Open Source Election Technology Institute
530 Lytton Avenue
2nd Floor
Palo Alto, CA 94301 USA
+1 650.600.1450

OSET INSTITUTE

TRUST THE VOTE PROJECT

Friday, 24.March 2017

Hon. Richard Burr
Chairman
Hon. Mark Warner
Vice Chairman

SENATE SELECT COMMITTEE ON INTELLIGENCE
United States Senate
Room 211 Hart Senate Building
Constitution Avenue & 2nd Street, NE
Washington, DC 20510

RE: Submission of Public Comment Regarding Russian Intelligence Activities Directed Against the 2016 U.S. Elections

May it please Chairman Burr & Vice Chairman Warner—

My name is Gregory A. Miller, and I have been authorized by my Board of Directors to write on behalf of the Open Source Election Technology (OSET) Institute—a nonprofit election technology research institute located in Palo Alto, CA and Portland, OR with over a decade of experience at the intersection of election system design and information security.

Our Chief Technology Officer and I offer this contribution to the Senate Select Committee on Intelligence ("SSCI") for reference in its information gathering process regarding foreign interference with the U.S. Election in 2016 and possible engagement with the winning campaign. Our intent is to help inform the Committee members and the investigation insofar as it addresses or concerns election technology, and attempted or successful criminal intrusions of the 2016 election, in the context of this investigation.

This information is intended to be an educational resource for all Committee members, and if appropriate, we appreciate it being added to the record. We are here to assist in any way we can within this domain expertise of electoral infrastructure security.

Respectfully Submitted We Are,

Gregory A. Miller	**E. John Sebes**
Co-Founder, Chief Operating Officer	Co-Founder, Chief Technology Officer

Before the
SENATE SELECT COMMITTEE ON INTELLIGENCE

In the Matter of	)	OPEN HEARING
	)	
A PRIMER IN RUSSIAN	)	Thursday, March 30th, 2017
	)	
ACTIVE MEASURES AND	)	10:00 am EDT
	)	
INFLUENCE CAMPAIGNS	)	Room 106, Dirksen Building

PUBLIC COMMENT SUBMISSION

THE OSET INSTITUTE'S STATEMENT REGARDING USE OF ELECTION INFRASTUCTURE TERMINOLOGY IN DISCUSSIONS REGARDING 2016 ELECTION VULNERABILITIES

Introduction

May it please the Chair and Ranking Member, my name is Gregory A. Miller, and I have been authorized by my Board of Directors to write on behalf of the Open Source Election Technology (OSET) Institute—a nonprofit election technology research institute located in the Silicon Valley with over a decade of experience at the intersection of election system design and information security. Our Chief Technology Officer and I offer this contribution to the SSSCI's information gathering process in hopes of helping inform the Committee members and the investigation insofar as it addresses or concerns election technology and the 2016 Election.

Given recent testimony and discussion in a House Permanent Select Committee on Intelligence Hearing on the same subject, we witnessed unintentional conflation of terms and descriptions of electoral infrastructure in the U.S. The OSET Institute offers the following statement intended to help clarify the various components of electoral infrastructure and related vulnerability points. We believe it is important that descriptions of vulnerabilities, compromises (*"hacking" or attempts thereof*) be clearly understood by all and void of unintended distorted definitions used for convenience or simplicity of discussion or explanation.

Terms

We begin by offering some terms and high-level description and explanation of the various components comprising America's electoral infrastructure.

Election infrastructure (EI) consists of all the assets that are necessary to successfully operate an election. EI is comprised of systems to manage three (3) distinct but inter-related types of data:

1. Voter data
2. Ballot data
3. Election data

Thus, an EI is comprised of systems to create and manage [**1**] voter data (*voter registrations systems*); [**2**] ballot data (*systems for creating, casting, and counting ballots*); and [**3**] elections data (*election management systems or "EMS"*). EI is generally configured with the EMS related to each of the voter registration and ballot casting and counting systems.

Disruption of EI at any point can lead to a disrupted (*or worse, failed*) election – one which lacks conceding losers, consensus winners, and legitimacy for transfer of power – which by itself could be a failure of a "national essential function" (*for infrastructure discussion purposes*) but also with consequent effects on national security and public safety.

EI also shares a characteristic with another important critical infrastructure sector: *financial services*. In both sectors, part of the critical mission is maintaining **public confidence** in the correct operation of the assets. If there is significant loss of public confidence—regardless of actual malfunction or the degree to which malfunction effects outcomes—the mission may be in danger. For both kinds of transactions—votes and payments – the underlying CI must be able to sustain public confidence that the transactions are performed accurately and legitimately. Unlike power distribution or traffic safety, adequate fraud prevention and detection is a key part of the mission, and even further, these protections must be **demonstrably** adequate. The public requires a basis for the belief that the protections are performed diligently, not the mere assertion by responsible parties that protection is in place.

