on election systems and data that may easily escape detection and redress, but the errors can also lead to data inaccuracies and machine unreliability having no basis in deliberate attack.

- ***3.3.2 Internet transmitted malware and options to manipulate data speed:*** The worms, viruses and other ubiquitous malware can impair election functions, as can strategically timed high Internet data volume that can cause speed of transmissions to fall precipitously.

- ***3.3.3 Labeling election technology products and websites as "Secure" and "Reliable":*** In contrast to the labeling requirements for prescription drugs, many food products, and dangerous chemicals, governments have generally not restricted vendors from using these quasi-scientific, psychologically seductive terms in their marketing literature and presentations. Even though the terms deceptively suggest compliance with accepted standards for security, governments have permitted their use.

- ***3.3.4 Re-transmitters access and consequences for information privacy and security:*** Third-party re-transmission sites such as ISPs permit some ISP employees the access to read message contents. This intrusion does not require sophisticated technical abilities or equipment, but only a text viewer or word processing program. The fundamental insecurity of these transmissions means that email forgery or modification, identity theft, and business transaction interceptions are becoming major types of criminal fraud. The SERVE Report

continues to stand as a comprehensive typology of Internet voting threat genre, most of which are insoluble with current architecture and engineering. [2]

- ***3.3.5 Encryption does not suffice***: Data encryption is not a complete or effective mitigation for most threats Internet information transmissions pose for elections .[2]

- ***3.3.6 Concealed, untraceable attacks yet the appearance of information security:*** Attacks that disrupt election processes, or result in fraudulent election totals, may be completely hidden and untraceable. [2]

- ***3.3.7 Security mitigations and Internet re-engineering solutions that will achieve high assurance are not imminent:*** Funding entities such as the U.S. National Science Foundation are underwriting major research efforts to re-envision the Internet. [26] As a result of this multi-faceted research, potentially radical revisions to Internet architecture, engineering, and communication protocols may occur. The transformations may, for instance, include multiple "Internets" with controlled network access and other enhanced technical security features. But these will not be available in the near future, and probably not for another decade or longer.

Even if current or future research endeavors successfully achieve high assurance security architecture and engineering, computer security science teaches that these do not comprise the entirety of factors relevant to evaluating information security risks. Computer and network security is not an output of merely technological attributes. Rather, physical security (such as locks on doors and surveillance cameras), staff expertise, staff continuing education and values commitment to security compliance, and other factors can play as significant a role in the security quotient as the technological features. [6] Further, physical, managerial, and staffing contexts within which the election technologies are deployed will not be static. Thus, threat analysis and policy formation must occur in a dynamic manner, a task that an effective elections cybersecurity agency should undertake.

4 A Governance System for Internet-Based Election Tasks?

Unquestionably, the Internet offers profound democratization and communicative benefits that should not be impeded[4] without a sound basis in other fundamental democratic elections values. The Internet need not be placed off-limits to deployment in elections. However, the rapid commercialization of the Internet and World Wide Web in ways incompatible with individual and the larger public interest raises concerns that election processes could be similarly skewed. As Peter Neumann and others have noted, such incompatibilities have surfaced in domain name policy, spam, security, encryption, freedom of speech issues, privacy, content rating and filtering, and many other areas.[24], [25] The governance systems that determine how to use the Internet in election administration must have the capacity to evaluate the risks soberly without becoming enmeshed in overly rosy technological utopianism or subject to regulatory capture by for-profit vendors. The structure should require, and the governance culture embrace, the duty to protect the integrity of elections processes.

[4] Michael Froomkin reviews strategies for achieving the communicative and democratizing opportunities the Internet offers as a part of his overall assessment of Internet governance structures. [21]

The proposal outlined here recommends a national regulatory apparatus that will not rely predominantly on issuance of rules and technical standards to be met, or particular product design. Rather, it should review and issue particularized decisions on whether an election office proposal for using Internet transmissions for a specified election task is permissible in light of all factors relevant to security based on layered defense. Thus, governance personnel would need to remain abreast of technical and security developments, and obtain information on staff education and security physical contexts, in order to decide the question before it.

The analogue in the Anglo-American legal system would be courts of chancery, where equitable review employed principles to guide wise decisions in light of all the facts, rather than use mandatory common law precedents to compel certain outcomes.

