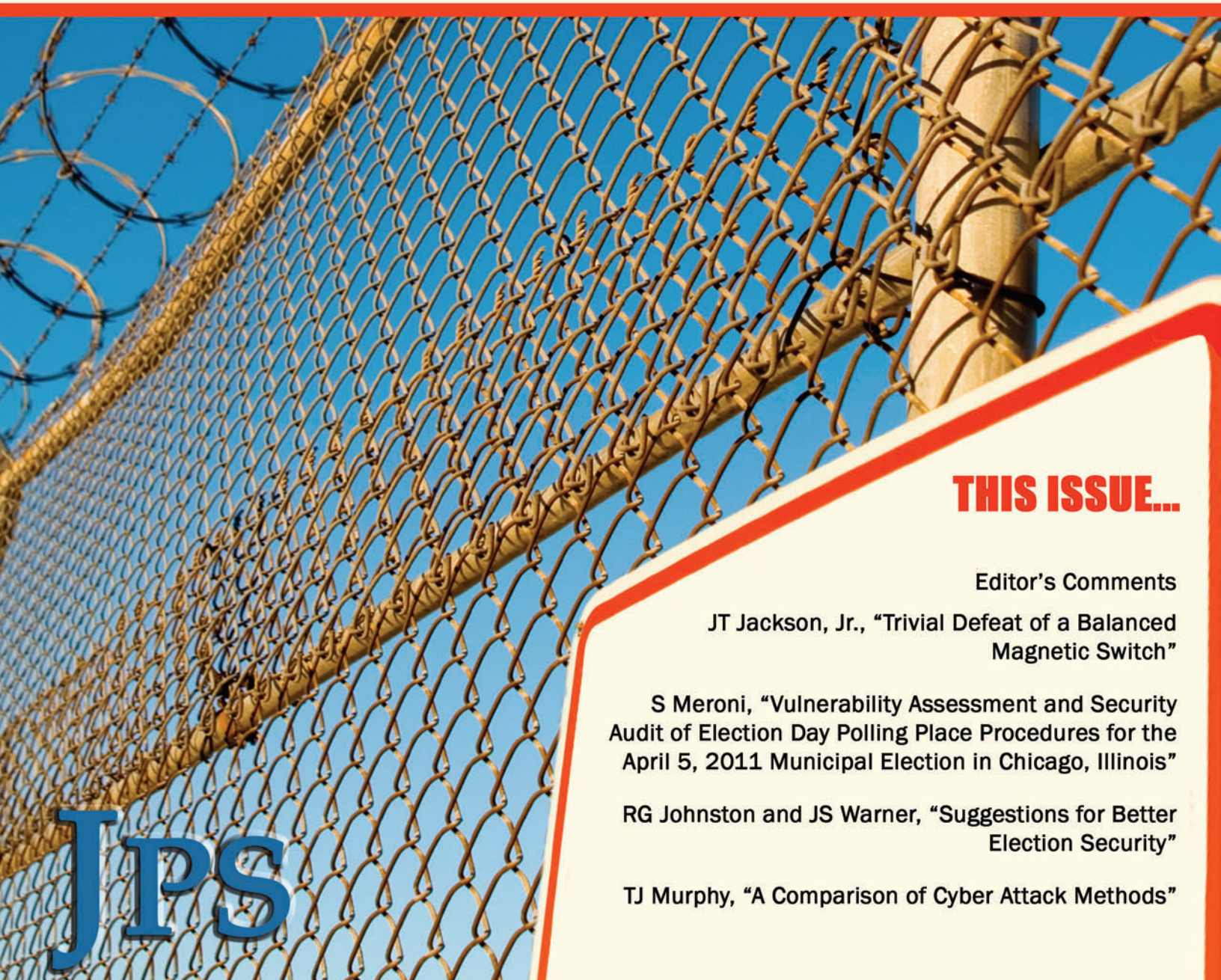
Argonne NATIONAL LABORATORY

The Journal of Physical Security

Volume 5(1), 2011



JPS

THIS ISSUE...

Table of Contents

Journal of Physical Security, **Volume 5(1), 2011**
ISSN 2157-8443
Web: http://jps.anl.gov

Editor's Comments

Welcome to the 5th Volume of the Journal of Physical Security (JPS). This issue contains articles about vulnerabilities in balanced magnetic door switches, elections, and computers.

The paper by Sharon Meroni discusses an analysis of election security in Illinois. The findings are disturbing and relevant to elections elsewhere in the country. Election integrity is a homeland security issue, and we had better start taking it seriously. Suggestions for better election security are offered both in her paper, and in the viewpoint paper that follows. Speaking of election security, we in the Vulnerability Assessment Team at Argonne National Laboratory recently demonstrated another man-in-the-middle physical attack on a different electronic voting machine. See http://www.ne.anl.gov/capabilities/vat/election-security.

We don't usually publish papers in JPS about cyber security, but the final paper by undergraduate student Tyler Murphy does a nice job of emphasizing the importance of physical security in cyber security, and also points out the risks of social engineering.

As usual, the views expressed by the editor and authors in *the Journal of Physical Security* are their own and should not necessarily be ascribed to Argonne National Laboratory, the United States Department of Energy, or the authors' home institutions.

****

Research at Harvard, Duke , and the University of Toronto indicates that people are more honest in filling out forms if they are asked to sign an honesty pledge or acknowledge an ethics policy or responsibility at the top of the form, rather than the more traditional bottom of the form. See K Weisul, "One Blindingly Simple Way to Improve Honesty", http://www.bnet.com/blog/business-research/one-blindingly-simple-way-to-improve-honesty/1641 and N Mazar, et al., The Dishonesty of Honest People: A Theory of Self-Concept Maintenance", http://duke.edu/~dandan/Papers/dishonestyOfHonest.pdf.

People seem to need to be reminded up front of the importance of being honest. There are significant implications for security involving such things as loss prevention, security incident reports, background checks, and security clearances.

****

Charles Kurzman has written an interesting book entitled, *The Missing Martyrs: Why There Are So Few Muslim Terrorists* (Oxford University Press, 2011). Kurzman points out that approximately 150,000 people have been murdered in the United States since 9/11. Islamic terrorism has taken fewer than 3 dozen lives on U.S. soil in the same time period. Fewer than 200 Muslim Americans have been caught planning or engaging in terrorist acts, out of a U.S. population of 2.5 million

****

Jon Ronson's new book, *The Psychopath Test: A Journey Through the Madness Industry*, claims that Chief Executive Officers (CEOs) of large corporations are 4 times more likely to be psychopaths than the general public, about 1% of whom are psychopaths. It's not clear what percentage of managers below the CEO level are psychopaths, but I'm betting on a much higher number. The percentage of sociopaths is presumably even larger.

A new research study. "The Destructive Nature of Power without Status", to be published in the *Journal of Experimental Social Psychology* finds that supervisors and managers with power but low organizational status or respect may be the most likely to be bully or demean their subordinates. There are important implications for mitigating the insider threat and for security managers and supervisors. More on this study can be found at http://www.cnn.com/2011/09/24/us/california-power-status-study/index.html?hpt=hp_t2.

****

Some interesting quotes about homeland security...

[The TSA is] moving towards risk-based security.
-- Jim Fotenos, TSA spokesman
Comment: It's been a decade since 9/11 and we're only **moving towards** risk-based security!?!

Taking my tweezers away is not going to win the war on terrorism.
-- Airline passenger Ross Ratcliff

So far, DHS seems pretty efficient at detecting losers and wackos, then entrapping them into some kind of inane terrorist plot. It would probably be better if they concentrated on serious threats.
-- Anonymous

After 9/11 it was literally like my mother running out the door with the charge card. What we really needed to be doing is saying, 'Let's identify the threat, identify the capability and capacity you already have, and say, OK, what's the shortfall now, and how do we meet it?'
-- Al Berndt, Nebraska Emergency Management Agency

So if your chance of being killed by a terrorist in the United States is 1 in 3.5 million, the question is, how much do you want to spend to get that down to 1 in 4.5 million?
-- John Mueller

****

The Center for Investigative Reporting has a web site that lists many questionable homeland security expenditures and initiatives: http://centerforinvestigativereporting.org. Some examples:

1. The Secure Border Initiative was a Boeing Co. contract to set up a network of surveillance cameras, radar, and other security measures along a 2,000-mile length of the U.S.-Mexico border. Originally intended to be up and running by 2009, the project missed deadlines, had serious performance problems, and resulted in severe cost overruns. The project ended up costing $1 billion before it was mercifully canceled.

2. $557,400 of rescue and communications gear was provided by Department of Homeland Security (DHS) funds to protect 1,500 residents of North Pole, Alaska.

3. In Idaho, the state's smallest county, Clark, population 910, received nearly $600,000 in anti-terrorism grants during the years immediately following 9/11. Clark County officials spent more than $20,000 on body bags. Another $10,000 paid for "explosive device mitigation and remediation equipment".

4. Cherry County, Nebraska (population 6,148) got thousands of DHS dollars to buy cattle nose leads, halters, and electric prods to deal with potential bioterrorism attacks on cows.

5. West Virginia purchased $3,000 of lapel pins with DHS funds.

6. The city of Denver used DHS grants to buy refrigerator magnets, baseball caps, pens, and other swag totaling over $35,000 for its "Ready Colorado" campaign, even though federal guidelines didn't allow such promotional items to be purchased with federal money.

7. Denver also forgot about a $1 million check from DHS and failed to cash it.

8. A 30-foot trailer worth $54K purchased with DHS grants by Hinsdale County, CO was apparently not used 4 years after it was purchased. New mobile radios were held in storage for nearly a year.

9. A high school in Tennessee spent $30,000 of DHS funds for a defibrillator to keep on site during a district basketball tournament.

10. Missouri spent several million dollars of DHS funds to buy 13,000 chem-bio warfare suits at $400 each. This was enough personal protection "for each and every full-time law enforcement officer in the state, regardless of the type of community in which he or she works."

11. New York spent $3 million on a custom automated public health record system to help identify bioterrorism threats. A 2008 investigation, however, learned that the employees who

used the system were completely unaware of its potential for bioterrorism detection.

12. In California, a so-called "fusion center" used by police to collect threat information bought 55 big-screen digital TVs to be used for training employees. But the training system was never purchased, and when auditors showed up, all of the televisions were tuned to a single television station.

****

Security often involves complex tradeoffs. This reality does not, in my view, excuse the reprehensible conduct of Bay Area Rapid Transit (BART) in blocking cellphone reception in San Francisco stations on August 11 for 3 hours due to threatened protests. (See *The Oakland Tribune*, August 12, 2011 or http://www.homelandsecuritynewswire.com/groups-seek-fcc-ruling-bart-s-cell-phone-shutdown.) The idea was that the loss of cellphone communication would make it more difficult for potential protesters to coordinate their efforts.

In undertaking this electronic censorship (also reportedly being contemplated by the United Kingdom to deal with flash mobs), BART firmly placed itself in the company of Hosni Mubarak, Bashar al-Assad, Mahmoud Ahmadinejad, Vladimir Putin, Wen Jiabao, Thein Sein, and other dictators, thugs, and oppressors. Interfering with the basic right of free expression—before anybody broke any laws no less!—is a violation of basic human rights. (There were also serious safety implications for BART passengers being unable to use their cell phones.)

The reality of liberty and freedom is that they are not consistent with absolute safety. They're dangerous. They are also more important than public safety. If we have to adapt unenlightened, illegal, or morally reprehensible tactics that compromise our basic principles in the name of security, we're no longer the good guys. As Ben Franklin said, "They who would give up an essential liberty for temporary security, deserve neither liberty or security".

-- Roger Johnston, Argonne National Laboratory, September 2011

Trivial Defeat of a Balanced Magnetic Switch

John T. Jackson, Jr., MS
Jackson Research
www.jrmagnetics.com

Abstract

Balanced Magnetic Switch vulnerabilities render it defeatable by trivial means. A detailed description of the most common BMS and procedures germane to its defeat including a method of how to design defeat tools and apparatus for analysis of any common BMS based upon glass reed technology are provided.

Introduction

The patent for the first Balanced Magnetic Switch or BMS, otherwise known as the Triple Bias Switch, was issued to Holce [2] in 1980 as a "High Security" device intended for use in physical electronic high security systems designed to protect high value targets. It was supposed to replace other magnetic sensor devices with known vulnerabilities. The intent was that it should be invulnerable to any kind of defeat or tampering so that even if its presence was known, there was no effective way around it. During its development, it probably could have met that criteria. However, by the time the patent issued, it was already obsolete and quite vulnerable to defeat by trivial means as was its predecessor. To see how this developed, we need to examine historical aspects that affected the technology and its perception. Then, we will take a detailed look at how it works and why it is so easily defeated. A laboratory set up will be described whereby anyone can tailor a defeat tool targeting any manifestation of the BMS switch based upon glass reed technology or any technology operating on a similar principle.

History

The first patent for a glass reed switch was filed by Elwood in 1940 [1]. The basic Form A device consists of two magnetic wires in close proximity separated by a small gap as shown in Figure 1. It is a Normally Open Single Pole Single Throw switch. The switch is closed when in proximity to a magnetic field, generally provided by a permanent magnetic in security sensor arrangements. The two blades attract each other under the influence of a magnetic field. The bare Form A device is actuated in the presence of a sufficiently strong magnetic field making a closed circuit. Although the actuating field zones tend to be lobed, the device is basically omnidirectional

The original magnetic sensor used on doors and windows for physical electronic security systems was a simple glass reed in combination with a single ferrite or Alnico permanent magnet. A typical application embeds the glass reed switch in a plastic shell of which two common embodiments of this approach are shown in Figure 2 and Figure 3. The moving part is always a permanent magnet. The switch side is connected to the security system by two conductors. Obviously, shorting out the two conductors makes the switch appear secure whether or not the switch is open or closed.

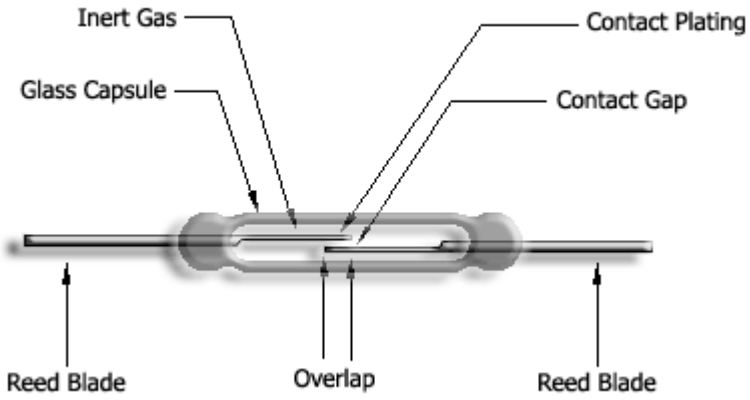


Figure 1: Form A Glass Reed Switch Architecture

This combination is still used in "Home Electronic Security Systems" today. Since it is frequently inconvenient to access the lead wires, it is quite common to find electronic security systems using this type of sensor breached by taping a permanent magnet onto or near the sensor switch allowing opening of the door or window, to which the sensor magnet is fixed, without detection. It is called the "Refrigerator Magnet Defeat" technique. These "singles" or "bullets", Figure 2, as they are sometimes called, are only an inconvenience to a professional. The surface mounted version is shown in Figure 3. These endemic devices obviously have no place in any "High Security" installation.

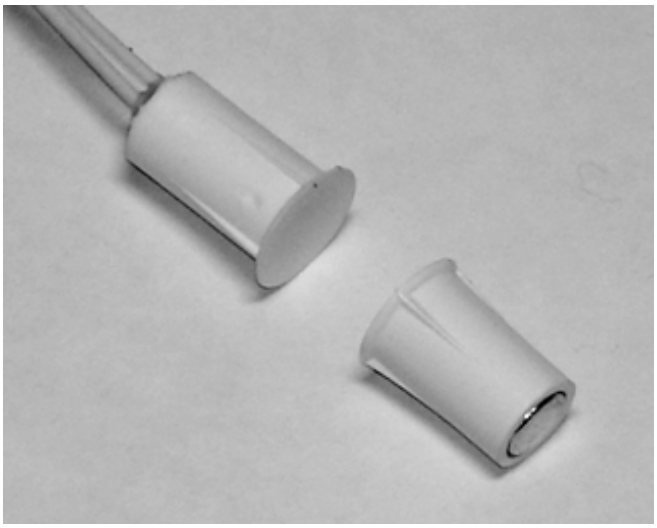


Figure 2: Typical single glass reed and permanent magnet security sensor or bullet.