Voter Registration System (VR) consists of all the assets required to register, maintain the registration of, and provides election information services to a specific class of citizen called a "voter." This includes a significant amount of infrastructure within government in the so-called "back office" to operate and maintain voter records in voter databases. One of the emerging ways of helping serve voters and administer "change management" is online voter registration and online voter services portal. These "front end" services, expressed in the form of web sites and mobile Apps, enable citizen-voters to manage their own voter record by requesting and submitting data about their registration and status. Another important form of voter record is the record of each voter checking in to vote in person, via a paper or digital poll book. Those records are required to prevent or detect double voting, and are essential to vote-by-mail (VBM) processes, ensuring that a VBM ballot is not counted if the voter had voted in person. Thus, voter registration systems create, curate, and protect *voter data*.

Voting System (VS) consists of all the assets required to conduct the casting and counting of ballots. These are combinations of hardware and software typically deployed in polling places in election jurisdictions. Deployments seldom, if ever, include any online or remote access capability. These are standalone systems (*typically integrated devices*) for the marking of a ballot and subsequent delivery into a counting mechanism. In some cases, voting systems are integrated such that marking a ballot is a digital exercise using some sort of a screen display and selection method (*e.g., touchscreen*), which immediately "casts" or adds selection choices into a "tally." With the exclusion of a special type of voting system comprised of digital means to distribute a blank ballot and digitally return a marked ballot, which is primarily restricted to controlled applications for overseas and military voting situations, voting systems are *never* remotely accessible by way of some internetworking means (*i.e., either a private digital network, or use of the public Internet*).

Election Management System (EMS) consists of computers running a specific type of software designed to administer all aspects of an election. The EMS includes the processing functions and tools that define, develop, and maintain election databases; perform election definitions and setup functions; format ballots; perform ballot tabulation; consolidate and drive results reporting; and (*should*) maintain audit trails. EMS Apps maintain information about a jurisdiction's precincts, the election contests and candidates, and the issues being decided. They also drive Apps to design and generate ballots, program vote casting and ballot counting equipment. Finally, aside from preparation tasks, the core function that makes an EMS most critical is its role as a "Tabulation Manager" where it combines tally data from voting machines to produce the election results data. This results data is later processed in a variety of reporting functions. Importantly, the EMS also interacts with both Voter registration systems and Voting Systems. In essence, the EMS is the "hub" of an election administration system. In fact, the EMS should be considered a *highly sensitive core* of electoral infrastructure and should be subject to the most strenuous security and integrity assurance protocols.

Election Administration System (EAS) is a descriptor for the combination of the VR, EMS, and additional elements including, but not limited to:

- Ballot design, layout, and generation tools;
- Poll books; and
- Election results reporting systems.

Networking and **Air-gapping** as these terms apply in the context of election administration and voting systems should be clearly understood for what they are, and more importantly, what they are not.

Computer Networks are generally not used, and in some cases legally prohibited in the context of voting, although they can play a role in election administration. Networking or the interconnecting of machinery can be handled by hard-wire (*copper cabling similar to phone lines*) or radio (*WiFi or other protocol*). When considering aspects of the electoral infrastructure, one needs to consider whether and to what extent machinery are connected to a network, and whether that network is accessible to and from the public network known as the Internet. More on this is discussed below.

Air gapping is a term of art that refers to the physical sequestration of a computer (*or network of computers*) or device from other computers or devices (*making them "stand alone"*) by requiring a removable media to transfer data (*or programs, applications, or other computer instructions*) to and from a stand-alone machine (*or separate network*). Precisely then, "air gapping" is a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network.

The name arises from the technique of creating a network that is physically separated (*with a conceptual air gap*) from all other networks. An important nuance about air gapping is that the air gap may not be completely literal. Computer networks can employ the use of dedicated cryptographic devices that can "tunnel" "data packets" in a special manner over untrusted networks which can be considered *air gapped*, as there is no ability for computers on opposite sides of this *virtual gap* to communicate. This distinction has significance when using the term, as explained below.

Application of Terms

The motivation for our offering this tutorial is having witnessed, in the context of discussing voting and election administration systems during the open hearing, the largely unintentional mischaracterization of which systems were compromised or hacked and which were not. Accordingly, we offer some discussion of the application of these terms above in cataloging the incident types below, also reported in the **ICA**

Assessment, "*Assessing Russian Activities and Intentions in Recent US Elections*," ICA 2017-01D, 06 January 2017.