Recognizing that information security is one objective among many, the agency will need to be structured to maintain personnel with election administrative knowledge and not only those with technical and security training. The range of expertise would facilitate balancing the competing objectives of speed of transmission, low administrative costs; auditability; reliability; environmental impact; and voter convenience/access as against data security.

4.1 Regulatory Scope and Definitions

Elections cybersecurity[5] recognizes that the election information systems hold valuable information that both outsiders and insiders may seek to compromise. The underlying policy objectives are to prevent or to neutralize potential negative consequences for voters and the election process because computers, networks, and information technology systems transmissions were used. The negative impact to be avoided may arise from deliberate attack, such as disruptions of electoral processes via DOS or viral attacks, and undesired intrusions that can produce fraudulent election records, such as by malware or unauthorized access to databases for manipulating voter registries or vote totals. Election cybersecurity also seeks to protect the personal and other data held within the election administrative system, where unauthorized access can lead to identity theft.

4.2 Principles for Trustworthy Public Elections

At present, the international community has not generated a common set of standards for democratic elections or even agreed on criteria for assessing the adequacy of election processes. The Carter Center's Democracy Program has urged the international community to recognize the need for election observation organizations to work collaboratively work to build consensus on criteria for assessing elections, including electronic elections.[i] Other commentators and courts have offered their views of fundamental election integrity principles based on the constitutional law of their nation. [27], [28], [30]

[5] "*Election cybersecurity*" encompasses the objectives of information and system security, reliability, and data integrity with regard to the computers and networks used to record, process, and report election-related information at all points in the electoral process. The term encompasses all electronic and electromagnetic communications including telephony, fax, and Internet, in each case inclusive of wired and wireless, analog and digital systems. The term reflects one facet of the more comprehensive systemic governmental duty to achieve election integrity.

Increasingly, courts and commentators are urging that election law include as fundamental rights principles of transparency and public accountability for election processes. [29], [30] Germany's high court invalidated certain uses of computers in elections, resting its decision on the core requirement of election transparency to the public. The Court emphasized the "principle of the public… which prescribes that all essential steps of an election are subject to the possibility of public scrutiny unless other constitutional interests justify an exception." [30] In the Court's view, the voters themselves must be able to understand without detailed knowledge of computer technology whether their votes cast are recorded in an unadulterated manner as the basis of vote counting, or at any rate as the basis of a later recount. If the election result is determined through computer-controlled processing of the votes stored in an electronic memory, it is not sufficient if merely the result of the calculation process carried out in the voting machine can be taken note of by means of a summarizing printout or an electronic display.

Translating the core principles for trustworthy elections into computer security terminology, elections must maintain in demonstrable ways data integrity at all points in the process; assure the availability of systems for voters to register and to cast valid ballots that will be counted; and, provide accountability systems such as random auditing that will provide public transparency and equipment checks. Election technology security and auditing features can be designed to achieve each of these objectives, but often software vendors do not invest in developing effective security. As one computer security commentator has noted, "the buying public has no way to differentiate real security from bad security." [18] A better regulatory apparatus can facilitate product development that meets higher standards of software security in the elections arena, without the need for expanding use of product liability lawsuits for defective software products.

4.3 Recommendations for the Elections Cybersecurity Regulatory Structure and Powers

4.3.1 Dynamic Decisionmaking

At the threshold level, two regulatory paths can be identified as potentially offering sufficient election cybersecurity policy determinations: (1) An aggressive, bright line approach: codification of a legal barrier to any use of digital equipment, of equipment that depends on software and networks, for any mission critical election task within the electoral jurisdiction; or (2) creation or revision of a regulatory apparatus that reviews applications and can authorize election administration to use digital equipment and networks for some election tasks under specified conditions.

While a complete barrier might appear to provide the most substantial election cybersecurity protection, its rigidity and overbreadth would render it an unstable policy approach. It would also invalidate many current practices without any review of the alternatives and their risk factors. Given that risks and technological options change over time, a more dynamic regulatory approach would be more prudent. The law could vest the regulatory entity (hereafter termed Board) with conducting sophisticated security assessments in light of all relevant factors known when the application is reviewed. This approach would be more consistent with the dynamism of the technologies and risk environments, allow review of the applicant's most recent record on security policies implementation, and other facts.