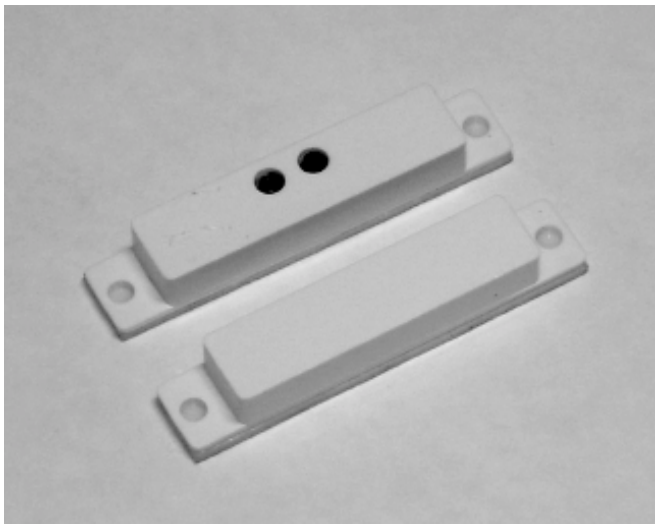


Figure 3: Common surface mount security sensor typically seen on doors and windows.

The BMS was invented by Holce to address this vulnerability. It should not be surprising that it was defeatable by a similar trivial technique by the time the patent issued. New advancements in the field of permanent magnet materials became the nemesis of the Holce BMS. The two most common permanent magnets, prior to rare-earth magnets, were Alnico

and ceramic ferrites. Ferrite magnets were quite popular because their cost was dramatically less than Alnico, being a cobalt alloy. These two materials were obvious choices for the BMS invented by Holce. It is unclear if Holce knew anything about the new rare-earth permanent magnets. He never mentioned them in any of his work. The first rare-earth permanent magnets became public during the same time period as Holce development work. In those days, rare-earth permanent magnets were Samarium Cobalt alloys. They had been developed at Wright-Patterson Air Force Base, declassified and released to the aerospace industry during the 70s just prior to the Holce patent issue date, 1980. Obviously, they were too expensive to be considered for general commercial applications. However, sacrificing security as a compromise against cost violates the fundamental concept of the BMS. Holce made the right choice for a commercial item, but the BMS has never been one. And, it is the rare-earth magnets that made his invention obsolete by the time the patent issued. We will see why later.

To complicate matters further, magnetic apparatus design was usually limited to slide rules and hand calculations. Calculators were a new item. Computers were usually limited to the aerospace industry and not available to the general public. Computer aided design was in its infancy. There was no finite element magnetics software. Obviously, numerous variations made in a prototype shop were cost prohibitive. Detailed numerical analysis by hand was time prohibitive. Consequently, there was considerable trial and error without a clear understanding of how those devices behaved from any analytical point of view. Even with the issued US patent, the actual manufacture of the original Holce device was shrouded in secrecy, requiring a complex bias magnet adjustment during the manufacturing process.

Shrouded in mystery and fighting an up hill battle all the way, Holce finally convinced the US government to use his invention. All of the original US government specifications [5] were written around the Holce device from a purely operational point of view and remain essentially unchanged. Some Lockheed security documents make reference to original device specifications. The present day device is literally identical to its very first manifestation with changes only in its packaging. Over time, the BMS High Security Switches became known as the "First Line of Defense" in modern electronic security systems.

How it worked was obvious the moment I saw it which led to the first alternative [3] that was unique while actually meeting all of the Federal device specific specifications [5]. It became the vehicle for my research into the next generation of BMS technology. The next technology became the basis for my Master's Thesis [6] at the University of Nevada, Reno and another patent [4] The new technology creates a BMS without any reliance upon glass reed technology. My thesis exposed some of the existing BMS vulnerabilities in graphic detail and hinted at a special defeat tool referred to as “defeat keys” and referenced the invulnerability of my new technologies to it.

Once my first BMS patent [3] issued and the Holce patent ran out, several other companies introduced clones. There are several on the market. They are all based upon the same underlying principle; triple biased glass reeds. They are all vulnerable to the defeat keys I have been selling as “Defeat Sticks”.

The Specifications

All Federal and UL specifications call out a small zone adjacent to the face of the fixed switch which is a dead zone. The switch is actuated/safe/secure when the actuator magnet assembly is between roughly 0.60 inches down to roughly 0.20 inches from the switch face. Closer than 0.20 inches sets off the alarm. This dead zone is its guaranteed vulnerability. It was detrimental, but sold as a feature by marketing people and written into all of the Federal specification documents as well as the latest UL 634 specification.

All High Security Balanced Magnetic Switches, BMS, based upon "Glass Reed" technology, regardless of architecture, can be easily defeated by trivial means. In fact, most BMS that can be characterized by 2-D magnetic field analysis, as opposed to "inherently 3-D" magnetic field analysis, can be defeated by a variety of trivial means. This is partly due to the fact that most existing BMS devices are either clones of the original Holce BMS device or a derivative of the under lying concept embodied in the original Holce patent [2]. The basic objective was to prevent defeat by a single magnet ignoring the fact that it was always defeatable by a copy of its own actuator magnet.

To make matters worse, the new UL 634 specification is both designed around the Holce device as well as designed to exclude it in a combination of contradictory requirements. The UL specification was lobbied by the electronic security industry's corporate executives with total disregard for anything technical. It represents fundamentally a war of specifications intended to include certain products while excluding others. One shining example is the requirement that all BMS must contain rare-earth magnets excluding all ferrites and Alnicos which obviously targets the Holce BMS. The UL 634 specification is intended to suggest that any BMS that meets its requirements is somehow undefeatable. This is simply not the case. It is a political document in its entirety imparting a false sense of security.

The UL 634 specification suggests a means to manufacture a "Defeat Stick". It suggests that any BMS that can pass this test is impervious to this form of attack. It is quite possible to design a BMS that passes these provisions and can still be defeated by a "Defeat Stick" not anticipated within the scope of the document. Here again, it produces a false sense of security. There are no known devices utilizing glass reed technology that are impervious to this form of attack. There is one manufacturer using a glass reed alternative and claims to be impervious to this form of attack. This is also not true.

One caveat is the inclusion of magnetic shielding by some manufacturers to protect against certain types of defeat attack. One such example is the use of a U shaped shield. It is neither novel nor effective. Since the Holce BMS is defeatable by its own actuator [6], magnetic shields were introduced to mitigate that possibility in competing designs. These magnetic sheet metal shields short out the actuator magnetic fields. When the magnetic field becomes sufficiently strong, the shield becomes saturated and no longer effective. Special devices similar to the Defeat Stick can be tailored to penetrate these shields, which is a brute force attack. Reference 6 goes into much greater depth.

The Technology

The basic principle of the BMS is to use three alternating polarity actuator magnets in combination with three polarity sensitive glass reed switches making the entire assembly resistant to defeat by a single magnet. This requires biasing the glass reed switches so that they are each actuated by low level local magnetic fields. The bias magnet in combination with the glass reed achieves polarity sensitivity to some extent. Form A switches cannot be used here since the biased glass reed switch in combination with the actuator magnet in a secure position would be an open circuit. A closed circuit with the actuator magnet in a secure position requires a Magnetically Biased Form C Double Pole Single Throw switch as shown in Figure 4. When the actuating magnets, whose polarities are in opposition to their corresponding biased glass reed switches, are in the secure position, the magnetic fields around the glass reeds cancel out by vector addition and fall below the actuation threshold. When the actuator magnets are outside the actuation zone, the bias magnets dominate. When the actuator magnets reach the dead zone, the actuator magnets over power the bias magnet's fields and re-actuate the glass reeds.

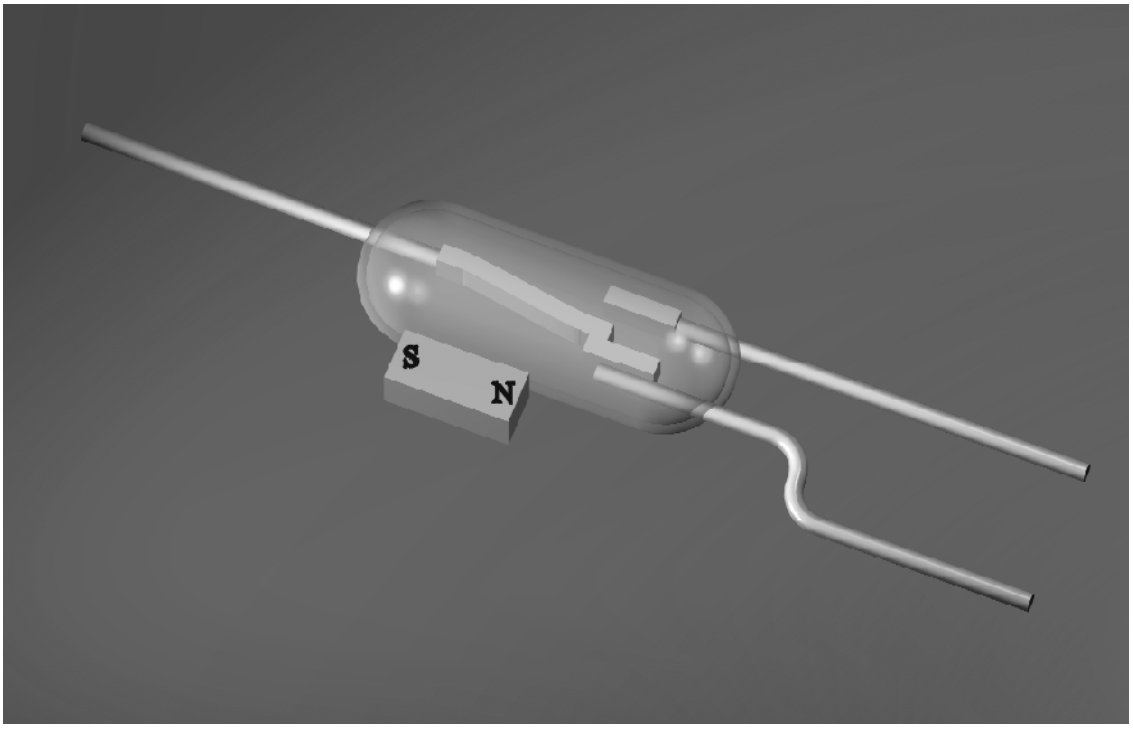


Figure 4: Magnetically Biased Form C Glass Reed Switch

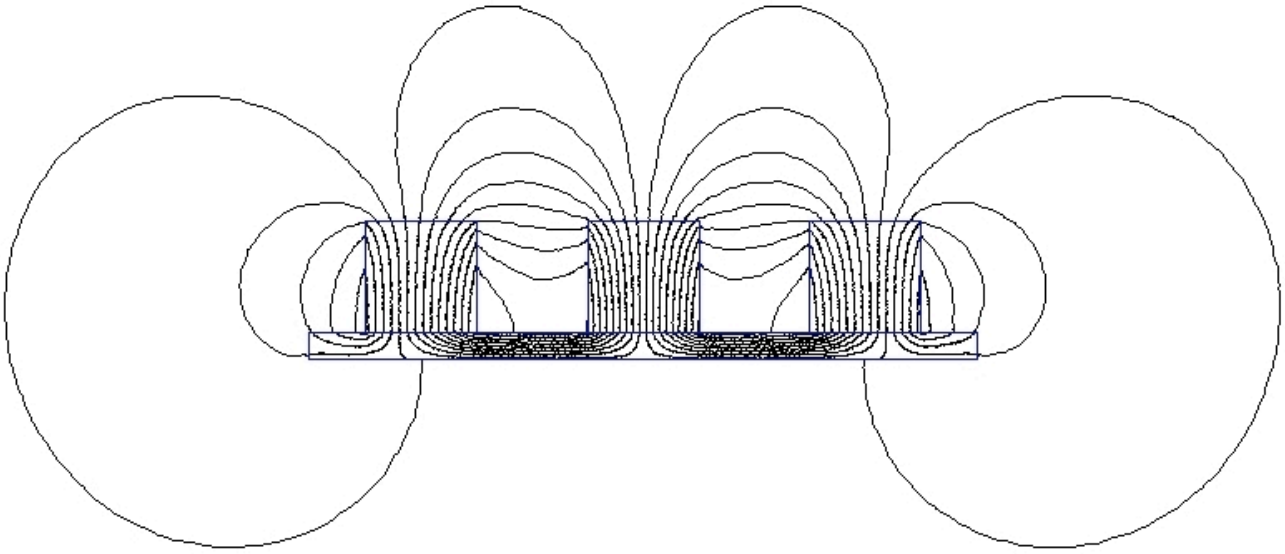


Figure 5: Holce Actuator Finite Element Magnetic Field Plot

Figure 5 is a Finite Element Magnetics field plot of the Holce actuator of the predominant device shown in Figures 6, 7, 8 and 9. It consists of three ceramic ferrite permanent magnets fixed to a sheet metal strip and embedded in epoxy as seen on the right side of Figures 6 and 7.

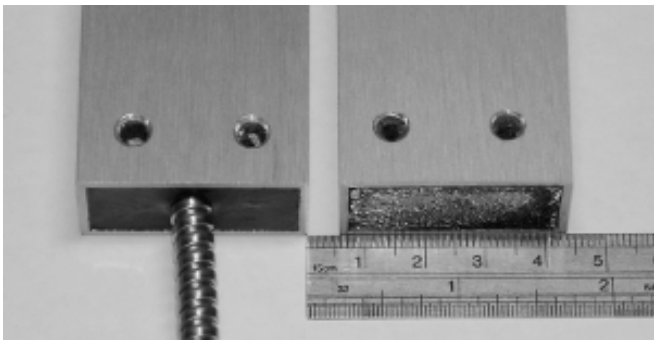


Figure 6: Minimum Actuation Gap Showing Dead Zone measured from the switch face.

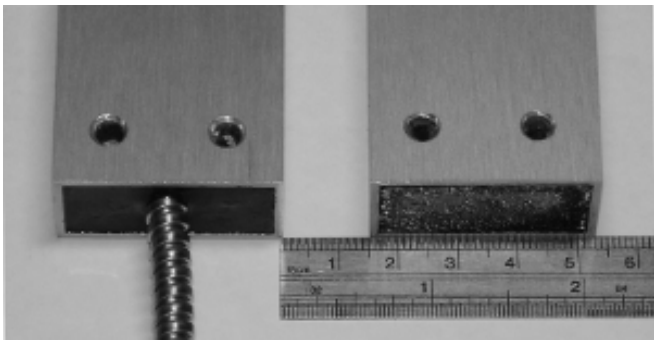


Figure 7: Maximum Actuation Gap measured from switch face.

