"Developing a Framework to Improve Critical Infrastructure Cybersecurity"

Under Executive Order 13636 [2] ("Executive Order"), the Secretary of Commerce is tasked to direct the Director of NIST to develop a framework for reducing cyber risks to critical infrastructure (the "Cybersecurity Framework" or "Framework"). The Framework will consist of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks. The Department of Homeland Security, in coordination with sector-specific agencies, will then establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities.

NIST has issued a Request for Information (RFI) in the Federal Register here: https://federalregister.gov/a/2013-04413. It is to this RFI that our response pertains.

The undersigned persons and organizations include experts on matters relating to election technology, election practices, encryption, Internet security, and/or privacy. We appreciate the opportunity to provide input on this RFI entitled "Developing a Framework to Improve Critical Infrastructure Cybersecurity".

Our response focuses on the discussion of specific practices as they pertain to elections practices and systems as part of the nation's critical infrastructure.

I. INTRODUCTION

I-A. Voting Systems As Part of Cyber Security Critical Infrastructure.

Protecting the physical security of critical assets must include protecting the integrity of the nation's voting technology, including technology we use for voter registration and support for election services. Much of our voting technology is purchased or leased by election officials from private vendors and is proprietary. As far back as 2005, the Congressional Research Service (CRS) commented in a report entitled "Creating a National Framework for Cybersecurity: An Analysis of Issues and Options" as follows (emphasis added):

> "*Voting Systems*. State and local government are categorized as a CI sector, and like other sectors, they rely increasingly on information technology to provide crucial services. One example is voting systems. Four out of five American voters now cast ballots using systems that rely on computers for casting, counting, or both. While not generally considered part of critical infrastructure, voting systems are central to the functioning of government. Concerns have been raised by many computer security experts about the vulnerabilities of current computer-assisted voting systems to compromise that could change the outcome of an election."[i]

More recent policy documents that detail Government Facilities CIP (critical infrastructure protection) and that discuss State and Local Government inclusion as part of CIP have unfortunately taken a crabbed approach that is inconsistent with the overall definition and purpose of CIP. The NIPP and DHS webpage continue to restrict the scope of Federal (i.e., national concern and protection) simply to subnational government cyber infrastructure that is necessary to the functioning of physical assets that are designated CIP. But fortunately PPD-21 (Feb. 12, 2013)[ii] directs the reconsideration and refocusing of the national effort to achieve critical infrastructure security and resilience.

The current conception of CIP has numerous deficiencies with regard to State, local, tribal and territorial (i.e., "subnational") governments. Its highly circumscribed CI scope fails to recognize and accord protection to the essential roles of State and local governments in maintenance of American civil society, for instance, in conducting elections for every level of government. The Federal institutions of government, namely Congress and the Presidency, cannot be legally constituted if the election system is not functional. The legitimacy of our governments at all levels is dependent upon election technologies and staffing that must achieve verifiably accurate elections. Stealth cyber attacks (of the sort that have notoriously harmed major corporations and Federal governmental entities) and software assurance deficiencies (that DHS has documented and sought to remedy), including the insider problem, are among the many cyber threats and vulnerabilities potentially damaging our highly electronic election systems.

Our elections are conducted in a decentralized way, at the local (county, parish or township) level. Voting systems, as noted by CRS above, have not been slotted into existing categories of critical infrastructure. Nonetheless, secure elections are essential for national security, and safeguarding electoral systems and practices from remote attack is certainly as important as safeguarding the other categories of our critical infrastructure. While there may be mitigations or means for recovering from challenges to other aspects of our infrastructure, however grave, it should be noted that there are no constitutional provisions for postponing or re-running an election. Thus while election systems have not previously been included in the CI scope, it should be considered in scope and at minimum should be incorporated in the discussions of the development of a framework that deals with cyber security.