4.3.2 National Supervisory Authority

Where the government must capably respond to external threats that are dynamic rather than static and that present threats to the entire nation, it is appropriate for the regulatory entity to be positioned at the national level. Economies of scale and heightened expertise can be achieved that preserve scarce resources. Given cybersecurity's dynamic set of serious threats, it is unrealistic to expect that local and Provincial/State governmental authorities will have the resources, the expertise, and the political will to invest in oversight of elections cybersecurity issues.

4.3.3 Structure and Staffing

A regulatory structure that can balance the need for diverse political involvement and public accountability with the need to utilize appropriate expertise is an independent Board with a professional staff. A statute could allocate to national legislative and executive leaders the power of appointment. Nominations of technical and security professionals could be allocated to qualified professional organizations as an extra assurance for appropriate expertise. Legislative leaders of varying major parties could be vested with power to appoint without a nominating intermediary experienced election administrators and public interest advocates on election transparency, privacy and security issues.

Professional associations having expertise in the requisite areas, such as the ACM and the IEEE, could be vested with the power to nominate a short list of experts with statutorily specified credentials.[6] The law could name high official (e.g., President or Prime Minister) to review nominees and appoint them to office for a specified term of office. Avoiding service at the pleasure of the appointing officials would help to ensure that the Board's decisions are evidence-based and not a matter of political influence.

The Board's cybersecurity work would require a professional staff. In some nations including the U.S., elections administrative processes have often been staffed with political patronage appointees who sometimes lacked the skill set and knowledge base needed to run administratively competent and secure elections. A national elections cybersecurity Board can provide a counterbalance. The permanent staffing expertise could be specified by statute and direct:

- Significant technical expertise be present (including network security, computer security, secure database and database management expertise, software development and testing; IT auditing and computer/voting system forensics);
- Significant election administration expertise, preferably having experience in computer-based election technologies and a record of achievement in implementing election security best practices, achieving a security culture, and establishing effective auditing and accountability systems;
- The Board and staff to engage election officials "in the field" – in their election offices and on-site in actual elections -- and with States' chief election officers to promote informational interchanges about the complexities and risks presented by election technologies and their possible mitigations
- Board and staff executives have both information systems and security expertise plus election administrative experience;
- Satisfaction of high personal and professional ethics standards.

[6] If international professional organizations such as the ACM, IEEE, and ISACA were each to develop the capacity for national divisions within specialized expertise, lodging nominating powers there might be less controversial.

4.3.4 Sophisticated, Nuanced Cybersecurity Assessments

While renowned computer and network security experts appear to agree that security is a series of complicated tradeoffs, [6], [23], [34] not an abstract property of equipment or systems, structuring a regulatory agency to undertake informed, nuanced and voter-protective cybersecurity evaluations is qualitatively different task than training individuals in these skills. Regulatory entities are often subject to political appointee leadership who might lack critical knowledge or capacities for sound judgment. The regulated firms often seek and sometimes achieve "regulatory capture." Flawed personnel decisions can vitiate a sound structural approach that is designed to achieve the nuanced decisions needed for national and election security-sensitive policies.

Despite the risks that the regulatory entity may not be staffed or structured well, the status quo presents too many risks for its continuation. By combining explicit requirements for expertise and public accountability, the regulatory framework may enhance the likelihood that nuanced, sound judgments will issue.

Given that effective computer security is virtually never strictly a property of technical equipment but rather a function of the interaction of people (including security training and practices), equipment features (such as avoidance of software coding errors known to introduce vectors for attack) and physical circumstances (including physical security, such as locks and video surveillance), regulatory systems dedicated to achieving high information and information system security cannot evaluate only the equipment's technical features. In the U.S., for instance, the Voluntary Voting System Guidelines and accompanying federal lab testing program commits precisely this error, among many others. [33] Highly laudable technical and network security features can be negated by human errors and omissions. Conversely, poorly designed software and other technical security deficiencies can be somewhat mitigated by security practices including staff compliance assessments. [6] "Layered defense" security principles prescribe multiple levels and types of security mechanisms, to force an attacker to breach several rather than only one to compromise the system. The Board should be charged to evaluate all defensive layers when determining the acceptability of a proposed use of the Internet in election functions.