2016 Election Cycle Compromise(s) and/or Threats Thereof

1. Much has been covered and discussed about whether and to what extent the 2016 election was "hacked." It is imperative to be clear and concise when discussing this matter, carefully distinguishing what aspects of electoral infrastructure are being considered.
2. **Digital Crime Against Campaigns**. Reference is often is made to the "hacking" or digital break-in of the Democratic National Committee's data and/or eMail servers (*the so-called DNC hack*), with similar reference to a related organization, the DCCC. It is understood in the technical security professional community that servers and digital assets of the RNC also experienced tampering and probable theft. However, it should be continually clarified that these criminal incidents ***did not*** amount to "*hacking the election*." These incidents amount only to disruption or hacking of the *election cycle*, *electioneering*, and/or *campaigning*, ***but not*** anything to do with the actual election.
3. **Digital Crime Against Voter Registration Systems (Election Administration)**. There were several states' voter registration systems that were poked, prodded, and in two cases penetrated—one resulting in possible data theft. These criminal incidents ***did not*** amount to hacking "**voting systems**" but ***did*** amount to hacking attempts against *election administration systems*.
4. **Digital Crime Against Election Management Systems (Election Administration)**. There were no detected or reported criminal incidents or hacks to election administration systems (*i.e., the EMS systems and related Apps and services*) used across the United States this past election in November 2016. It is also true that by the time of the actual election no EMS was connected to or accessible by the public Internet. However, it is unclear if any EMS machines across the country were ever Internet accessible; some may well have been for reasons explained below. By and large these systems remain "*air-gapped*."
5. **Digital Crime Against Voting Systems**. There were *no* detected or reported criminal incidents or hacks to the *voting systems* (*i.e., ballot casting and counting equipment*) used across the United States for this past election in November 2016. It is also true that none of that equipment (*save a system deployed in Alaska*) was accessible from, or connected (*directly or indirectly*) to the public Internet. This machinery was effectively "air gapped" from other constituents of electoral

infrastructure including EMS and VR systems (*as these terms are defined, supra*). We can be confident that no cast ballot data or local precinct-tallies were affected or compromised.

Terminology Insights

Below we offer some comments and insights into the use of these terms and the recommended characterization of digital crime in the 2016 election.

1. For the most technically credible general characterization of attempted or actual digital criminal activity waged against the 2016 national election **we recommend the following statement**:

    > "The 2016 election was marred by concerted foreign state sanctioned activities to compromise both the campaigns and the actual election itself. The campaigns were compromised by digital break-ins and theft of content for at least the DNC. It is likely RNC resources may have been compromised, although there has been no reported removal of content. The election administration infrastructure itself had attempts against voter registration systems, with possible attempts against other assets of election management systems, although it is difficult if not impossible at this point to ascertain if there was any success in such digital penetration. However, there were no reports or findings of any attacks or compromise to any of the ballot casting and counting devices in the field."

2. In general, in 2016, here were the particulars of (Russian) meddling:

    a. The election was *not* compromised by hacking efforts waged against aspects of election administration assets including, but possibly not limited to, voter registration systems.

    b. There was no "hack" of the vote itself (*to the very best of our knowledge.*)

    c. However, the campaigns, namely for the Democrats, were compromised including a digital break-in of the DNC digital servers. The campaign hacks amounted to meddling in the election *cycle*, but *not* the election itself.

3. Although ballot casting and counting devices are, in general, *never* connected to the public Internet (*with the exception of an Internet-based ballot casting process allowed in Alaska for all voters, and several states providing for a digital balloting process for overseas and military voters*), it is possible (*but highly discouraged*), to have PCs that contain election management system (EMS) applications connected to the Internet due to the limited capabilities of local registrar offices to properly isolate a dedicated computer for purposes of election administration (*a budget and resource limitation discussed below*).

4. These so-called "back-office" election administration computers should <u>*never*</u> be connected to the Internet, but rather air-gapped from the public Internet, just as the ballot casting and counting equipment (*typically stored in warehouses*) are also "air-gapped." However, it is imperative to remember that an air-gapped machine does <u>*not*</u> mean it is guaranteed to be in a safe quarantine void of possible compromise. **Here is why**: an air-gapped computer means that there is no network connection to that machine. As such, it is not possible to introduce any content (*of any kind*) into that computer or to extract any content from that computer using a network (*whether physical copper cable or wireless radio networks such as WiFi.*) However, that air-gapped computer still needs a means of loading and unloading content. "Removable media" (*think: a CD disc or USB "thumb drive" or "data stick"*) must be used to introduce or extract content from an air-gapped device. And therein lies a potential vulnerability. Unless the introduction of any digital content by means of removable media can be safeguarded against the possible introduction of unauthorized content, then the "air-gapped" computer is no safer than one accessible through a computer network. It is imperative to never assume that just because a stand-alone device (*or collection of devices in a self-contained network*) is air-gapped from an external (*let alone public*) network means it is more secure than those connected to a network. Certainly, being disconnected reduces the likelihood of unauthorized access, but doesn't eliminate the malfeasant opportunity.