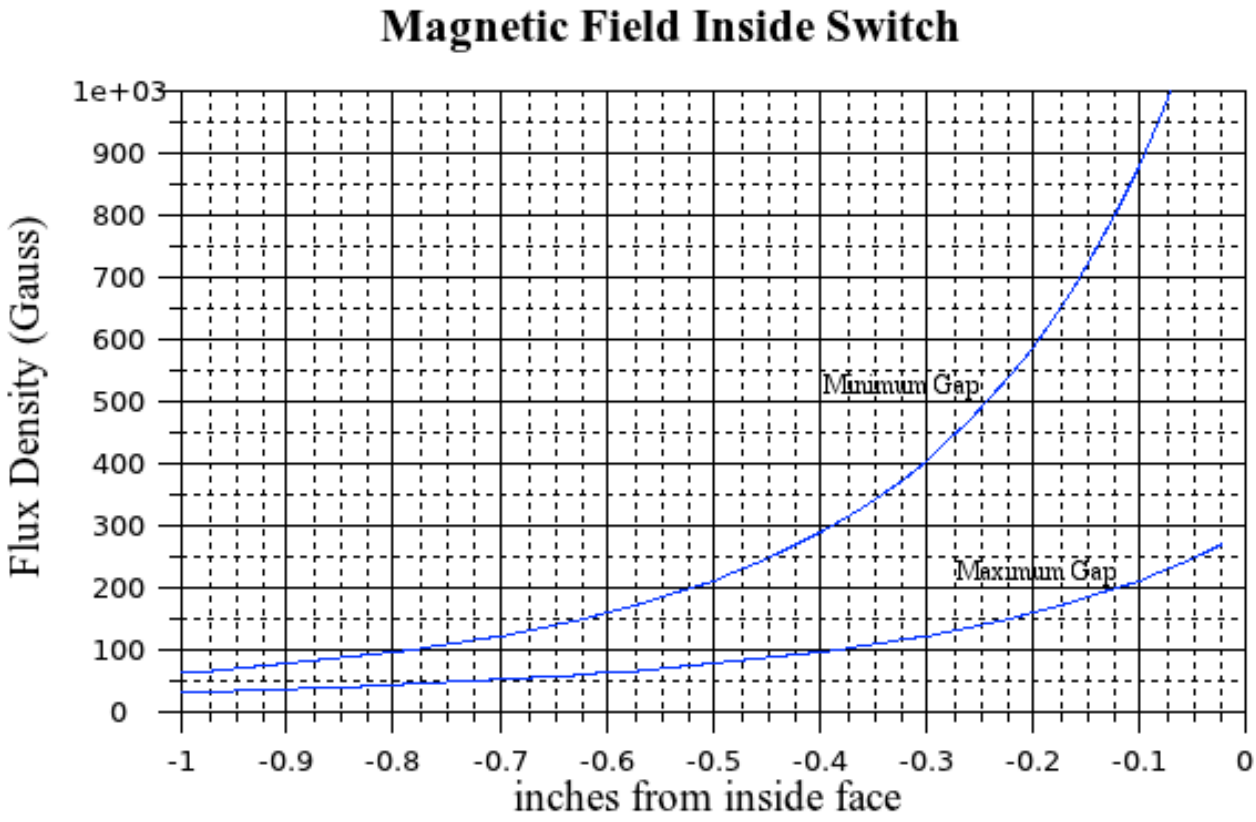
Gap distance is measured from the BMS housing face set as the origin. Gap lengths are positive and position inside the housing is negative. Figure 6 shows the minimum gap, 0.2 inches, for which closer approach sets off the alarm; the "Dead Zone". The upper curve labeled Minimum Gap in Graph 1 is a plot of the magnetic field inside the switch when the actuator magnet is at its minimum approach. Figure 7 shows the maximum separation distance, 0.6 inches, from the switch. The lower curve labeled Maximum Gap in Graph 1 is a plot of the magnetic field when at maximum separation. The space between these two extremes is the safe or secure position. A gap greater than the Maximum sets an alarm state.

How to Defeat It

The defeat stick fits into the dead zone and makes the switch think it sees its own actuator. The defeat stick is quite innocuous and not usually noticed under casual inspection. This dead zone is an artifact of the bias glass reed technology. The defeat stick is made possible by rare-earth permanent magnets and computer aided design.

The only requirement to defeat the switch is that an actuator narrower than 0.2 inches be introduced into the "Dead Zone" with a suitable magnetic field. The Defeat Stick magnetic field, as measured normal to its center magnet, must fall between the upper and lower curves shown in Graph 1. These two curves are found by measuring the field normal to the center magnet of Figure 5 and off setting it by 0.6 inches to get the bottom curve and off setting it by 0.2 inches to get the top curve with the origin at the face in each case. Clearly the magnetic field will be greatest at the nearest approach and decrease in magnitude as the separation increases. These two curves represent the magnetic field upper and lower boundaries of the secure state inside the switch housing.

Figure 8 shows a Defeat Stick on its side at the actuation face of the switch. Figure 9 shows the Defeat Stick properly positioned in the Dead Zone. The switch registers safe or secure in this position. To further aggravate the situation, the Defeat Stick can be inserted when the actuator is in position without a single glitch.



Graph 1: Maximum and Minimum magnetic fields inside the BMS housing for switch activation measured from the housing face toward the housing back wall.

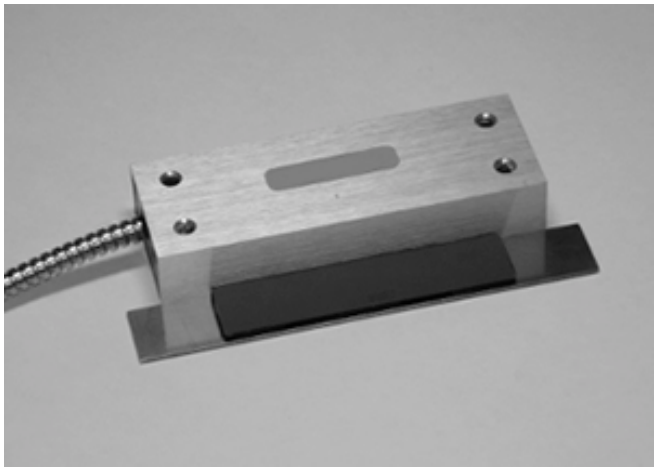


Figure 8: Defeat Stick top view near BMS housing face.

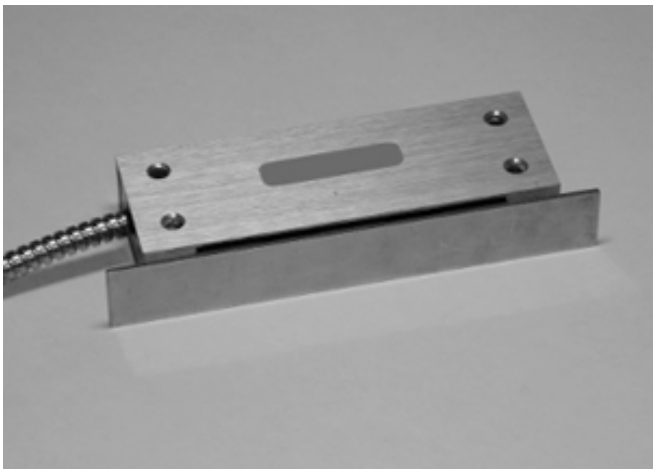


Figure 9: Defeat Stick in position for "live" defeat. The BMS thinks it sees its actuator.

The argument that the actuator magnets should be rare-earth materials to avoid this type of attack is irrelevant, because the glass reeds inside the switch only need to see the actuator magnetic field range between the two curves in Graph 1. The type of permanent magnet material only affects the physical dimensions of the actuator magnets needed to achieve the required actuator magnetic field profile. The defeat stick will always be effective regardless of the magnet material. Making the bias permanent magnets more powerful causes the actuator magnets to be more powerful, but can shorten the actuation range dramatically. The balance between all of the components can only be effectively achieved with computer aided design targeting specific geometries.

The concept of alternating magnet poles from N-S-N to S-N-S only means there needs to be two defeat sticks and a hall sensor to determine which polarity arrangement to use. I have one that looks like a pen and only indicates N or S. Swipe the hall sensor through the gap and pick the appropriate defeat stick. The entire kit fits into a shirt pocket resembling a pen and small ruler.

The Intruder

The most common misconception regarding high security physical electronic installations is that most intrusions are from the outside breaking into the facility. However, nearly 75% of all security breaches are "inside jobs." [7] In either case, high security is usually focused on the professional intruder who has some expertise defeating electronic physical security systems with the intent that these systems make this difficult, error prone and time consuming. Professionals study their targets and develop a breach strategy. Even a non-professional who is just an employee has all the time in the world to study the system, devise a scheme and execute it at just the right moment. If handled properly, the breach might actually go completely undetected. With the security sensors sabotaged, one could walk in and out unnoticed unless something was actually missing that exposed the breach. The BMS is perfect for this type of operation. Anyone could sabotage these sensors, breach the system completely undetected and later restore the system without raising suspicion. Too make matters worse, the BMS is widely believed to be "undefeatable." Due to this misconception, they are even placed exterior to an egress with the total confidence that no one can pass undetected. The BMS is so highly regarded that other types of sensors are frequently not installed with complete reliance on the BMS. In fact, some video surveillance cameras are only active when triggered by the BMS, so that anyone could walk in and out of a facility at will without ever being seen.

Laboratory Measurements

The test fixture shown in Figure 10 is all non-magnetic on a precision tooling plate with jeweled bearing slides and 3 axis stages. The combined position accuracy is within ±0.001 inches. Gauss meters are laboratory grade to within ±1%. The laboratory environment is kept a 22°C ±1°C with Relative Humidity less than 40%. The standard deviation observed on commercially available BMS was ±20%.

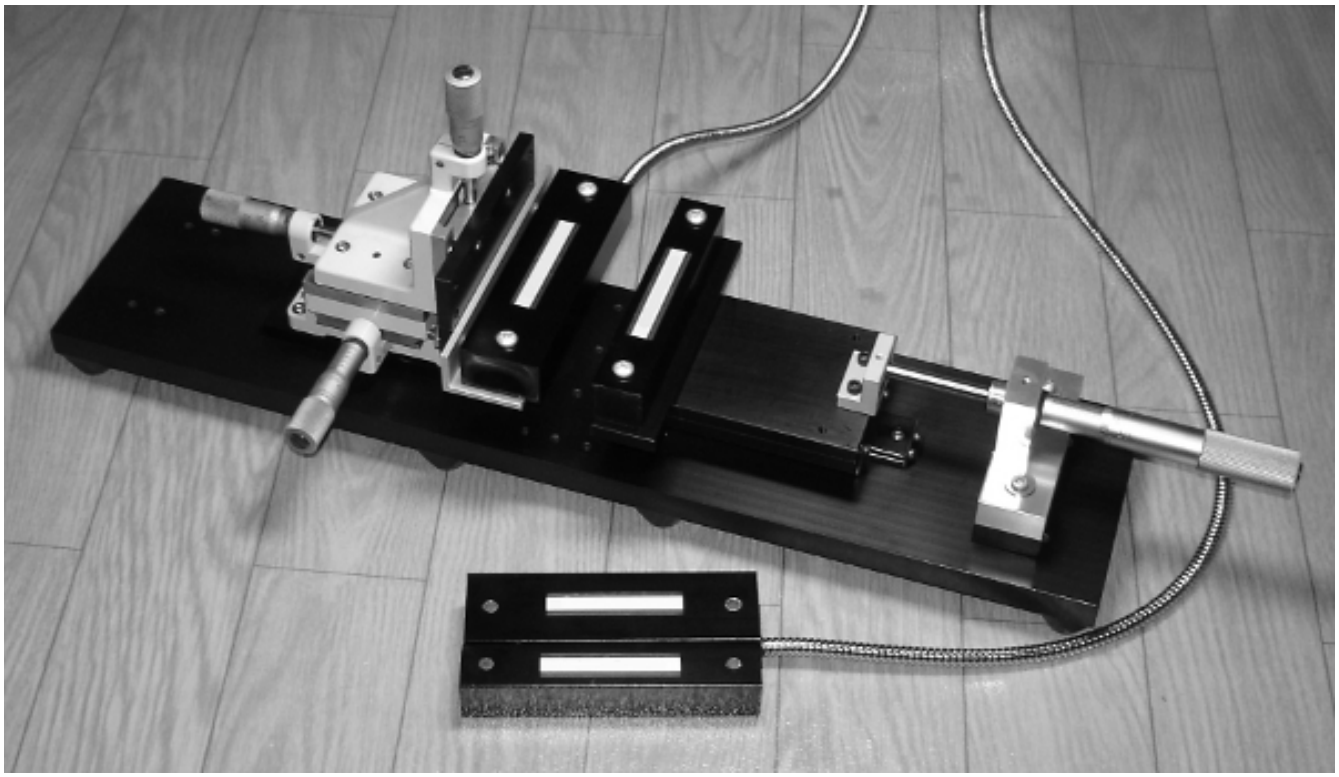


Figure 10: Precision Tooling plate and 3D stages for BMS laboratory grade measurements.

Only the field plot of any particular actuator magnet along the actuator magnet normal axis for any BMS that deviates from the Holce construction and its actuation range is needed to determine the specifications for a new defeat stick using computer aided design. The procedure is to measure and plot the actuator magnetic field and adjust the defeat stick's magnetic field until it fits into the gap with the same profile. All the BMS I tested were defeatable by the same set of defeat sticks. This same principle can be applied to any angle of approach, such as the top or the back. Shielding only means the magnets must be larger to penetrate the shield, which can be taken into account with good computer aided design. Blocking the Dead Zone is not enough. All BMS consisting of glass reeds have other similar zones of vulnerability as detailed in Jackson et al., [6].

Conclusion

The basic concept behind the traditional BMS as described in the current literature and various specifications is obsolete, highly vulnerable to trivial attack and imparts a false sense of security. A plurality of alternating magnetic poles in combination with glass reed switches, or their equivalent, can always be defeated by trivial means in any physically realizable practical configuration. The "Defeat Key" is the principal form of successful attack. It is virtually impossible to protect against except for a few very specialized cases. The BMS is not an obstacle to a professional intruder. It is only an annoyance. Any alternative technologies considered as replacements for the BMS should be very carefully examined to avoid an

unfounded confidence on trivially defeatable or unreliable technologies. The standard BMS utilizing glass reed technology is no better than a home security single and imparts a false sense of security. Anyone, not just professionals, can defeat it trivially, including the janitor.

About the Author

John T. Jackson, Jr., MS received his BS Physics from Oregon State University and his MS Electronic from the University of Nevada, Reno. He is the inventor of the "Wide Air Gap Permanent Magnet Motors" (slotless motor). He has patents in the field of physical security. He is a magnetics specialist and maintains a private research and development laboratory in Hong Kong.

References

[1] Elwood, Walter B., "Electromagnetic Switch", US Patent # 2,264,746, filed 1940.

[2] Holce, Thomas J., "Magnetically Actuated Sensing Device", US Patent # 4,210,889, 1970

[3] Jackson, John T., Jr., "High Security Balanced Type Magnetically Actuated Proximity Switch System", US Patent # 5,668,533, 1997.

[4] Jackson, John T., Jr., "Balanced Magnetic Proximity Switch Assembly", US Patent # 5,929,731, 1999.

[5] Federal Specification Components for Interior Alarm Systems, Balanced Magnetic Switches, W-A-450/1 August 28,1990.

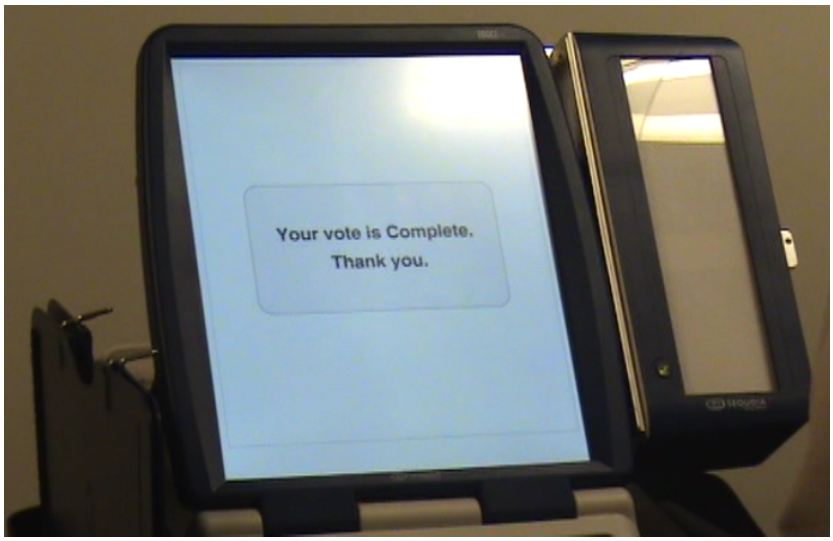
[6] Jackson, John T., Jr., "The Jackson High Security Switch and Radio Frequency System", thesis UMI Number 1389436, Copyright 1997 – 1998. Download PDF copies at www.jrmagnetics.com

[7] Improving Security from the Inside Out, A Business Case for Corporate Security Awareness, copyright 2004 National Security Institute.