4.3.5 Initial Decisions and Burden of Proof

The Board will face threshold decisions concerning which election administrative or voting tasks that are currently using the Internet can continue to do so and under what conditions. The Help America Vote Act of 2002, [35] by contrast, in some respects appears to assume that all election related activities can be securely conducted over the Internet -- a flawed assumption. [36] [2] The law could impose the burden on proof that the on the applicant for permission to utilize the Internet, with a required showing that risks to election data security and integrity are highly remote and very low in potential impact. The risk of nonpersuasion would thereby be legally reposed in the applicant.

Another structural mechanism by which to protect the voting public and election integrity could be to require a specified supermajority of Board members, for instance,75% or 85% of the members, to approve any proposed elections use of the Internet as sufficiently secure.

4.3.6 Specific Powers and Duties

The Board could be vested with broader statutory authority to protect election security and integrity, including for instance:

- The authority to identify election practices and procedures, such as connecting an election tabulation server to the Internet, that present grave security threats, and have the power to require cessation of the practice.
- The power to issue binding technical, operational, and other *minimum* standards for each discrete election function that is permitted to be conducted over the Internet or other networks, and to bar functions if network involvement presents significant risks to the security, reliability, ballot secrecy, and accuracy of elections.

If a bright line statutory barrier to Internet delivery of voted ballots should be contemplated instead of vesting the power in the Board, three major arguments will be raised that these questions should be subject to a more nuanced agency decision making process. First, in those nations that maintain a two-stage election tally process, where preliminary or unofficial vote tallies are followed by more a more careful thorough canvass (often known as the official or certified results), the claim will be that any intrusion into networked tallies and transmissions of voted ballots can be corrected at the official count. Thus, use of networked communications should not be off limits for transmitting preliminary tallies and voted ballots.

Second, arguments will be lodged that where Internet communications are permitted to be used for delivery of voted ballots and vote tallies, whether for unofficial or official tallying, rigorous auditing will deter attacks and also permit correction of tallies if attacks should occur. While rigorous auditing indeed should be mandatory, its limits must be recognized. While auditing is a commonplace in government and business financial matters, auditing elections remains quite novel with nascent professional standards. When pressed to audit elections, governments often claim to "audit" without using, for instance, random sampling procedures, auditing every contest, or using statistical auditing models that provide a 98% degree of confidence that the audited races' results were correctly reported. Post-election auditing cannot function as a reliable check on networked election communications as through the Internet, nor can it recover blocked ballots or tampered

Finally, in some locations, internal election administrative culture urges employees not to disrupt public confidence in the agency or its electoral process by reporting irregularities. Given that some administrators would have decided to use vulnerable networked transmissions, tacit or explicit pressures may be placed to confirm that no mischief occurred in the original transmissions or other discretionary tallying processes, rather than might reveal the flawed planning and ignorance of the serious risks.

Legislation can remove from the arsenal of discretionary local and State decision making the options that imperil election integrity. The legislature need not conclude that voted ballots and vote tallies can never be securely transmitted over networks such as the Internet, but rather recognize that the array of prerequisites and resources required, such as exceptional expertise, contingency planning, ongoing training, and special equipment, to effectively manage and respond to the dynamic development of cyberthreats, does not warrant discretionary authority be placed outside the national Board. Allowing the local governments to be more security conscious than the national Board should remain within the permitted range.

4.3.7 Achieving Public Accountability and Effective Cybersecurity Compliance

To achieve transparency and accountability objectives, [37] the Board must be subject to "sunshine" laws that compel an agency to publicly post its activities, actions and documents, and conduct its decision-making sessions in the public domain. These requirements would necessitate that security clearances and classified information not be presented to the Board.

To achieve the accountability needed for public confidence and legitimate elections, the elections cybersecurity statute should also:

- Authorize the Board's rulemaking powers to encompass procedures to guarantee meaningful end-to-end auditability and accountability for every ballot, including those transmitted electronically or electromagnetically;
- Vest the Board and the national Justice ministry with concurrent authority to commence an investigation into any violation of the elections cybersecurity rules;
- Direct the Agency to initiate a process by which citizens can provide notice to it of alleged violations of elections cybersecurity rules, shield their identity from public disclosure, and provide effective whistleblower protection from adverse employment consequences to those who report possible elections cybersecurity violations.