I-B. Voting over the Internet

A grave challenge to secure elections has arisen since the publication of the CRS Report mentioned above in I-A, as today in more than thirty states, remote voters are permitted and in some cases encouraged to transmit voted ballots over the public networks. These ballots are sent through various means: as attachments to email, as faxes, including online fax systems, as uploads to Internet portals, and even as transmissions through online ballot marking systems to a remote vendor's portal, where the ballots are rendered for printing or for electronic transmittal back to an election official. In some states, Internet voting systems provided by private vendors have been used to access, mark and cast voted ballots in live elections. While most of these systems currently are used for military and overseas voters, this past November several states allowed some form of electronic return of voted ballots for <u>all</u> absentee voters. These practices place ballots, voter privacy, in some cases election management systems, and certainly electoral outcomes at grave risk.

The challenges to security and privacy of the ballots arise because the digitized vote information transmitted over the public networks is vulnerable to modification in transit and cannot be ascertained as having arrived as the voter intended; that is, such ballots are not auditable nor recountable because they cannot be certain to contain an accurate representation of the voter's original intent. We vote by secret ballot; no means exists for either the voter or the election official to confirm that the ballot was not manipulated in transit. And although some systems may incorporate encryption methods, encryption does not protect against distributed denial of service (DDoS) attacks, spoofing, vote selling, coercion, design flaws and other problems.

Many huge corporations have had their web services taken down by DDoS attacks, and rarely has the attacker been caught. Such an attack on an internet election could result in disenfranchising large numbers of voters who are unable to vote before the deadline. The entire government infrastructure of Estonia was brought down for 2 weeks by a long attack originating in Russia. DDoS attacks have been successfully used against real elections. The Canadian NDP leadership elections conducted over the Internet were brought down twice by DDoS attacks in 2004 and again in 2012. In neither case were the perpetrators ever caught. The same thing happened to the alternative Presidential election in Hong Kong in 2012. In an attack on the Democratic primary conducted in Arizona in 2000, response was seriously slowed on the first day as a result of a DDoS attack.[iii]

There are serious technological challenges that must be addressed if federal elections are to be secure and verifiable. As a cyber security expert from the U.S. Department of Homeland Security (DHS)[iv], pre-eminent computer technology experts from academia, industry and government[v] and even the National Institute of Standards and Technology (NIST) have indicated that the Internet is not sufficiently mature at this time to be employed as a platform for something as important as voting.

II. SPECIFIC PRACTICES

In the RFI, NIST poses a series of questions about the adoption and deployment of a list of practices as they pertain to critical infrastructure components. These are the practices:

- *Separation of business from operational systems;*
- *Use of encryption and key management;*
- *Identification and authorization of users accessing systems;*
- *Asset identification and management;*
- *Monitoring and incident detection tools and capabilities;*
- *Incident handling policies and procedures;*
- *Mission/system resiliency practices;*
- *Security engineering practices;*
- *Privacy and civil liberties protection.*

We respond by discussing several of these practices as they pertain to cyber security and are currently deployed in elections. This is not meant to be a comprehensive set of responses, but this set, along with the foregoing commentary, is designed to clearly identify why elections infrastructure should be considered an important part of cyber security frameworks for national security. We anticipate continued discussion around these and other practices as the framework process moves forward.

II-A. "Mission/system resiliency practices; Security engineering practices"

Because local elections offices rarely have extensive financial resources and indeed, many have seen significant budget cuts over the past decade, most do not have the kind of security and information technology staffing, procedures or budget that corporate entities or larger government institutions may have. Often elections tasks are carried out as a part time job along with other county or local administration.

Given that large corporate entities, banks, government institutions and others have experienced security breaches and sometimes sustained significant losses despite being well-resourced, it is unlikely that an under-resourced elections office if targeted would be able to evade similar breaches or even detect them in a timely manner.

Election officials enabling the online return of voted ballots, online ballot marking systems or other related practices must either build a system in-house or rely on commercially available systems and components. Commercially available voting systems that enable online voting are typically proprietary, not under the control of elections administrators and not really even understood by them.