VULNERABILITY ASSESSMENT AND SECURITY AUDIT OF ELECTION DAY POLLING PLACE PROCEDURES FOR THE APRIL 5, 2011 MUNICIPAL ELECTION IN CHICAGO, ILLINOIS

SHARON MERONI
Executive Director
Defend the Vote

Telephone: 847-382-1100
Email: Sharon@DefendTheVote.com



KEYWORDS

Election Security, Election Auditing, Election Integrity, Defend The Vote, Audit The Vote, Chicago Elections, Chicago Board of Elections, Illinois State Board of Elections, Voting, Election Integrity, Elections, Audit, Illinois, Sharon Meroni

-Well, Doctor, what have we got—a Republic or a Monarchy?
-A Republic, if you can keep it.
--Benjamin Franklin (1706–1790)

Does my vote really count? It's amazing how complicated it can be to answer such a simple question. The more ballot integrity is investigated, the more questions that arise!

At Defend the Vote, we believe the only way to have an accurate vote is through strict and transparent procedures that hold those in charge accountable for the security of the ballot. These procedures must provide a transparent record on the chain-of-custody of each event that potentially impacts the integrity of the vote, especially during the process of casting and counting the ballot. It also includes security protocols around election machines and materials during their storage and transportation; before, during and after elections.

Seal protocols are vital to the integrity of any election, but just because someone places a seal on a device does not magically protect it. Seals can be tampered with even with the best protocols in place. In Illinois, "tamper evident" seals are placed on ballot supplies and equipment to secure ballot boxes, voting-machines and the components that operate them, the bags used to transfer election results, and the large equipment containers that transfer the equipment from one location to another.

On the surface, the Chicago Board of Elections (CBE) looks like a legitimate organization that is genuinely concerned about the integrity of our vote—that's their job, after all! Does the CBE have security measures in place that reasonably assure an accurate vote?

The research contained in this report concludes they do not. We find the actual procedures in place are inadequate even when they were followed. Our investigations uncovered that current Election Day voting security procedures are not tracked, maintained, or reinforced. Seals used to indicate tampering, their use protocols, and other related security measures are not sufficient to detect or deter tampering with the ballot. How lax has the system become?

This report focuses on the processes and procedures in place to secure votes cast during Election Day polling. We looked at procedures designed to provide a chain-of-custody over ballot related supplies and equipment. We looked at evidence through FOIA's by attending public testing of machines before elections (Pre-LAT's), the 5% Auditor ballots cast after each election, and through a surprise vulnerability assessment and security audit of procedures in place at 239 precincts during the April 5th Municipal Runoff Election.

We found the following:

- Current seals and related security measures do not provide sufficient guarantees of election integrity.
- The seals in use do not reliably indicate when they have been tampered with.
- Procedures in place for the use of seals completely invalidate their use as a measure of security.
- Procedures in place for testing machines both before and after elections are inadequate in assuring a tamper resistant voting environment.
- The CBE fails to provide adequate security practices in the storage, transportation, and chain-of-custody for voting supplies and equipment.
- Current seal installation, training materials and instructions, and follow-up protocols are insufficient for developing a security culture.

- The current security culture at the CBE fails to provide independent security and vulnerability assessment of the CBE performance on providing a secure voting environment.

GENERAL STATEMENT OF PURPOSE

This report and its underlying investigation support transparent and public elections to assure fair and accurate recording of the vote. Ballot integrity is vital to assure that no voter is disenfranchised, that every eligible voter is able to cast a ballot, and that every legitimate ballot cast is accurately tabulated. Voters cannot presume the accuracy of the vote without adequate means to evaluate voting systems and processes. This includes independent evaluation and testing of procedures put in place by election authorities to assure the integrity of the elections, as well as subsequent compliance with these procedures.

Being a human endeavor, no election will be perfect. But elections can be improved, both to ensure accurate vote totals and to prevent fraud.

Accordingly, for the "Supplementary Aldermanic Election of April 5, 2011" (the municipal run-off election in 14 Wards), a vulnerability assessment and security audit of ballot integrity procedures in the polling place (hereafter the "Audit") was conducted as an investigatory measure.

In the Audit, pollwatchers asked questions of CBE personnel and inspected equipment. Pollwatchers used worksheets derived from the Chicago Board of Election's judge training manual, which addressed 13 different questions or inspection tasks directed to ballot integrity. A key aspect of the Audit was to observe and record the use of seals at the polling place.

Elections cannot be effectively or fairly conducted without the vital service of literally hundreds of thousands of volunteer election judges across America. The Audit was undertaken with complete confidence that the vast majority of Chicago Election Judges are simply fellow citizens honestly serving their community in a complicated role. That opinion remains unchanged after the Audit.

No part of the Audit was, or is now intended to impugn the judges or their good service. Rather, the Audit is designed to provide a view into a complicated, but still suspect system of ballot integrity in Chicago elections under which our election judges must operate.

In performing the Audit, a preliminary database of information was created to assess how the Chicago Board of Elections is performing in the administration of Chicago's elections. We believe that the Audit results and related implications have a wider application throughout the State of Illinois.

Reasons for the Audit

Preliminary investigations of Chicago Board of Elections election procedures were conducted by attending public pre and post election events, by visiting voting sites in Chicago during Early Voting and Election Day balloting, through review of election training manuals, and with the use of FOIA's for additional information. These investigations, conducted prior to the Audit, indicated that issues of non-compliance with ballot equipment security standards and procedures might widely exist in Chicago elections.

Preliminary investigations indicated a pattern of problems related to maintaining valid security seals on balloting equipment, which represented a significant security risk in the operation of elections. The potential implications to the integrity of the vote raised by these preliminary investigations were profound.

A second rationale was that the Chicago Board of Elections does not currently audit processes or procedures for Election Day polling place activities. Illinois statute requires a 5% mandatory statewide audit;* however, the local election authorities confine that audit to ballots cast on Election Day in the polling place.†

In addition, motivating this Audit is the lack of information available to the public about security in the voting process. For example, it is difficult and sometimes impossible to obtain information about the administration of the voting process, and the data is not collected or readily available to the public.

Methods

Over 20 Pollwatcher Auditors and 6 Supervisors audited 7 wards; visiting 239 precincts. Each pollwatcher conducted observation of poll opening procedures, poll closing procedures, and inspection of multiple polling places during the period the polls were open.

Results Summary

Of the precincts audited, **90%, were found to have substantial issues of non-compliance with important ballot security procedures**. 57% of the precincts had multiple instances of procedural non-compliance. Only 21 precincts of the 239 had perfect scores, or less than 10%.

Main Conclusion

This study finds that significant procedural failures are occurring on an ongoing basis throughout the election process. We find even if current procedures are followed, these procedures completely fail to provide a tamper-resistant balloting environment. As a result, the integrity of votes cast in Chicago elections is subject to question.

Our next step is to do a citizen-run security assessment (an audit) of the entire state of Illinois.

A more detailed summary of the audit's results can be found starting on page 30. The section on polling place equipment (pp. 20-26) is rich with information specific to Chicago and Illinois. The section on "Seals and Facts About Seals" (pp. 27-29) explains the significance of seals. The information found in "Additional Vulnerabilities" provides important information about how our elections are run. (pp. 45-47)

---

* Prior to the proclamation, the election authority shall test the voting devices and equipment in 5% of the precincts within the election jurisdiction. 10 ILCS 5/24C-15

† Our research also demonstrated that Early Voting programs in Illinois have never been audited. The Illinois State Board of Elections has not developed procedures to audit Early Voting.

OVERVIEW

Background and Scope

The introduction of new electronic voting systems has significantly altered how elections are conducted, especially in the past decade. Yet multiple methods still exist by which an election can be compromised. The method chosen to compromise the vote is often contingent on the level of access to unprotected (or poorly protected) ballot equipment or materials that a potential offender has. The first area of focus must therefore be the polling place, where the vote is initially collected.

Procedures for equipment use and ballot collection are installed in the polling place to assist in preserving the integrity of the election. These procedures include seals that are designed to secure vulnerable aspects of the technology or equipment in the polling place. The scope of this investigation involved observation and recording of procedures on Election Day at the polling place.

This Audit did not focus on a specific area in response to a specific report or suspicion of fraudulent activity. The Audit was not designed to detect specific instances of fraud. The Audit checked processes and procedures on Election Day to determine compliance with ballot security measures and procedures.

Additionally, absentee voting, nursing home voting, and early voting are not included in this Audit. No assessment of voting systems can be considered complete without considering early voting and absentee voting. Receiving Stations where election materials are processed immediately after the election were not included in the Audit.

Gaps in Knowledge

It is impossible to quantify how effective the current procedures are in preventing fraud. There is a lack of oversight leading to a lack of accountability, especially in critical matters relating to the security of the voting equipment. We cannot accurately assess what is not measured by election authorities.

Additionally, knowledge of the procedures for election equipment storage and protection between elections and just before Election Day remains largely limited or unavailable. Chain of custody gaps in voting equipment, material management, and the related processes can create vulnerability for the integrity of the vote.

What cannot be seen, traced, or inspected can be corrupted in the election process. The problem is magnified when there is no public oversight, auditing, or accountability. This Report should therefore be regarded as only a beginning in the work of Defend the Vote.

Approach and Audit Methodology

Timing was very short. There were but 4 days to plan and organize the Audit after final commitment of financing. We had a small group of lawyers on call, including Steve Boulton, General Counsel for the Chicago GOP, who volunteered to be in the field the entire day. Steve also acted in a general advisory role for the Audit, and assisted in the writing of this Report. Peter Bella, as

Executive Director of the Chicago GOP, recruited and supervised teams of pollwatchers and acted in a general advisory role.

Teams: The city was divided into sections based on geography. Each Chicago ward had supervisors and 2 or more pollwatchers in teams which were coordinated to cover the ward. Besides Steve Boulton on the ground all day as a volunteer lawyer, we had several local lawyers on call.

The best case scenario conceived was that teams could travel to 3-4 precincts an hour. Each stop was expected to take 10 minutes plus travel time. About 30% of the polling places have multiple precincts, shortening the travel requirement. The teams were designed to make 3 stops an hour. Supervisors generally drove and coordinated the teams; occasionally they went into the polling place.

Just before Election Day, two training sessions were held for the teams. Worksheets to be used in the Audit were distributed. Pollwatchers were instructed to get in and out of the polls as quickly as practicable, and not interrupt judges who were busy with voters. The pollwatchers were instructed to take on the role of an objective observer and recorder of information, and not to correct errors at the poll unless it involved a seal. If a seal was broken, the pollwatchers were to record the issue and ask the judges to place a new seal on. The pollwatchers were instructed to report other issues to their supervisors, who would decide if they would contact the legal team or Election Central.

On Election Day, the teams began the day before dawn, deploying as close to 5:00 am as possible at multiple precinct polling places. The pollwatchers began by auditing the opening of the polling place until the polls opened using the Poll Opening Procedures worksheet. Following the opening, teams were to switch worksheets to the Daytime Procedures worksheet and visit multiple polling place locations. There was time allocated for lunch breaks. Teams picked polling places that had multiple precincts to audit the closing procedures and to collect the closing tapes, using the Poll Closing Procedures worksheet. That night, the teams met to receive pay and to turn in their worksheets and poll tapes.

Worksheets: Three worksheets were created and used containing specific questions and inspection procedures to be asked of polling place personnel:

- Opening Polling Place Worksheet: 5:00 am to 6:30 am
- Daytime Worksheet: 6:30 am to 6:30 pm
- Closing Polling Place Worksheet: 6:30 pm to 8:00 pm

The worksheets targeted procedural compliance at the polling place and, in particular, the tracking of seals used as security measures on balloting equipment. The worksheets also guided the pollwatcher in what information to record. The worksheets provided space for notes by the pollwatcher on what was observed.

The worksheets were primarily based upon the procedures stated in the The Judge of Election Handbook for the Feb. 22, 2011 Municipal General Election and the April 5, 2011 Supplementary Election issued by the Chicago Board of Elections. It was expected pollwatchers would attempt to get as many answers as possible. The pollwatchers were instructed not to press for answers if they encountered any resistance from the election judges on answering a worksheet question.

The answers were transcribed into spreadsheets sorted by wards and then by the number of red scores. Thus, the worksheets are the basis for the subsequent data analysis for the Audit.

Data: Sorted by wards, the data is grouped based on 13 tasks, to which three responses are possible. Yes (in compliance); No (not in compliance); and N/A (no answer is recorded). N/A responses are counted but not otherwise scored. The data is sorted by counting the Yes and No responses, then determining a percentage for "No" indicating noncompliance. Data percentages are calculated for the 13 items for the precincts, the ward, and finally a city score. Averages are used to provide a score for the section.

The 13 questions or tasks are coded as "Red" (critical: potentially impacting the vote) or "Yellow" (caution: does not likely impact the vote.). In some of the scoring, Yellow scores were noted but not included in the results. 11 of the 13 areas audited were scored as Red. 2 questions were scored as Yellow. Compliance with each question was answered as a Yes, No, or N/A.

Results, Merit and Applications

As demonstrated by the database summaries attached, out of the 239 precincts audited, 215 precincts failed with one or more Red Task error. 135 precincts (or 57%) had more than one Red Task error, 79 (or 34%) of these had 3 or more Red Task errors.

Only 21 precincts (or 9%) had no errors.

This Audit provides a current database of knowledge assessing the effectiveness of procedures in place on Election Day. Results will be used to encourage voluntary compliance to new audit procedures beginning with the March 2012 Primary Election and to guide future audits across the state. These requests will begin with Chicago Board of Elections and the Illinois State Board of Elections.

MATERIALS, ESSENTIAL INFORMATION AND DATA

WARDS AND THE POLLING PLACE

On April 5, 2011, there were 14 Chicago wards that held run-off elections.

The following wards were audited:
36, 38, 41, 43, 45, 46, and part of 50.

Attempts were made to gain credentials‡ to polling places in the following wards: 6, 15, 16, 17, 20, 24, 25. Without candidate credentials, these polling places could not be audited.

Election Judges: The polling places should have a minimum of 5 judges. Chicago Election Judges must be registered voters in Cook County. Judges are assigned based on Party affiliation; Dem:Rep or Rep:Dem in a 2:3 ratio that switches equally from precinct to precinct. According to Commissioner Rowan's office, the turnout for this election was anticipated to be low, so some precincts had fewer judges than usual.

Each polling place is allowed two Student Election Judges. These students are trained at school. In general they have the same responsibility (and pay) as regular Election Judges. Student judges cannot, however, take election supplies to Receiving Stations. They are counted as part of the regular 5-person election team, but in some instances they are in addition to it.

Polling Place Administrator: Each polling place should have at least one Polling Place Administrator ("PPA"). A PPA is a Chicago Board of Election employee. They are responsible for assuring the poll is set up correctly and that it runs smoothly. PPAs are trained to assist with the equipment related problems that do not require a technician.

The Chicago Board of Elections hires and trains PPAs then assigns them to supervise each of the polling places. Single and multiple precinct polling places will be supervised by one or more PPAs.

To qualify as a PPA you do not need to be a USA Citizen. The PPA fills out a Form I-9. The PPA does not declare a party affiliation, and information about party activities is not collected. The PPA reports to the CBE. They are not an election judge and do not make decisions about voters at the polling place. PPAs have unsupervised access to election materials and equipment. They help with set up, closing, and Election Day procedures.

THE POLLING PLACE AND RECEIVING STATION

Polling Place: Polling is done in-precinct on Election Day at single or multiple precinct polling places. Chicago polling places are located within the Ward at a convenient location within (or as close as possible) the precinct. Polling places are schools, restaurants, churches, libraries, etc. Many polling places have multiple precincts.

‡ Democrat and Republican pollwatching credentials were not available for this election. Pollwatchers used various candidate credentials.

Receiving Stations: According to Illinois statute, once the polling place closes, voted ballots, memory devices and other essential materials are to be transported to a pre-designated counting station (AKA: Receiving Station) where Illinois statue designates the chain of custody switches from election judges to Chicago Board of Election employees.[§]

The Chicago Board of Elections establishes receiving stations across the City. Based on geographical proximity, election judges' transport voted ballots to the receiving station that is assigned to them. As a team of two, one person from each party is supposed to transport the materials. Judges do not have to drive together but they should travel as a team.