4.4 Transnational Cooperation

Internet and information security threats are systemic and world-wide. Sharing information on election cybersecurity risks and attempted attacks can augment mitigations and criminal prosecutions. Internationally negotiated procedures will be needed.

4.5 The U.S. Election Assistance Commission

The chief federal agency acting on electoral administrative issues is the U.S. Election Assistance Commission (EAC). An extensive analysis of the EAC's structure, powers, staffing, and record on technical issues in elections leads to the conclusion that a different agency, likely located within the Department of Homeland Security, should be vested with the powers to regulate the electoral functions that could securely utilize the Internet. [38] The EAC has no national security expertise, and the agency record shows that it has lacked both appreciation of the risks that inhere in the Internet and the types of technical expertise requisite to manage complex computer networks when election tasks are concerned.

5 Conclusion

Internet security experts might analogize the Internet to a swiftly moving river within which information can be trapped or modified with the ease of trout fishing in a well-stocked backwoods stream. But at the elections policy and equipment procurement levels, the Internet security information gap means the Internet is hazily viewed as analogous to an armored currency delivery truck, protected by security guards who are trained and equipped with weapons befitting paramilitary officers. Thus protected, they mistakenly gauge cause as an extremely remote possibility the likelihood of intercepted or fraudulent information deliveries.

The computerization and networking of governmental functions including elections, the critical importance of election legitimacy, and the serious Internet security information gap warrant innovative thinking and redesigned governmental structures. Democratic governments must structurally assure that appropriate technical and security expertise plays a decisive role in policy decisions concerning election administrative use of the Internet. ican be structured to manage elections cybersecurity, thus providing far better voter and national security protection than available previously.

Acknowledgements

The author is indebted to Dr. Matt Bishop, Dr. David Jefferson, Dr. Barbara Simons, and Dr. Gene Spafford for suggestions but they shoulder no responsibility for errors and omissions. Research assistance was provided by Pleurat Dreshaj.

References

1. Help America Vote Act (HAVA), 42 U.S.C. §§ 15301- 15545.

2. Jefferson, D., Rubin, A. D., Simons, B. Wagner, D. , A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE) (2004), http://www.servesecurityreport.org/

3. PEW CHARITABLE TRUSTS, NO TIME TO VOTE: CHALLENGES FACING AMERICA'S OVERSEAS MILITARY VOTERS 6 (2009), http://www.pewtrusts.org/our_work_report_detail.aspx?id=47922&category=488

4. ALVAREZ, R. M., HALL, T.E. ELECTRONIC ELECTIONS: THE PERILS AND PROMISES OF DIGITAL DEMOCRACY (2008).

5. Operation Bravo Foundation, http://www.operationbravo.org/pilot_projects.html

6. Bishop, M., *Overview of Red Team Reports,* Office of the Secretary of State of California, 1500 11th St, Sacramento, CA 95814 (2007) http://www.sos.ca.gov/elections/elections_vsr.htm

7. Bishop, M., Blaze, M., Vigna, G., et al., *University of California Red Team Reports on Voting Systems* (2007), http://www.sos.ca.gov/elections/elections_vsr.htm

8 HOKE, C. AND KETTYLE, D., DOCUMENTATION ASSESSMENT OF THE DIEBOLD VOTING SYSTEM (2007). http://www.sos.ca.gov/elections/elections_vsr.htm

9. Hall, J. L., Quilter L., Documentation Review of the Hart Intercivic System 6.2.1 Voting System, http://www.sos.ca.gov/elections/elections_vsr.htm

10. Burstein, A. J., Good, N. S., Mulligan, D.S., Review of the Documentation of the Sequoia Voting System, http://www.sos.ca.gov/elections/elections_vsr.htm

11. Bishop M., Wagner, D., *Risks of E-Voting*, Communications of the ACM, 50(11), p. 120 (Nov. 2007).

12. Neumann, P. *Illustrative Risks to the Public in the Use of Computer Systems and Related Technology*, 1.22 Election Problems
http://www.csl.sri.com/users/neumann/illustrative.html#25