Consequently elections infrastructure, particularly for systems connected to the Internet, is often dependent on the mission/system resiliency practices of private vendors, particularly where systems lack properties of auditability (see III, below) and thus cannot be effectively checked for proper functioning and accurate outcomes. If such systems were subjected to testing against a set of agreed upon standards, it might be possible to determine if any vendor claims of security were reliable. However, unlike polling place voting equipment, systems enabling voting over the Internet carried out via email, e-fax or through portal systems or other means are not currently subject to any federal standards, testing or certification of any kind.

II-B. Use of encryption and key management

Encryption, while useful for one part of the process, does not protect voting processes from many of the kinds of attacks that could occur, with potentially dire consequences. In the breach of the experimental system fielded for a public test prior to a pilot in Washington DC in 2010, voted ballots were discarded and replaced with other encrypted ballots by security researchers acting as white-hat attackers. The researchers involved indicated that after carrying out a shell-injection attack they were able to:

- codify all the ballots that had already been cast to contain write-in votes for candidates they selected, and rig the system to replace future ballots in the same way; and
- install a back door that let them view any ballots that voters cast after their attack.[vi]

Developers of other experimental systems have acknowledged that while they can encrypt each voter's ballot, they cannot protect adequately against client side security problems, including viral attacks that could modify the contents even before it is encrypted.vii Further, since many states are now permitting votes to be transmitted via email, it is important to note that while technology exists to encrypt email, the same technology raises difficult authentication and key management issues. Authentication and storage are problems for long-term keys, needed for encrypted email. These problems include determining when keys are first generated and stored, getting copies of keys to all machines to which one might send or receive email from, adequately securing keys in all places where stored, and revoking keys that have been compromised. Because of some of these difficulties, encrypted email has not been widely deployed. Therefore, email return of voted ballots is potentially even more risky than web-based methods, because email has all the problems of a web-based solution, while lacking encrypted communication. Nonetheless, email is in broad use as a method of returning voted ballots over the Internet today.

II-C. *Identification and authorization of users accessing systems*

For election systems, "identification and authorization of users accessing systems" is relevant in several ways. On the elections office side, identification and authorization of users must include the elections staff. Where elections offices contract with private vendors for systems enabling online balloting, the system can be accessed by the vendor's staff or contractors, so there would need to be explicit controls for identification and authorization of users at the vendor level as well. The ability of the elections staff to remotely control or even be aware of vendor user access is limited at best.

On the voter's side, authentication is a challenge. For ballots returned by postal mail, we know how to authenticate voters via a wet-ink signature affixed to the outer physical envelope. But authentication that relies on a PIN and other front-end processes can be circumvented, with dangerous effect. For example, in the breach of the experimental system fielded for a public test prior to a pilot in Washington DC in 2010, letters containing voter information and PIN numbers were discovered by the researchers on the server. In a real election, a hacker could have used that information for malicious purposes.

II-D. Monitoring and incident detection tools and capabilities

Banks and e-commerce sites invest billions of dollars a year in monitoring systems for attacks, and refunding customers where thefts occur. In elections, it would not be possible to "refund customers" even where monitoring might reveal a breach. And it would not be possible for a jurisdiction to inform a voter that his or her ballot was intact and contained the original intent of the voter, because voting requires anonymity, in other words the voters' identity must be separate from the contents of their ballots. Further, an election official would likely be unable to detect if any manipulation of the ballot had occurred prior to reaching the elections server. Because private vendors' systems have not been subjected to any federal testing nor certification to any set of standards, their capabilities for monitoring and incident detection are unknown.

II-E. Privacy and civil liberties protection

In their summary of their breach of the public test of the Washington, DC experimental Internet voting system mentioned above in II-B, the researchers note that the back door they installed allowing them to view any ballots that voters cast after their attack was a modification that recorded the votes, in unencrypted form, together with the names of the voters who cast them, which violated ballot secrecy.

In vendor-provided online ballot marking systems which also contain vote-transmittal capabilities, the vote data, once selected by the voter during the online session (which also involved the voter authenticating his/her identity in some way) is transmitted to a remote server for rendering with a barcode, then back to the voter's computer for local printing or for transmittal directly to the elections office. At least one vendor has indicated that such data is not "retained" there, but because the system is not under the election officials control, they have no capability of checking to ensure that is the case, and the vendor likely would be unable to prove that they do not retain that data. It's also not possible to determine if the voter’s information has been intercepted and transmitted elsewhere.