This study did not score procedures at the Receiving Stations; however preliminary investigations frequently demonstrated these procedures are not followed.

THE POLLING PLACE EQUIPMENT

Ballots and Ballot Styles: Each precinct has multiple ballot styles; most precincts in Chicago have 2 or 3, some as many as 7. Different ballots styles allows voting for candidates and issues that are split within precincts.

There are paper and electronic ballots. Paper ballots are delivered on card stock which, immediately after voting, is scanned into the ballot scanner to record the vote. Electronic ballots are delivered through the Sequoia EdgePlus - Touch Screen machine and recoded on a paper scroll and on a USB flash drive.[**]

On Election Day, the vast majority of voters take a paper ballot. Paper ballots are placed in the ESC (Equipment Supplies Carrier) before it leaves the Pershing Street Warehouse. When the ESC is opened on Election Day, the ballots are found inside, unsealed, unnumbered, packaged into groups of 50, and wrapped in plastic wrap. Unused ballots are returned unsealed in the same ESC.

After the election, voted ballots are processed by the election judges. Once counted, these ballots are placed in a plastic bag that is sealed with a paper seal signed by all of the judges. Instructions say:

> ***Seal and sign the bag:*** *Place the Voted Ballots Security Seal over the recloseable seal. Record the precinct and ward on the seal. All judges of election must affix their signature on the security seal." P 59*[††]

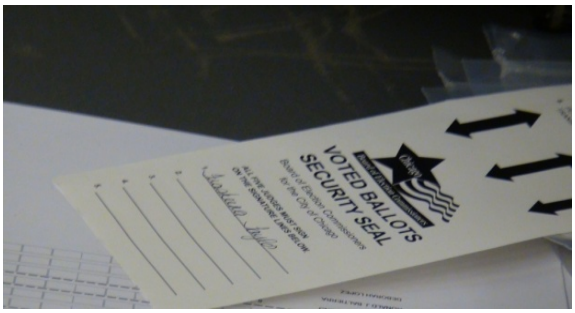
The clear plastic ballot bag is placed inside the blue transfer case pictured on the next page. All 5 judges must sign a paper seal used on the clear bag. The blue transfer case is delivered to the Receiving Station during the evening of Election Day and contains the ballots, poll tapes, etc.

[§§] Thereupon two of the judges of election, of different political parties, shall forthwith and by the most direct route transport both ballot boxes to the counting location designated by the county clerk or board of election commissioners. (10 ILCS 5/24A-10)

[**] All Early Voting in Chicago and Cook County is done on the Sequoia EdgePlus. Note: City and county wide, each of these machines contain all of the ballots for Chicago and Cook County. These are loaded from the *results cartridge*.

[††] Our research documents that the CBE does not track compliance with this requirement. When the 5% audit is completed, the auditors do not check compliance with this procedure. Auditors (who are CBE employees and not Election Judges) break the seal when they open the bag for the recount. At the conclusion of the audit, they replace the paper seal with a similar one that they sign.

Memory devices are returned in bubble bags. Also, an unsealed black bag is sent to the Receiving Station containing provisional ballots, spoiled ballots, and other forms that are required to be completed and then processed by election authorities (pay vouchers, etc). Only the blue transfer case is sealed with a red seal.



Voted Ballots Security Seal


Sealed Ballot Bag and the Transfer Case

Investigations show the sealing of the transfer case does not provide a secure chain of custody for the voted ballots. While the election judges sign a paper seal placed on the plastic bag containing voted ballots, election judge names are not cross-checked in the 5% audit to assure they are the actual judges. Election judges do not record ANY seal numbers during opening or closing procedures. The election judges do not record the seal number on the blue transfer case before leaving the poll at the end of the voting.

The red seal number on the blue transfer case is written down **during** the 5% Audit, but that number is not cross-checked with the original seal placed on the blue transfer bag by the judges. If the number is recorded on Election Day at the Receiving Station, that number is not sent to those completing the 5% audit to assure it is the same seal. There is no place in the paperwork to check seal numbers originally placed on the transfer case. The 5% audit records the number of the seal they find, but the number is not crosschecked presumably because originally it is not recorded.

Investigators checked paperwork, and questioned election judges, and were unable to locate any place where seal number are recorded by election judges at in-precinct polling places, or cross-checked when they go through the 5% audit.



Year after year, the same ESC (Election Supply Carriers) is usually sent to the precinct filled with that precinct's equipment. The ESC is sealed and locked with a filing cabinet type key that fits multiple ESCs. The ESC is sealed with a thin green seal on the outside of the door.

Election Supply Carriers (ESC's): Large containers called ESCs *(Election Supply Carrier)* are used to store the election supplies for each precinct. At the Pershing Street Warehouse, these are loaded and locked with a universal key, and then sealed with a thin plastic green seal.

The ESC contains collapsible voting booths, three machines, a ballot box, all election instructions and supplies, and the paper ballots for the precinct. Polling places with multiple precincts have a separate ESC for each precinct.

Reviewing documents provided through a FOIA, shipping documents for the ESC containers do not record the seal numbers. Investigators prove when the ESC is delivered from the trucking company to the polling place, the number on the sealed ESC is not recorded. The form provides a section for "damage from delivery" but this is only used if the actual ESC is damaged, not the seal. The seal number is not mentioned in any of the documents we reviewed.

Investigations through FOIA and from a review of training manuals prove ESC green seal numbers are not provided to the election judges or the PPA to record or verify.

In November 2010, investigators questioned Robert Sawicki, deputy chief administrative officer for the Chicago Board of Elections. Mr. Sawicki stated that the green seals trigger personnel at the warehouse that the ESC is ready to be shipped.

Inside an unsealed blue box that is stored inside each ESC, there are extra green seals placed to reclose the unit with. These seal numbers are not recorded. Used seals are not retained. Election judges report they routinely throw them out because they are not given any instructions to retain them. Election judge paperwork, which lacks record keeping procedures for the seals, backs this claim up.

There is a smaller version of the ESC that is used in polling locations where the larger version has access difficulties. These ESCs do not secure all of the voting equipment inside. **IMPORTANT:** The ESC is dropped off and picked up by 4 outside trucking companies currently under contract with the Chicago Board of Elections. ESCs may be dropped off as early as two or three weeks before an election. Based on the logistical rotation for drop off and retrieval, the ESCs remain in place at the polling place for approximately the same amount of time both before and after the election.

ESCs are received at a polling place by a *responsible party* who signs for it. While there is the expectation that the ESC will be protected, there is no requirement to keep the ESC in a locked room. They might be stored in a corner in the gym, or sometimes tucked away in a hallway. Investigations looked for and could not find documentation of the chain of custody of the ESCs while at the polling place. The Chicago Board of Elections explains this is the responsibility of the owners of that facility.

Ballot Box:

Securing the ballot box is basic to the integrity of the polls. By law, ballots must be under seal.[‡‡] Our investigations found ballot boxes were not sealed 59% of the time at polling place. Based on 10 ILCS 5/15-1 (from Ch. 46, par. 15-1) the CBE is required to seal the ballot boxes.[§§] Similarly, the

‡‡ While the ballot box discussed here is for paper ballots, electronic ballots (and their paper copy) must also be kept sealed.

§§ (10 ILCS 5/15-1) (from Ch. 46, par. 15-1)

Sec. 15-1. (a) Except in municipalities operating under Article 6 of this Act, the county board shall provide a sufficient number of ballot boxes, with secure locks and keys...

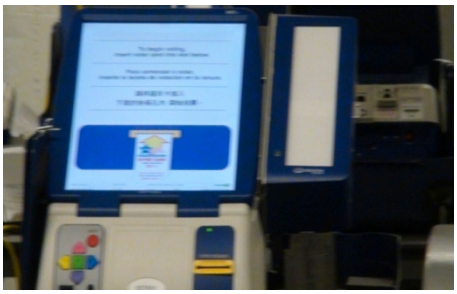
(b) The county board may provide ballot boxes not of a permanent type, not of wooden or metal construction, not requiring locks or keys, nor having doors or windows, if (1) such ballot boxes are so constructed as to be completely sealed and empty units upon delivery to the polling place. (Source: P. A. 77-6).

transportation of ballots after voting is not done according to code which requires they be securely sealed.

The ballot box is set up by the election judges and/or the PPA. The ballot scanner is placed on top of the ballot box. Pollwatchers and judges check to that the box is empty prior to the sealing of the box. Two seals are placed on the ballot scanner and the ballot box, binding them together. Providing a 'chain of custody', the purpose of the seals is to assure no one disturbs the ballots after voting.

It is the job of election judges and the PPA to seal the collapsible ballot boxes to the ballot scanner. Reports are plentiful of investigators and other Board employees coming and going at polling places without assuring the ballot boxes are sealed. Instructions for sealing states: *"Secure ballot scanner to ballot box by threading the seal through the holes"* (pg 17).

Unsealed, the ballot scanner on top of the ballot box



EdgePlus Touch Screen – paper scroll on right side.

Election Machines: There are three machines used to cast a vote in Chicago:
Sequoia (Dominion) Touch Screen EdgePlus (VVAT - Voter Verified Audit Trail – Paper ballot)
Sequoia (Dominion) Optech Insight Plus Optical Scan (Ballot Scanner)
Sequoia (Dominion) Hybrid Activator and Accumulator (HAAT – Card Activator)

Sequoia (Dominion) Touch Screen EdgePlus – This machine is called the Touch Screen (T/S). The T/S contains the electronic ballot. As already noted, the T/S is used for Early Voting too.*** The vote is recorded onto a *"results cartridge"* which is a USB Flash Drive inserted into the cartridge port. Voters are given an activated voter's card when they register. This card is inserted into the machine which recognizes what ballot to electronically provide to the voter.

The T/S machine is a firmware shell††† driven by the software loaded from these cartridges. The results cartridges record the serial number of the machine used to record the vote. These machines are tested and sealed at the Pershing Street Warehouse prior to being loaded into the ESC.

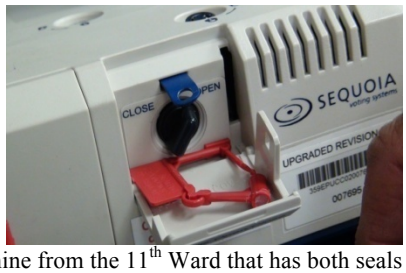
At the warehouse, the machine is loaded with the ballots for that precinct through the cartridge port using a results cartridge. A results cartridge is left in the machine inside the cartridge port which is secured at the warehouse with a red seal. Election judges are not given this number to check to assure the seal was not tampered with after it was placed on at the warehouse. We were unable to document any chain of custody on these seals or their numbers once placed on the machine. Election judges report they routinely toss these seals in the garbage.

*** Procedures for Early Voting are different then Election Day. The T/S is loaded with the ballots for the entire City for Early Voting. This will be discussed in a separate document.
††† Firmware is a combination of software and hardware that have data or programs recorded as 'read only' on them.

A paper scroll is located on the side of the machine and is the paper trail for the vote cast. The voter approves what is printed on the scroll before removing their voter card and leaving the voting booth. This paper scroll is the record of the electronic ballot and as such it must be secured at all times. It is the mandated (IL Public Act 093-0574) Voter Verified Paper Audit Trail (VVPAT).

Voter cards for the EdgePlus are programmed with the Card Activator machine. They are reusable.

The T/S has three seals. One on the paper scroll, one on the Open/Close Port and one on the Cartridge Port (pictured below). The Open/Close Port arrives at the polling place with a yellow seal. The red seal is stored in the port as shown in the picture on the right below. When the poll is opened, the yellow seal is broken and replaced with the red seal. The Election judges are responsible for replacing the seal. Seal numbers are not recorded. There are extra seals in the ESC supply box which are unrecorded.

The back of the touch screen has two seals. The picture on the left shows a machine from the 11th Ward that has both seals open. The yellow seal is replaced by a red one when judges open the polls. The middle picture has the seals correctly applied. The picture on the right shows the red seal stored in the open/close port.

Sequoia Optech Insight Plus Optical Scan (Ballot Scanner): Election Day voting is primarily done through paper ballot. The ballot scanner reads the paper ballot. The ballot scanner is hardware and a firmware shell. It records the vote by optically scanning the ink marks on the ballot. The machine records the vote on the ***memory pack***, which is a memory device. Besides the memory pack, ONLY when there is a problem scanning the ballot, the error is recorded on the paper scroll printed by the scanner. This alerts the judge to issues recording the vote, prompting resolution to allow the ballot to be counted. This scroll does not print the vote, it records errors that occur causing the ballot to be rejected when scanning (i.e., over vote, under vote, no vote, no judge's initial). The memory pack records the actual vote that is cast.

There are three seals on the ballot scanner. One for the memory pack (applied at the warehouse) and two to secure the scanner to the ballot box (applied at the poll). These seals are essential to security of the ballot.

The back door of the ballot scanner is locked with a universal key. This key is stored in the ESC in an unsealed supply box. The memory pack is secured inside this locked port door with a numbered red seal. The seal is placed on at the warehouse. Again, there is no tracking of the number on the seal and multiple untracked replacement seals are left in the supply box.

> *"Remove ballot scanner key from blue supply box. Unlock rear door of ballot scanner and verify that red seal is attached to door. If memory pack door is slightly opened, push door closed. Make sure the power cord is plugged into the rear of the ballot scanner"* (pg 18).

Judges are instructed to check for the seal; there is no instruction to record the seal number or what to do if the seal is not properly secured. These instructions fail to alert judges that a breach of this

seal is a security issue that Election Central must be informed about. There is no place in the paperwork to record seal issues. Frequently election judges did not want to open the locked door to prove the memory pack has a seal. Many judges reported they were unaware the seal exists.

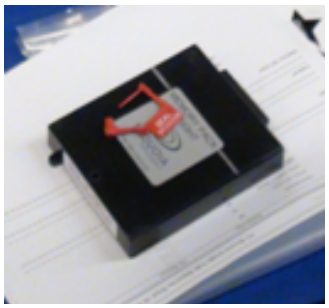
At the end of the election, the machine is turned off, the seal is broken and the memory pack is removed and placed in the HAAT or Card Activator to read. The paper scroll is placed in the blue transfer bag that is taken to the Receiving Station after the election. The red seal is routinely tossed in the garbage. There are no procedures or instructions to return used seals to election authorities.

Front of Ballot Scanner


Back of scanner-The memory pack is placed here.


Key locks the back of the ballot scanner

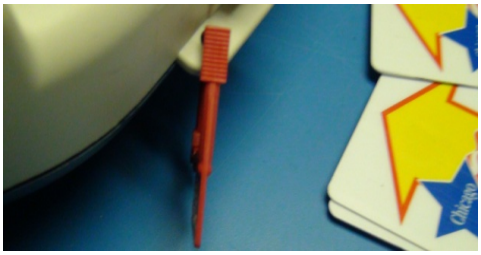
The seal on the memory pack


The memory pack

Sequoia Hybrid Activator and Accumulator (HAAT): The Voter Card Activator has several functions: it activates the voter's card with their ballot style on the T/S, re-programs the electronic voter cards for each voter, consolidates the ballots from the T/S and the Ballot Scanner, and transmits the election results to Election Central. The voter card activator transmits election results to Election Central with cellular technology. Election Central on Washington Street records if the voter card activator is online during the voting day.

After voting concludes, the results cartridge and the memory pack are removed from the T/S and the ballot scanner, and placed into the voter card activator (HAAT) which consolidates the two types of ballots into a single total. This total is then transmitted through cellular technology to Election Central on Washington Street.

When the Card Activator does not properly consolidate or transmit the results, the record of the vote is retained on the two memory devices. These are taken to the receiving station, and they are consolidated and transmitted there. This procedure should be done in front of election judges from both parties.



This is the seal on the Card Activator paper scroll.

Judges instructions neglect to inform the Election Judges of the use for this seal or to replace it when changing the paper scroll.