13. BISHOP, M., GRAFF, M., HOKE, C., JEFFERSON, D., PEISERT, S., RESOLVING THE UNEXPECTED IN ELECTIONS: ELECTION OFFICIALS' OPTIONS, Appendix 2: Partial List of Voting Systems Studies (Oct. 2008) http://www.electionexcellence.org/

14. Commission on Electronic Voting (Ireland), First Report (Dec. 2004)
http://www.cev.ie/htm/report/first_report/part2_5.htm

15. Hoke, C., *Public Monitor's Memorandum on Possible Legal Noncompliance in the November 2006 General Election* at www.urban.csuohio.edu/cei

16. *Experts Announce Agreement on the 25 Most Dangerous Programming Errors - And How to Fix Them: Agreement Will Change How Organizations Buy Software*,
http://www.sans.org/top25errors/

17. *MITRE,* Common Weakness Enumeration, www.cwe.mitre.org/top25/

18. Schneier, B., *The Process of Security*, Information Security Magazine, April 2000
http://www.schneier.com/essay-062.html

19. Regenscheid, A. & Hasting, N., *A Threat Analysis on UOCAVA Voting Systems*, NISTIR 7551,
http://vote.nist.gov/

20. BISHOP, M., INTRODUCTION TO COMPUTER SECURITY (2004).

21. Froomkin, A. M., *habermas@discourse.net: Toward a Critical Theory of Cyberspace*, 116 Harv. L. Rev. 749 (2003).

22. Schwartz, P. M., *Privacy and Democracy in Cyberspace*, 52 Vanderbilt L. Rev. 1609, 1614 (1999)

23. Neumann, P. G., *Illustrative Risks to the Public in the Use of Computer Systems and Related Technology,* ACM SIGSOFT Software Engineering Notes 21:1 (1996),
http://portal.acm.org/citation.cfm?doid=381790.381797

24. Neumann, P. G., *Risks in Trusting Untrustworthiness,* CACM 46: 9 (2003)
http://portal.acm.org/citation.cfm?id=903893.903924

25. Cortorer, A., America's Newest State Holds America's Newest Election (May 2009) http://www.huffingtonpost.com/aaron-contorer/americas-newest-state-hol_b_203639.html

26. Workshop on GENI and Security, January 22–23, 2009, University of California at Davis, Davis, California, USA http://seclab.cs.ucdavis.edu/meetings/genisec/

27. The Carter Center, Democracy Program, Declaration of Principles for International Election Observation, http://www.cartercenter.org/peace/democracy/des.html

28. Jones, D., *Developing a Methodology for Observing Electronic Voting,* http://www.cartercenter.org/peace/democracy/des_e_voting.html (Oct. 2007).

29. Hoke, C., *Trustworthy Elections? The Way Forward,* http://fora.tv/2008/07/03/Candice_Hoke_Restoring_Legitimacy_to_Our_Election (Chautauqua Institution Lecture in the *Restoring Legitimacy to Our Elections* week, July 3, 2008).

30. Federal Constitutional Court (Germany), Press Office, Use of Voting Computers in 2005 *Bundestag* Election Unconstitutional, No. 19/2009, 3 Mar 2009.

31. Tokaji, D., The Paperless Chase: Electronic Voting and Democratic Values, 73 Fordham L.R. 1 (2005).

32. Pinkerton, J. P., Will Democrats Become a Permanent Majority Thanks to Internet Voting? http://foxforum.blogs.foxnews.com/2009/05/26/pinkerton_democrats_internet/.

33. U.S. Election Assistance Commission, Voting System Test Laboratory Program Manual (July 2008, http://www.eac.gov/program-areas/voting-systems/

34. Schneier, B., Secrets and Lies: Digital Security in a Networked World 12, 15 (2000, 2004).

35. Help America Vote Act, 42 U.S.C. § 15385.

36. National Institute of Standards and Technology, Initial Project Plan for NIST UOCAVA Efforts, http://www.eac.gov/program-areas/voting-systems/

37. President Obama, Memorandum For The Heads Of Executive Departments And Agencies (Jan. 21, 2009) http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government/

38. C. Hoke, *Evaluating the Federal Voting Technology Regulatory Record* (forthcoming).