States that allow the return of voted ballots via fax or e-mail attachments ask voters to also return a statement that indicates they acknowledge that the ballot they are transmitting is not secret. Other absentee voters not using online systems can safeguard the secrecy of their ballot by the use of the inner ballot envelope/outer authentication envelope process. But we now deprive remote voters using online systems of a right that is accorded to all other voters. Given that this is not an individual right but rather a “systemic requirement” the benefits of which accrue to all involved in US elections, offering individual voters a waiver of such a right is inappropriate. Without ballot secrecy, voters, especially those in hierarchical organizations such as the military, can be subjected to coercion. And having a subset of voters be treated differently than other voters is a dangerous practice in elections.

III. Other Core Practices for Inclusion in the Framework

In the RFI, NIST asks whether there are other core practices that should be included for consideration in the Framework. One such practice relevant to elections is audits. The vulnerability of vote data transmitted over the Internet results in election systems which lack a key property of auditability, sometimes described as using or producing a true record of voter intent which the voter had a chance to verify, and which is independent of the software used for transmitting, recording, and/or counting the votes. Those records can be audited to ascertain the correct outcome of the election. In a presentation of the NIST Auditability Working Group in 2011, auditability was defined as “the transparency of a voting system with regards to the ability to verify that it has operated correctly in an election, and to identify the cause if it has not.” Given that elections are not likely to be postponed nor subjected to a “do-over” the potential impact of a successful attack is significant. To have a evidence based elections,[viii] it must be possible to both identify and solve for breaches that affect the verity of the outcome. For this to be possible, audit capacity is a core requirement, and the conduct of robust audits an essential practice.

IV. Conclusion

We hope the foregoing discussion sheds some light on how some common practices relating to cyber security intersect with our elections technology and practice today, and why elections must be considered within some framework on cyber security and in any discussion of critical infrastructure. As indicated, the discussion is meant to be a starting point, not a comprehensive review of all the questions NIST posed in the RFI. We look forward to continuing this important conversation in the future.

Signed (*organizational affiliations listed for identification purposes only*):

David L. Dill
Professor, Computer Science and, by courtesy, Electrical Engineering, Stanford University; Founder, Verified Voting

Jeremy Epstein
Senior Computer Scientist, SRI International

Candice Hoke
Founding Director, Center for Election Integrity at Cleveland State University; Associate Professor of Law (Election, Regulatory and Employment Law)

David Jefferson
Lawrence Livermore National Laboratory; Board Vice-Chair, Verified Voting

Peter Neumann
Principal Scientist, SRI International Computer Science Lab, Moderator of the ACM Risks Forum

John Savage
An Wang Professor of Computer Science at Brown University

Barbara Simons
Member, Board of Advisors of the Election Assistance Commission; former President, Association for Computing Machinery (ACM); Board Chair, Verified Voting

Pamela Smith
President, Verified Voting Foundation

[i] http://www.fas.org/sgp/crs/natsec/RL32777.pdf

[ii] http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[iii] "Voting on the Web" by Kurt Hyde and Steve Bonta, in The New American, Oct. 9, 2000

[iv] http://www.npr.org/blogs/itsallpolitics/2012/03/29/149634764/online-voting-premature-warns-government-cybersecurity-expert

[v] https://www.verifiedvoting.org/projects/internet-voting-statement/

[vi] https://freedom-to-tinker.com/blog/jhalderm/hacking-dc-internet-voting-pilot/

[vii] B. Adida. Panelist remarks – Internet voting panel. EVT/WOTE'11, the Electronic Voting Tech. Workshop at the Workshop on Trustworthy Elections, Aug. 9, 2011. http://www.usenix.org/events/ evtwote11/stream/benaloh_panel/index.html

[viii] http://www.stat.berkeley.edu/~stark/Preprints/evidenceVote12.pdf