There is one seal on the Sequoia Card Activator. This seal is on the paper scroll which secures a paper record of actions recorded by the Sequoia Card Activator. The Handbook does not provide reference to this seal, except in the definition of seals on page *66, "red seals are on the following equipment when delivered to the polling place…"*

Election judges print a "zero count" receipt at the beginning of the day, and place this in the blue transfer case. This machine also prints out the closing tapes at the end of the elections. These tapes are given to pollwatchers. Poll tapes must be signed by all of the judges and placed in the transfer case. This procedure is not tracked for compliance.

Back of the Card Activator – Preparing to transmit to Election Central.

Box where some seals are placed.

Software: All software is placed on the *USB Flash Drive* and the *memory packs* at the computer room at the Washington Street office. Investigation of this process is ongoing. There are contractual and copyright restrictions on access to this information. There are also security-based restrictions.

The public does not have access to the software code. There is a small window where the political parties can request access; however they must provide a specialist to examine it. This is especially costly when one considers there are over 2500 precincts, each with 1 to 7 separate ballot styles. There is a procedure to seal the software code. This procedure is under investigation. In general all access to the information about the software code is secretive and cumbersome to find out about and requires access through multiple restrictive barriers.

There are employees from Sequoia who are part of the CBE team. These employees have offices and facilities on site. During the April 5% test, one employee was available at the test site but would not answer the investigator's questions.

There is an assumption that the integrity of the software code is affirmed in the Pre-Lat testing when each machine is tested to assure all candidates get a vote. Investigations of Pre-Lat testing are ongoing and have already proven that this testing does not test the integrity of the software.

Further investigation is URGENTLY needed to address the substantial integrity issues in this area.

SEALS AND FACTS ABOUT SEALS

"Generally speaking, a seal is a device that is not difficult to remove, but is supposed to leave evidence of tampering if it is removed. Seals must have a physical design that will show some difference in appearance or behavior if they are removed and reapplied. Seals are generally serial-numbered (or otherwise marked with a unique identifier), so that if someone removes the seal and replaces it with a fresh one, the new one will have a different number.

The purpose of seals attached to a ballot box is to assure that ballots are not tampered with (or replaced) between the time that voters deposit them and the time they are counted. Seals attached to voting machines are meant to protect against many attack vectors, in particular to assure that the vote-counting software is not replaced (with fraudulent vote-miscounting software) between the time the vote-counting software is installed (e.g., when the machine is manufactured) and the time that election results are reported. Clearly, in the latter case the seals have a much more difficult job to accomplish, since they must protect for a period of years during which many more people may have access to the voting machine."[###]

Plastic seals are used as part of the security check and balance on machines. Seals are used to secure the memory packs, USB results cartridges, and the paper scrolls. They are also used for the ESCs that transport equipment to the precincts for Election Day and for the blue transfer case that is used to transport voted ballots after the election. The intended purpose of seals is to provide proof that the election materials are secured and undisturbed. There are separate procedures for tracking seals on the equipment used for Election Day and Early Voting. This section relates only to Election Day processes.

A huge weakness in the present system is that seal numbers are not tracked before or after they are placed on balloting equipment. Seal numbers are not recorded by CBE procedures. Tracking of the seal numbers once they are on the machines is nonexistent. New or broken seal numbers are not recorded. Election judges are not trained to watch for missing or damaged seals. The training for replacing seals is inconsistent or lacking altogether. Frequently, PPAs do not replace broken seals. When technicians come out to replace malfunctioning machines during the election, they frequently do not replace the seals. Election Day procedures do not require broken seals to be returned in the ESC. Election judges report that they are routinely tossed in the garbage.

The plastic seals used are especially susceptible to counterfeiting and tampering. Unrecorded seal numbers provide untraceable opportunities for counterfeited seals to be used to replace valid seals. The particular brand of seal used is flimsy and especially vulnerable to tampering.

Seals Used: There are at least 4 plastic seals used in Election Day polling places: the green seal on the ESC, red seals used on paper scrolls and memory devices, yellow seals that are replaced by the judges when the poll is opened, and blue seals to seal the ballot boxes. These numbered seals are flimsy and easily opened without damage by inserting a paperclip inside and dislodging the serrated top from the bottom.

[###] Security Seals On Voting Machines: A Case Study, by Andrew W. Appel. *ACM Transactions on Information and System Security (TISSEC)*, 2011, in press. http://www.cs.princeton.edu/~appel/voting/SealsOnVotingMachines.pdf

Besides the plastic seals, upon closing of the polling place, paper seals are placed on used ballots in clear plastic bags before they are taken to the receiving station. Election judges are supposed to sign these paper seals. This procedure is not checked. In addition, during the mandatory 5% audit, auditors are not asked to check or record if the sealed ballots have an undisturbed paper seal or if the paper seal on the ballot bag has the correct names of the judges on it.

Judges also sign various envelopes across the flap closing the envelope to seal inside provisional applications and ballots, and spoiled ballots.

The Judges Manual provides this information on red seals:

> ***Red Seals –*** *Red means STOP. Do not break a red seal until the polls close. Red seals are on the following equipment when delivered to the polling place: the ballot scanner memory pack door; the touch screen printer, the results cartridge door and the Polls Open/Closed door (after the polls have been opened). A red seal will be placed on the transfer case after all the required items have been placed inside"* (pg 66).

Other than this warning, a few limited seal instructions are provided in sections on setting up the polling place.

Closed Seals and Security: The availability of a variety of untracked seals invalidates the seals as a security measure**.** The investigation continues, but we have proven the key to unlock the ESC is not specific to the unit. The same key opens multiple units.

Included in the extra seals provided in the supply box stored inside the ESC are several green seals used to secure the outside of the ESC. Once inside the ESC, there is unfettered access to ballots, election machines, and memory devices. If a machine is disturbed, an untracked replacement seal is kept inside the same ESC. The equipment and ESC is simply resealed with one of these extra seals. There is no tracking of the numbers or retention of seals.

In conclusion, a closed seal does not indicate that tampering has not taken place. It is smoke and mirrors shielding a complete breakdown in security.

Training on Seals: There is little to no training on seals for the election judges or the PPAs. Instructions do not include securing seals or recording seal numbers for the machines. Instructions do not highlight the importance of seals or require the reporting of seal issues. In many cases the election judges are not informed they need to attend to seals. Their training manual has few instructions about seals.

The Troubleshooting Guide provided to election judges (p 68-77) does not have a section on seals. The Judge of Election Handbook does not instruct the judges to replace the seal on the T/S scroll. It does not provide instructions for the card activator scroll.

When the ballot scanner needs to have the paper scroll changed, instructions are to cut and replace the blue seals on the side of the ballot box[§§§]. This act exposes the ballot box so two judges must be present for changing the paper roll. This indicates the CBE is aware it must keep a chain of sealed

[§§§] There is generally only one set of blue seals included in the ESC. These are the same ballot box seals that were not applied in 59% of the precincts.

custody on voted ballots, yet the Board's employees and investigators visit polls without assuring the ballot box and/or the paper scroll is sealed.

Significance

The seal issues present a significant security flaw. The lack of overall tracking and the liberal access to untracked seals completely invalidates them as a security tool for Election Day voting. They do not provide any meaningful evidence of tampering or lack there-of.

- Seal integrity issues occur at all levels of the election process.
- The Chicago Board of Elections cannot state that seals provide security at any phase of the election process.
- Tossing used seals in the garbage is very poor practice for many, many reasons.
- Seal numbers have to be secured, not just the seals themselves.
- To prevent counterfeiting, seals must be secured prior to use, and before they are applied, seals must be checked to assure they have not been tampered with.
- The yellow and red seals shown on page 14 are especially susceptible to tampering and must be carefully guarded and inspected to discern if tampering occurred.

AUDIT RESULTS

In total, 239 precincts were successfully audited in 7 wards. There were 13 questions or tasks areas: 11 critical (red) and 2 cautionary (yellow) which were checked.

- **90% (215) of these precincts failed at least one of the 11 critical Red questions/tasks.**
- **57% (135) of the precincts failed in more than one task area.**
- **3 precincts (1%) had Yellow failure scores because they failed to follow procedures relating to identification of the judges and PPA with badges at the polling place.**
- **21 out of 239 precincts (9%) received perfect scores.**

The timing of the decision to perform this Audit was such that we were not able to get credentials from each ward. As a result, the Audit was scaled back accordingly. The following wards were audited: 36, 38, 41, 43, 45, and 46.

Worksheets:

Open Polling Place Worksheet (5:00am to 6:30am): Completed at 30 locations. These answers are recorded in the appropriate ward's spreadsheet which is in the Appendix – (Summary of Results for Wards)

This worksheet is specific to opening procedures only. Two questions on this worksheet are not included in the data analysis of the 13 questions on the 239 precincts. The first question was, "Do the judges check for a zero public count?" Results: 24 yes, 0 no, and 6 N/A. The procedure for checking the zero count is reinforced because the opening poll tape must be printed and placed in the transfer case when the polls open. The second question was, "Was the ballot box empty before the polls open?" Results: 10 yes, 0 No, and 20 N/A. The pollwatchers did not check the ballot box 2/3 of the time and when they did, it was empty. The primary reason for 20 N/A is because many of the boxes were set up prior to the pollwatchers' observations.

Daytime Worksheet (6:30am to 6:30pm): Completed at 209 precincts. The detailed responses are available on the **Summary of Results for Wards** data sheets. The data is grouped by ward and itemized at the precinct level. The Summary of Results for Wards breaks down each precinct but does not display the precinct numbers.

Closing Polling Place Worksheet (6:30pm): Completed at 19 locations. These precincts had previously been visited during the daytime portion of the Audit. The data collected on the Closing Poll Worksheet was insufficient to score. The majority of responses were N/A. Poll tapes were collected, however.

A few teams were not able to get to their closing poll in time to observe the closing procedures. In others, multiple precincts were observed in the closing because polling places for multiple precincts were located at one site. As it worked out, to complete the worksheet the pollwatcher could only observe one precinct. In these situations, poll tapes were collected but closing procedures were not completely observed and answers were marked N/A. In addition, the worksheet had flaws in the phrasing of some of the questions, which clouded interpretation of the answers.

Key data needs to be obtained to verify how accurately judges perform their roles of closing the polls, tallying the ballots, consolidating the results, transmitting to Election Central, and closing up the ESC for later return to the warehouse. Key seal information needs to be tracked that affirms judges sign the paper seals and records seal numbers on the ESC and the blue transfer bag.

Part of the closing procedures include placing the following into an unsealed black bag: special voted ballots (provisional, spoiled, returned absentee, etc.), poll documents (such as poll tapes, pay vouchers, and credentials), the ESC key**, and the bubble bag containing the electronic vote recorded on the memory pack and USB flash drive (the results cartridge).** This unsealed black bag is then transported to the receiving station and left there for CBE employees and contractors to process.[****] This action should be completed by two election judges together. The instructions in the Handbook are not clear about how these should be transported. It is clear there is no sealed chain of custody when transporting the black bag containing the electronic ballots and some of the paper ballots. This lack of security is magnified when the votes did not consolidate and transmit correctly from the poll.

During the Audit, one key question involves the seal applied on the transfer case (containing regular voted paper ballots) during the close of the polls. How is this seal tracked in the system?

During the 5% Audit, the seal number of the blue transfer case is recorded as it is broken and again when the case is re-sealed at the end of the audit. However, the seal number and the signed paper ballot seal are not checked to assure they are the same seals applied on Election Day by the election judges.

Procedural information on closing procedures needs further investigation.

[****] From the receiving station the memory devices are taken to the Pershing Street Warehouse. Later, they are transported back to the Washington Street Office. In the section "Additional Vulnerabilities" (p33-35) we discuss flaws in the security with storage of these memory devices.

DATA ANALYSIS

	Ward Audited	Totals	Percentage	
	The number of precincts Audited by 13 Procedures = total Items: Answers = Y, N, N/A	239 (x 13) = 3107 (Yes + No) Yes No N/A	Procedure Fail Rate % = ProcFR% ProcFR% = % of No's (Yes + No)	
1	2 Judges were present when the ESC opened and poll set up. (Red Error)	(225) 190 35 14	35 No's is 11% of 225	
2	Green Seal was closed on ESC. (Red Error)	(233) 174 59 6	59 No's is 25% of 233	
3	Judges have badges on. (Yellow Error)	(201) 177 24 38	24 No's is 12% of 201	
4	PPA has a badge on. (Yellow Error)	(191) 152 39 48	39 No's is 21% of 191	
5	Judges took their oath. (Red Error)	(212) 198 14 27	14 No's is 7% of 212	
6	Blue cones were at 100ft. (Red Error)	(217) 204 13 22	13 No's is 6% of 218	
7	T/S scroll is sealed. (Red Error)	(234) 218 16 5	16 No's is 7% of 234	
8	Red seal is on T/S Open/Close port (Red Error)	(230) 189 41 9	41 No's is 18% of 230	
9	T/S Cartridge Port is sealed. (Red Error)	(230) 210 20 9	20 No's is 9% of 230	
10	The Card Activator is sealed. (Red Error)	(227) 203 24 12	24 No's is 12% of 227	
11	The Ballot Box is sealed. (Red Error)	(236) 97 139 3	139 No's is 59% of 236	
12	The Ballot Scanner is locked and the Red Seal is on the back. (Red Error)	(215) 168 47 24	47 No's is 22% of 215	
13	The Early Voter labels are on the ballot applications at 6am. (Red Error)	(173) 150 23 66	23 No's is 14% of 173	
	Total = (Y+N) N/A not figured in FR % Yes No N/A	(2824) 2330 494 283 AvgProcFR=18%	(ProcFR%) = 228% No	
	ProcFR% is N% of (Y+N): WardProcFR averages the ProcFR% by Ward (See pg 23, part 6} The CityProcFR averages WardProcFR to provide a score across the city.	20% CityProcFR	AvgProcFR = 228% /by 13 228% /13 = 18% 18% Avg FR (of 13 Procedures)	
	239 Precincts were Audited Citywide Precinct Fail Rate: CityProcFR By Ward, precincts with error on one or more of the 11 red error procedures noted above.	90% Fail Rate 215 Precincts w/Red Errors 21 Precincts w/ No Errors 3 Precincts w/Yellow Errors	215 Red = 90% 21 Perfect = 9% 3 Yellow = 1% 90% = CityProcFR	

Data was collected at 239 precincts in 7 Wards. 13 areas were examined.

(N/A) responses, while they are recorded in the data, are not factored into the score. Each of the percentages calculated are based only on information recorded as a Yes or No. There are different totals for responses to the 13 items because, for varying reasons, the pollwatchers did not record a Yes or No response.

11 procedures are marked Red Error, 2 procedures are marked Yellow Error. Red error procedures are judged as having a potential impact on the vote. The two Yellow procedures relate to the badges of the Election Judges and PPA. Proper identification at the polls is an essential part of security. The identification errors are scored as cautionary.

Percentages are determined by:

1) **Citywide Procedure Fail Rate ("CityProcFR"): 90%.** 239 precincts were successfully audited. 215 of these (90%) failed in at least one of 11 Red error procedures, and were scored as Red. 3 precincts (1%) received a Yellow score related to badge issues, and 21 precincts (9%) achieved a perfect score by successfully following all 13 procedures.