5. Why would a back-office EMS computer ever be connected to the Internet? In many counties and election jurisdictions across the country, registrar offices are small, budget-strapped, and serve multiple purposes. A dedicated computer for election administration is an absolute luxury in these offices, let alone having the additional space of a controlled-access isolated secure room for these machines to reside. Accordingly, the OSET Institute has found in its work over the past decade that it is possible PCs used for election administration and the EMS App may <u>*also*</u> be used for eMail, web browsing and connecting to other data services. And as a result it is possible for such a machine with its multipurpose use, will be connected from time to time (*or continuously*) to the public Internet. This is not a good thing for the integrity and protection of the EMS App that also resides on that machine, but it can be a reality. Therefore, it must be remembered that there are no guarantees that a back-office election administration system somewhere in the country doesn't have Internet accessible machinery.

6. EMS machinery compromises did not need to happen during the actual election, and probably would not. Actually, such compromises of this element of election administration systems would've happened months prior to the election and likely even before the Primaries—in other words early Spring of 2016 or earlier. And this might have amounted to introducing malware or other infections to compromise those EMS devices, in particular, including those PCs that might have been (*even temporarily*) connected to the Internet. Those machines that were air-gapped would've been marginally more secure, assuming the processes and protocols for physical access and use of digital media were in place to ensure the integrity of the device.

7. It is actually inaccurate to suggest that an election cannot be compromised or derailed because of its antique dispersed, and disconnected voting machines. That assumes an analogy of transportation: "*I can move from point A to point B by bike, car, train or plane.*" But that is not the proper analogy. The analogy for voting machinery (*specifically ballot casting and counting machinery*) is: "*I can get from point A to point B in anyone of five different automobiles.*" The key here is that in the first analogy, the transportation vehicles are vastly different—a bicycle and a train are completely different vehicles. The latter analogy is far more accurate: I have a choice of five different automobiles, but they all have several characteristics in common. And in fact, if I know how to operate automobile "A" then there is a significant likelihood I know how to operate automobile "B." That is the situation with our current voting systems deployed across all 10,079 jurisdictions in 3,300 counties nationwide. There is a finite set of machinery types; they all have a common "architecture" or base platform: 1990's era PC technology. If an intruder knows how to break into one machine, it is likely very easy to compromise any other. As a result, it is technically incorrect to assert that the very arcane disconnected nature of our dispersed balkanized (*by design*) infrastructure of voting machinery contributes to its security. That's incorrect, because all machinery shares a common architecture or basic design.

8. Finally, it is equally important for an intellectually honest conversation about the integrity of our elections and the current electoral infrastructure to understand that to compromise, derail, or destroy a national election does *not* require a massive attack on the infrastructure to succeed. In fact, the only attack surface required is a "swing state" with a highly contentious county, electoral district, or precinct. All that is required to send a national election into question or chaos is a highly targeted attack on that portion of the overall vote for a state's Electoral College votes. Therefore, such an election derailment only requires a jurisdiction with, for instance, a lack of any paper audit trail

and/or election administration systems that can be compromised by Internet-borne attacks or physical attacks by surreptitious introduction of an attack agent by way of removable media. So, the assumed integrity by virtue of antiquated, dispersed, disconnected voting machines is cold comfort at best.

We thank the Chair, Ranking Member, and the rest of the SSCI Committee for considering our contribution of some explanation of terms and their use as they may apply in your investigation and research on the matters of this Hearing and related on-going activities.

We believe that our electoral infrastructure is a matter of national security. We believe that any attempt to compromise that infrastructure, or the administration of elections, or any of the processes of free and fair elections as a part of the operational continuity of our democracy, is a violation of our nation's sovereignty and should be redressed accordingly.

Going forward, we further believe this electoral infrastructure must be updated and upgraded to afford it the verifiability, accuracy, security and transparency essential to free and fair elections where ballots are counted as cast, and confidence is high in elections and their outcomes. We understand that is subject matter outside the scope of your work, although we believe it should be a background mandate and consideration here and for all of Congress.

We thank you for your dedicated patriotic bipartisan service.

Respectfully Submitted,

Gregory A. Miller	E. John Sebes
Co-Founder & Chief Operating Officer	Co-Founder & Chief Technology Officer
OSET Institute, Inc.	**OSET Institute**, Inc.
Palo Alto, CA	Palo Alto, CA