   239 precincts across 7 wards
   90% = 215 precincts had one or more Red scores, plus some also had Yellow scores
   9% = 21 perfect scores – Error free
   1% = 3 had Yellow scores only (no Red scores)

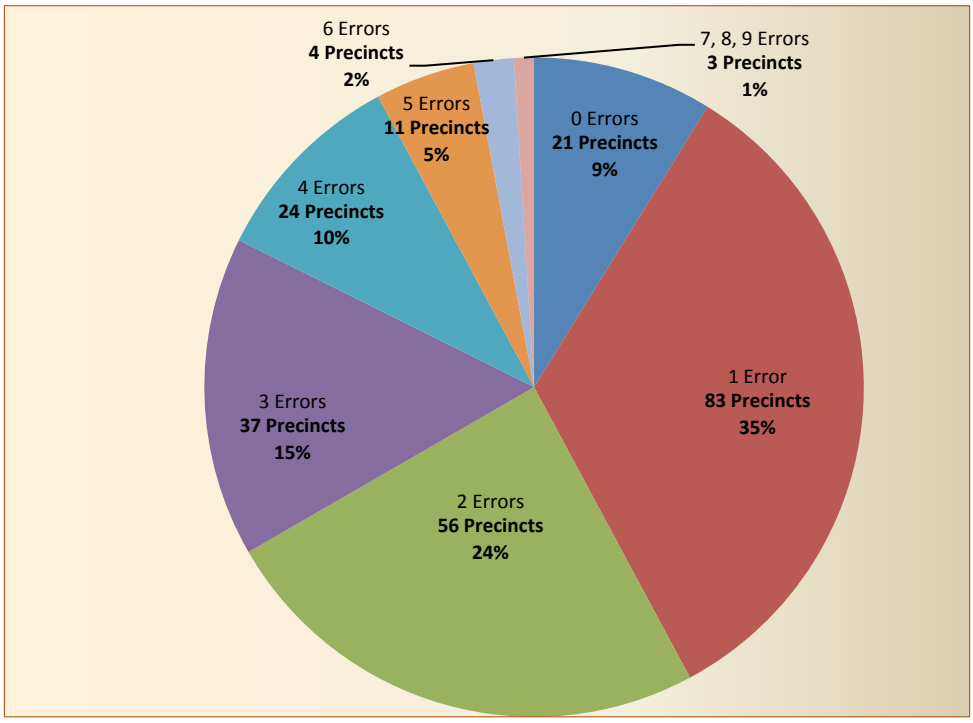
2) Multiple Procedural Errors – Per Precincts: The number of errors per precinct are totalled. These are then compiled into a graph to illustrate how many precincts have multiple errors. The numbers are stunning.

Number of Errors - and Number of Precincts with that error		**101% (Rounded %)**
0 Errors	**21 Precincts (21.51)**	**9%**
1 Error	**83 Precincts (83.65)**	**35%**
2 Errors	**56 Precincts (57.36)**	**24%**
3 Errors	**37 Precincts (35.85)**	**15%**
4 Errors	**24 Precincts (23.9)**	**10%**
5 Errors	**11 Precincts (11.95)**	**5%**
6 Errors	**4 Precincts (4.78)**	**2%**
7, 8, 9 Errors	**3 Precincts (2.39)**	**1%**

The CityProcFR of 90% indicates that 90% of the 239 precincts had a Red score or at least one critical procedural violation. When we look deeper into the actual errors, we find that out of 239 precincts, 57% (135) had 2 or more errors.

The graph on the next page provides a visual representation of the number of multiple procedural fails that each precinct had.

3) Procedural Errors Per Precinct: 239 Total Precincts



4) **Procedure Fail Rate Percentage ("ProcFR%")** is tallied by adding the (Yes) and (No) answer to each of the 13 questions and then determining what percentage of that total the (No) reflects. This percentage takes in consideration all answers to that item. It does not factor in N/A responses. Precinct by precinct breakdown on each procedure is included in the Summary Results by Ward that is attached in the Document portion of this report.

The ProcFR% tallies all of the precincts for a city-wide score on each procedure.
The ProcFR% provides insight, citywide, into what areas are in need of reinforcement. It also demonstrates critical lapses in security, allowing for further analysis.

Individual variances between procedures illustrate particular areas where the lapses are more prevalent. For instance, sealing of the ballot box failed 59% percent of the time; contrasted with the procedure for judges to take the Oath, which failed 7% of the time.

5) The **Average Proc Fail Rate Percentage ("AvgProcFR")** is 18%. The AvgProcFR is tallied averaging the ProcFR% for all 13 questions into one score.

On average, across all 13 items in the Audit, procedures were not followed 18% of the time. Statistically, city-wide, there is a 1 in 5 chance any given procedure will not be followed. This figure provides perspective on how well the CBE is doing in its role as administrators of the

critical election procedures on Election Day. On average per question, they fail on security procedures 18% of the time.

What is an acceptable score? Statistically there is no basis for comparison. Considered with the ProcFR% of 90%, and the fact that 57% of these precincts have multiple Red scores, 18% alerts the citizenry that security at the polls is inconsistent, often happenstance, and untraceable.

6) **Ward Average Procedure Fail Rate Percentage ("WardProcFR")** Precinct by precinct, the total answers for each ward are tallied and averaged. Again, only the Yes and No answers are figured in††††. This number identifies the average percentage of non-compliance ***per procedure*** in that ward. To understand the data consider that in Ward 46 (23% WardProcFR) there is a about a 1 in 4 chance that any given security procedure will be not be followed. In Ward 36 (WardProcFR 18%) the chances are closer to 1 in 5. This statistic is meant to provide prospective on the overall non-compliance with the any procedure in the individual wards.

   Grouped by ward, individual numbers are shown on the Summary Data Spreadsheet. (See Addendum: Summary Data p38)

   In order of non-compliance**:**
   Ward 20 – 27% non-compliance with security procedures
   Ward 46 – 23% non-compliance with security procedures
   Ward 45 – 21% non-compliance with security procedures
   Ward 38 - 16% non-compliance with security procedures
   Ward 36 – 18% non-compliance with security procedures
   Ward 41 – 16% non-compliance with security procedures
   Ward 43 - 15% non-compliance with security procedures

Data Review: Citywide

90% (215 out of 239) of the polling places had a Red score indicating non compliance in a critical location.

Ward 20 – 81% Precincts had Red Errors
Ward 36 – 91% Precincts had Red Errors
Ward 38 – 91% Precincts had Red Errors
Ward 41 - 83% Precincts had Red Errors
Ward 43 – 94% Precincts had Red Errors
Ward 45 – 90% Precincts had Red Errors
Ward 46 - 100% Precincts had Red Errors

Many precincts had multiple issues. The data is represented in individual spreadsheets broken down by wards into precincts on the Summary of Results by Ward sheets. Relevant comments on individual polling places are included. The Summary of Results by Ward records answers from the worksheets. Individual procedures are reviewed by ward and by procedure in the Data Summary.

†††† The reason only yes and no answers are used is because we cannot factor the N/A, meaning Non-Answer. This Audit assumes all items would not necessarily be answered. The auditors were instructed to do their best. While the N/A total is included, only the yes and no answers are factored into the results.

Data Summary - Of the 13 Procedures Studied: ProcFR%

59% Fail Rate: (139 out of 227) Ballot Box: Ballot boxes are required to be secured to the ballot scanner to assure that ballots are not added to the box except through the scanner. In part, this high failure rate is because of training. The election judges and PPAs are responsible for applying these seals, yet many did not know they existed. One PPA insisted she had just gone through training and had never been informed about these seals. Shockingly, in multiple instances, technicians and investigators from the Board arrived and left polling locations without checking that the ballot boxes were sealed.

Failure of this procedure means that in 59% of the polling places, the ballot box was unsealed for the election. When the scanner is lifted slightly from the box, the top is open and exposes the ballots below.

25% Fail Rate (59 out of 233): The Green ESC Seal: The seal on the ESC was missing in 59 instances. This is important because the seal should ensure that no one has tampered with the locked ESC. The key for the ESC is a generic key with multiple copies.‡‡‡‡ This seal is originally applied at the warehouse. It should be reapplied if the ESC is opened and left unattended both before and after the election.

There are many problems with this security system. In essence, the ESC is transported and then stored for a couple of weeks at the polling location. For example, it may be stored in a school gym. There is no basis in fact allowing the citizen to assume, nor the Board to assert, there is reliable security measures that assure the ESC is not tampered with after it is prepared for Election Day and sent to the polling place. There is none. The key is not specific to the unit. Once the unit is opened, multiple untraceable replacement seals are located in the supply box to reseal the ESC unit.

Keep in mind that the ESC contains unsealed (wrapped in plastic) ballots. It also contains the machines which are loaded with their memory devices. It contains untraceable seals for these machines. Seal issues on the machines further expose the vote to glaring security vulnerabilities.

There is no evidence to substantiate that a sealed ESC insures the ESC was not tampered with.

In the specific instance of the 25% failure to have seals, there is no chain of custody to discern at what stage in the process the seal was lost. Was it not properly placed on at the warehouse? Did the shipping process cause for it to be opened? Was it opened before Election Day at the polling place? And then there are the "who" related questions!

22% Fail Rate: (47 out of 215) Ballot Scanner Memory Pack Seal: The ballot scanner contains a memory pack in the back of the ballot scanner. This seal ensures that the correct memory pack is secured in the scanner. The memory pack contains the software that runs the machine and records the vote. The seal is put on at the warehouse. There is a locked door in the back of the scanner, potentially preventing easy access to the ballot scanner. The key to this door is a universal key. It is stored in the supply box, so anyone with access to the ESC has access to the memory device. Again, there are multiple red seals also placed in the supply box.

The importance of this lack of security is immeasurable when evaluating the integrity of the vote.

‡‡‡‡ The chain of custody on the keys is under further investigation

In one instance, a mature election judge team expressed dismay that the night before they had set up the voting booths up as a team and properly re-sealed the ESC, which still contained the election equipment. In the morning, they found a ballot scanner out on the table. No one knew how it got there, nor did they know who had access to the room after they left. As a team, they passionately confirmed it was not there the night before. Still, they had not reported the problem to Election Central and they were using the machine to record votes.

The lack of accountability and instructions on security procedures results in problems such as unsealed ballot scanners going unnoticed and/or unreported by our election judges.

We documented multiple instances where the technicians had been out to the poll to repair malfunctioning equipment and had not placed seals on the machines when they left.

Sometimes judges refused to open the back to allow inspection of the seal. These were recorded as a N/A.

21% Fail Rate (39 out of 191) PPA Badge: Did the PPA have their badge on? This is a Yellow item for scoring because the lack of ID does not jeopardize the vote. It is a security lapse that needs to be remedied.

Worthy to note: the PPAs, who are CBE Employees, were twice as likely to fail to put their badges on compared to election judges. The Audit found multiple instances of poorly trained PPAs.

The identification of people in the polling place is part of security. The current badges are adhesive badges which are hard to read and get lost because of simple problems such as hair getting caught in them.

Proper identification in the polling place is important and should be treated as such. It would be simple to provide plastic pin badges with blanks for the election team to personalize.

18% Fail Rate (41 out of 230): Seal issues on the Open/Close Port T/S EdgePlus. This machine is supposed to come with a yellow seal attached by CBE contractors at the warehouse and with a red seal stored inside the port door to be applied by the election judge when the polls are open, securing no one turns the machine off and on during voting.

Sometimes the negative score was because the machine arrived without the proper seals. Other times, the election team did not put the red seal on the machine. There was an instance where the machine came without the red seal, but it had the yellow seal attached. The election team did not think to get a red seal from the supply box. In other instances, technicians arrived to repair the T/S and did not re-apply seals.

What is the effect of this port being disturbed during the voting day? Why is there a seal there at all? Why is there a yellow seal? We have not found documentation to explain the potential consequences of failure in this procedure. What happens if the machine is turned off and on while in transport? Does that indicate a vulnerability to vote tampering? If so, why is this process not tracked? If the machine is turned on and off during the voting day, how does this impact the integrity of the process? Further answers are required.

Without tracing the chain of custody, we cannot discern the cause for this procedural failure. However, the CBE cannot blame poorly trained judges, as the PPA, technicians, and investigators also did not secure seal placement.

14% Fail Rate (23 out of 173): Early Voting stickers were not placed on ballot applications. EV stickers are included in the paperwork given to the key judge the day before the election. Election judges are to apply them to the ballot applications before the polls open. These labels contain Early Voting, Grace Period, or Absentee Voting information for voters.

This is a critical fail related to applying the EV stickers to the ballot applications to assure duplicate voting doesn't occur. 14% of the time, the stickers were either not applied at all or not applied completely. There were two reports of teams not having received stickers. One judge team did not know they existed.

The problem with recording Early Voting voters is that the voter books are manually updated. This leaves room for human error (accidentally or deliberately) to miss recording who voted, allowing for potential multiple voting. One reason for this failure is because the judges simply do not have the time to apply EV stickers during the hectic early morning set up. Training is also lacking. In the Handbook, pages 28 and 32 have a few paragraphs about the stickers. There is no check and balance to assure the judges have completed this task. Generally speaking, unless caught by a pollwatcher or investigator, the lapse will go unnoticed if they fail.

Audit investigators are unaware of procedures to check the incidences of multiple voting as a result of early, grace, and absentee voting. This would involve a fairly simple data check and should be routinely followed up on with election authorities. To prevent multiple voting, there should be a state-wide requirement for a reconciliation of voters who voted using one method or the other. This reconciliation would take place after the election, allowing law enforcement to become involved in instances where multiple voting is found. At this point, no evidence is collected and we do not know how often multiple voting occurs.

12% Fail Rate (24 out of 227): Seal on the Card Activator. In 24 instances, the card activators lacked a seal on the paper scroll. The paper record verifies the actions of the card activator. The paper scroll prints poll tapes for the morning and evening procedures and establishes a record of zero and a final vote count. The card activator controls electronic voting, consolidating of the vote, and transmitting the vote. This paper record, recorded on the scroll, is a security measure.

The seal procedure on the card activator is not mentioned in the Judges Handbook. The red seal is applied by contractors at the warehouse. This seal should be present 100% of the time. Unless the printer is not working, there is no reason for the seal to be broken. Because the tracking of the seal is nonexistent, we cannot discern the reason the seal is missing or the potential consequences such a security lapse indicates to the integrity of vote.

12% Fail Rate (24 out of 201): Judges' Badges. Generally speaking, election judges usually have their badges on. This is a Yellow area of non-compliance. If some judges had badges on and some did not, it was tagged as a (No) but recorded in the notes.

Proper identification is important to security and it is important for the voter, who relies on the election judges. Voters should be able to easily identify who the judge is and what party they represent.

11% Fail Rate (35 out of 225): Poll Set-up Procedures. In 45 instances, the polls were set up without compliance to the security process. When the poll was set up by at least 2 election judges, it was scored as in compliance even though all election judges were not present.

Multiple instances were documented where a single person was present when the ESC was opened. The set up of polling equipment requires for a Republican and Democrat Judge to be present. The ESC is frequently opened with only one person present, or without both political parties represented. It was not uncommon for the Precinct Captain, who is not an election judge, to open the ESC to allegedly make sure everything was ready for the vote.

Improper procedures for setting up polls are a security risk because it allows for untraceable access to the election equipment.

Polls are frequently set-up the night before. Polling place set-ups the night before the election are done to remove the stress of set-up in the early morning. Yet all too often it is done without the required team of election judges. Understandably, judges want to have the polling place arranged the night before, and the Handbook recommends the judges meet the day before to assure everything is present and working. The Handbook does not stress correct security procedures for setting up the polls as a team. These procedures do instruct the team to reseal the ESC until the following morning. The manual does not insist that a Democrat and Republican be present. Security procedures are not reinforced by requiring documentation of who set the polls up. Essentially, this information is not asked for, nor is it collected (Handbook pages 10-11).

We documented instances where only the booths (no voting materials) were set-up and others where the entire poll was set-up the night before. This becomes a compliance issue when voting materials are left unsecured when election judges are not present. Also, the ESC is frequently not resealed following its opening.

The reason for poll set-up security lapses is ease of access, lack of training, lack of accountability, and an old boy mentality – *"we have always done it this way."* There is a systemic practice of precinct captains opening the ESC to check it before the election.

Importantly, as already noted, a sealed ESC does not assure it was not tampered with. The seal is essentially window dressing.

Voter Privacy: The auditors documented numerous instances where the arrangement of the polls did not provide voter privacy. We noted this, but otherwise did not score it.

9% Fail Rate (20 out of 230): Seal missing on the T/S Cartridge Port. The T/S is a firmware shell driven by the software that is accessed through the cartridge ports. It records the vote totals onto the USB flash drive. The USB flash drive loads the ballots and records the vote. It is called a *results cartridge.*

The touch screen machine has a cartridge port where the results cartridge is inserted. In 9% of the instances, the seal securing this critical results cartridge was missing. **This seal is put on at the warehouse.** After the election, the judges break this seal and remove the USB flash drive. This results cartridge contains the record of the vote, specific to the precinct's ballot styles. There is no reason for it to be touched by anyone until after the election.

The causes for security lapse could be as innocent as an election judge opening the wrong compartment, to seals not being placed correctly on machines at the warehouse. Even if a seal is there, it does not mean the machine was not tampered with. Multiple untracked seals are stored in the supply box for easy replacement after tampering.

In 20 instances the T/S Cartridge Port was not sealed. We are not aware of any calls to Election Central about these seals despite these instructions:

> *Election Judge Handbook states: "Verify that a red seal is on the Cartridge Ports (results cartridge) door. If the seal is missing, immediately call ELECTION CENTRAL at 312-269-7870* (pg 22).

The results cartridge drives the T/S machine. Tampering with results cartridges of the exact same T/S model was recorded in 2009 in the Philippines, where results cartridges were found in the garbage dumpster with recorded votes on them. A lack of security on the results cartridge assures there is immeasurable vulnerability to vote manipulation.

Note: Even though the T/S machine is broken, the chain of custody of the results cartridge should be similar to the ballots. This is not the case. Seals are routinely not replaced or ignored altogether.

It is impossible to state that a sealed T/S cartridge port provides security that the results cartridge was not tampered with. There is no evidence recording the chain of custody on the seal securing the port. Because the seal numbers are not recorded and cross-checked, election judges cannot reliably detect tampering which effectively is a 100% fail rate.

7% Fail Rate (16 out of 234): The Touch-Screen voter verification's paper scroll. The seal on the paper scroll is essential as a record of the ballot. It can be legally argued that it requires a seal. The T/S Scroll was not secured with a seal 7% of the time. This scroll is the printed record of the vote and is considered a backup for the results cartridge. The seal is secured to the machine by the CBE contractors at the warehouse.

The printing mechanism that prints the scroll frequently breaks. When it does, training instructions and follow-up do not assure a seal is placed on the machine when it is repaired. It is not credible to say that the error is caused by the election judges. Technicians and PPAs repairing the scroll are documented as not replacing the seal.

In addition, the scroll container is attached to the T/S machine as a separate numbered part. The part number should be the same as the machine's SN number. This is not checked. This is important because the scroll is the paper record of the vote. The chain of custody on the scroll recording the vote should be similar as the paper ballot. The scroll can be changed without touching the seal simply by switching the parts.

Voters are assured that the paper record provides security that the vote is recorded correctly. In fact, this is a smoke and mirrors illusion. Yes, a paper record does help, but without access to the software, proper auditing techniques for the paper scroll[§§§§], and to a chain of custody on the parts

[§§§§] We do not audit Early Voting which is all done on the T/S. In April 2011, the CBE has admitted to the Audit investigators that they do not have techniques available to audit Early Voting and the ISBE has not provided them with techniques. Further report is forthcoming.

and seal, this record of the vote is vulnerable to manipulation. This security vulnerability is magnified when there are security lapses with the results cartridges.

7% Fail Rate (14 out of 212): Taking the Election Judge Oath. In at least 7% of the instances, the election judges did not take their oath. This is critical because every act the election judge takes in their official role is potentially nullified if they are not under oath.

The oath is taken by reading a card. It is included in the handbook as an important procedure. In one instance an auditor noted that an experienced team did not take their oath. Apparently, they did not see the immediate importance for it. Investigators are not aware of a back-up procedure to assure the oath has been taken or to follow up when it was not.

6% Fail Rate (13 out of 218): Marking of 100ft with the blue cones. The blue no-electioneering cones were not correctly placed outside. This is considered a critical area because of the importance of allowing voters to vote unmolested by electioneering conducted too close to the polling place.

Election judges tend to be aware of the placement of the cones because without them, voters will complain when electioneering does take place. Some teams did not have the cones in their ESC. Sometimes the cones had been moved and sometimes they were improperly placed. Besides the election judges, the PPAs should assure that signage and cones are placed correctly. This needs to be re-checked intermittently throughout the day.

We also noted, but did not score, multiple instances where the signage was incorrect.

Summary of Results by Ward: More in-depth data analysis is available in the Summary of Results. The raw data was consolidated into summary sheets for each ward and are included in this report. This Summary of Results by Ward provides a visual overview of the results of the scores. They are sorted based on the number of "Red" and then "Yellow" scores. The precincts with the highest number of Red scores are sorted top to bottom.

General Limitations and Assumptions:

This study represents a surprise audit of 239 precincts on Election Day, April 5, 2011. We did not look for fraud, nor did we identify the presence or lack of fraud. Our study is on the procedures used to keep tampering or fraud from occurring, or to alert us that it did happen.

It is impossible to assess fraud caused by a lack of procedures because data is not collected.

DISCUSSION

Summary of Main Findings:
One of the primary responsibilities of government is to assure the accuracy of the vote. There is a tendency of the citizenry to trust this is being done. Equally so, there is a frustration among the electorate that feels the integrity of the vote is so corrupted, why bother to vote. This is especially true in Illinois, which has a globally infamous reputation for holding corrupt elections.

With the evolution of technology, balloting systems have been undergoing rapid change. Since 2000, the rise in electronic voting has substantially changed how Americans vote. In addition, changes to Absentee Voting and Early Voting have impacted how we cast, record, and tally the vote. These changes continue, frequently untested by objective analysis about their impact to the integrity of the vote. We are in a place of rapid change in voting methodologies. This impacts legislation; especially in Illinois, which is infamous for its patchwork approach to election legislation and the related case law.

There are several trends in elections which are noteworthy of investigation, but this study primarily addresses the veil that is placed on equipment to provide an appearance of security. A lack of transparency of the voting process is inherent in electronic voting. Voters are told that there is enhanced accountability and security in recording the vote electronically, but don't know how or where to determine if there is such security.

Our study did not look for fraud. We studied how adequate the system is in preventing and/or catching fraud through maintenance of procedures designed to assure the system's security and thus, the integrity of the vote.

Our findings prove that the Chicago Board of Elections fails to maintain security sufficient to assure that each vote is accurately cast and counted. Generally the system relies on seals as measures of security. Seal use protocols are crucial to understanding the use of seals on election equipment and supplies.

Seal use Protocol: Election authorities need to have secure, consistent and verifiable seal use protocols.

"Seal use protocols are the formal and informal procedures for choosing, procuring, transporting, storing, securing, assigning, installing, inspecting, removing, and destroying seals. Other components of a seal use protocol include procedures for securely keeping track of seal serial numbers, and the training provided to seal installers and inspectors. The procedures for how to inspect the object or container onto which seals are applied is another aspect of a seal use protocol. Seals and a tamper-detection program are no better than the seal use protocols that are in place." [Dr. Roger Johnston, Argonne Labs 2010, *****¶24]

***** JOHNSTON, R. G. 2010. Insecurity of New Jersey's seal protocols for voting machines. http://www.cs.princeton.edu/~appel/voting/Johnston-AnalysisOfNJSeals.pdf

Dr. Johnston discusses vital considerations in choosing seals for election equipment. "The physical design of seals used for this purpose need to be easy to remove, and should provide evidence when they are removed or tampered with. These seals need to be serial-numbered so that when new seals are applied, the numbers are recorded as part of the trail of evidence of security." *(Personal communication with Roger Johnston, Vulnerability Assessment Team, Argonne National Laboratory)*

Standard protocols for seal security include a number of steps to be effective.

- Organized records must be kept relating to seal numbers and to when the seal was put on and removed. These records need to be secured.
- Quality Assurance procedures need to be followed that include inspection of the seals and the documents supporting the application of the seals.
- Seal users need to be trained on the proper use of seals. This includes how to apply seals and how to detect obvious and subtle signs of tampering.

This study provides indisputable evidence there are few controls providing accountability that security procedures are followed. Most of the security related procedures in place present a mere veneer of security, when in truth they are not tracked, maintained, or reinforced.

When seal protocol is accounted for, this study finds there is a 100% fail rate. The seal use protocols used by the Chicago Board of Elections are completely inadequate in detecting tampering.

Importance of Quality Assurance: Without tracking, we frequently don't get to "If" it was tampered with. Forensically, it becomes difficult to reconstruct what is lost. Statistically, we cannot assess vulnerabilities when there is no data collected by the election authorities. To establish a base line for assessment requires extraordinary means such as this Audit represents. Otherwise, the data is not collected!

The CBE's management of seals is entirely ineffective, which causes the seals to create a mere veneer of security. Generally, election judges and PPAs do not know the purpose of the seals and no one records their numbers. Moreover, there are uncontrolled supplies in the ESC, allowing seals to be broken and reinstalled without raising any alerts of tampering to responsible parties.

The vote is vulnerable at any point where the process is not transparent. We lose control over the process when we lose sight of the chain of custody. An offender finds places to compromise the vote according to their access point to do so. There are multiple points of access: warehouse, shipping, inventory, polling place interference, computer rooms, mechanical and electrical interference, etc. Assuring security becomes especially problematic with varied voting options such as is presented in Election Day and Early Voting.

The results from this audit are stunning! Were they predictable? In the complicated polling place, surely there is always room for variations and mistakes! The task of administering elections is not a small one. Variations in procedural compliance do not necessarily represent evidence of fraud. Indeed, most of our election authorities are elected and the County Clerks are accountable to the people.

This does not mean the voting system is secure nor, is it an excuse for a lack of security!

The problem remains: how do we hold our government accountable to conduct secure, fair, and honest elections? The only way to assure an accurate vote is to have security oversight. This oversight must be 100% transparent and accessible to voters and to candidates. It must include seal use protocols. There must be a quality assurance program employed to hold election authorities accountable for standards that are recognized in the industry as providing a reasonable measure of security over the process of casting and counting the American vote.

The citizens must also recognize the importance of their involvement in the process of casting and counting the vote. There is an element of citizen involvement that is part of the oversight of elections and thus part of election security. For the most part, to be involved, you must be a registered voter. Pollwatching programs provide important access and as pollwatchers, voters have access to view all election equipment and materials. Election judge programs are another avenue for voter involvement. Individuals and groups (you don't have to be registered to vote) have the right to FOIA documents and to attend public demonstrations of the equipment.

Citizens cannot assume elected officials have the integrity of the vote secured.
This Audit proves they don't!

ADDITIONAL VULNERABILITIES

Our investigations have uncovered the following additional vulnerabilities:

Stacks of open ballots in the warehouse:


Unprotected ballots photographed during the 5% audit and the open doorway 65ft away.

Unprotected ballots photographed at the Pershing Street Warehouse; around the corner from these ballots is an open doorway to the shipping dock and street ally which employees routinely use without visible security present. Audit investigators were repeatedly denied access to this doorway's security. These ballots were stored just feet away from the 5% State-wide audit that was taking place in the same area.

Lack of Security around Memory Devices: Note in the picture of the open door (taken during a different visit to the warehouse), the unsealed cardboard boxes to the left (close-up below).

INCREDIBLY, each one of these boxes contains ALL of the electronic memory devices for one of the City's wards. These memory devices (USB flash drives called results cartridges and the ballot scanner's memory pack) control the election machines. These boxes were left unsealed next to the open doorway while warehouse contractors were testing the machines and while dock workers and truckers were busy moving election equipment. The unsealed boxes were waiting for shipment back to Washington Street and were stored in the location in the picture for weeks.


Close-up - These are the boxes waiting for shipment back to Washington Street and are left without security for extended periods of time next to the open door leading to a shipping dock. The box on the left is the box being used for Pre-LAT testing of Ward 11 at the same location. All memory devices are shipped and stored in this box.

Contractors and Employees: The Chicago Board uses both contractors and employees to supervise and operate all aspects of the election process. Although not included in this report, our investigations have proven that the Chicago Board of Elections is not in compliance with I-9 regulations which identify the right for the individual to work in the USA. Evidence conclusively proves the Board approves Forms I-9 where the employee did not check their work status. Further investigation is underway.

As the picture above proves, contractors have access to the most vulnerable parts used in voting. Yet who are they? The CBE does not secure they are legally entitled to work and **routinely** looks the other way when they do not identify their right to work on the I-9.

This security lapse is critical. Who is working as PPAs, contractors at the warehouse, and in other critical roles? What background check is completed? Who is responsible for screening procedures? What are these procedures? Who checks up?

Importantly: Early Voting sites in Chicago use employees in place of election judges. These employees are not required to be citizens. Defend the Vote has documented the re-occurring procedure of Chicago Early Voting sites being operated by non-citizens. In addition, we document the CBE has workers running Early Voting with Forms I-9 on record that are filled out without the declaration (under perjury) of the right to work status of these individuals running the Early Voting polling locations. This means we don't have any declaration or confirming record that they are legally eligible to work!

Equipment Failures: Election Code requires a state-wide 5% audit of all election equipment and results. In the April election, investigators observed that there was a precinct with 34 ballots; 22:12 votes cast by paper ballot for the Alderman's race in the 24th Ward, 16th Precinct. This precinct was randomly chosen as part of the 5% audit which Defend the Vote investigators attended. During the 5% audit, the CBE contractors re-scanned the ballots (into a new ballot scanner and memory pack) and the votes recorded 21:13. Visual counting assured the results were 22:12. Multiple attempts to get the same results from the ballot scanner were futile. After about 2 hours, the auditors (CBE contractors) discerned they could not figure out what the error was and sent in their results for that precinct, noting but not resolving the vote discrepancy. Multiple CBE supervisors were involved in this situation.

CBE supervisors reported that there was no paper trail following this audit result. No repair record or trouble shooting report would be filed. Essentially, there was no way for our team to track the resolution of this problem in the system. No further resolution was forthcoming with the CBE.

This is a critical flaw in testing procedures. The lack of accountability when error is found secures that it cannot be investigated to discern the potential reasons for and implications to the vote this flaw causes. How can we assess the flaw when it is not recorded? **Simply, by maintaining no tracking procedures, the issue remains incidental and cannot be used to discern flaws in the voting system that the 5% State-wide audit is designed to catch.**

Absentee Voting and Early Voting: Defend the Vote has documented substantial irregularities in Early Voting and Absentee Voting procedures. A follow-up report on this topic will be forthcoming.

Cellular Technology: The CBE has a policy restricting cellular technology around the voting equipment at the Washington Street facility and at the Pershing Street warehouse. They have only

stated that it could interfere with the operation of the equipment. How is interference caused, what can it do, and what measures are in place to prevent it and/or catch it should it occur? **Importantly, why is such equipment used in polling places where cellular phones are used by election personnel?**

Note: The card activators transmit election results by cellular technology. There is no notation in the Handbook restricting cell phones at the polling place.

Software: The fact that we have no public or private records proving the veracity or not of software running our voting equipment demonstrates just how vulnerable we are to vote manipulation. Security checks on contractors who work for the Board programming the software is problematic and must be investigated**.**

There are multiple pieces of equipment involved in elections, each with firmware and software that is not accessible to public review. Some of this equipment has been investigated, but is not mentioned in this report. With a 90% failure rate on security procedures, we prove how closely the CBE monitors security procedures. The current system relies on proof of fraud to inspire corrective procedures and establishes practices that make it impossible to prove if there was tampering with the vote.

There is no security check accessible to the public verifying the accuracy of the software recording the vote. The software code must be transparent to provide any hope for security of the vote. Yet, access is denied by vendor contract, lack of procedures, and with other security-related justifications.

CORRECTIVE ACTIONS AND NEXT STEPS

There are several next steps that we recommend that will solve **some** of the security issues.

1) Election judges should be given a check list that must be completed and signed off by all judges at 6:00am. This includes checking and recording seal numbers. The check list will remind the election team of each step and hold them responsible for compliance as a team. When equipment comes without a seal or with a damaged seal, the election judges should note that for **immediate** follow up investigation.

2) All seal numbers applied at the Pershing Street Warehouse should be recorded on a triplicate-duplicate form. One copy is for warehouse records, one for the CBE, and the other goes to the election judges. Election judges check these seal numbers to confirm they are the same. Currently, the CBE uses forms with multiple duplicates for other aspects of record keeping at the warehouse. Adjusting the form is all that is required to fix this aspect of the problem.

3) Seals numbers placed on equipment and on the blue transfer case by elections judges should be cross-checked at the Receiving Stations and for the 5% Audit.

4) All used and unused seals should be returned to the warehouse in a separate envelope in the blue transfer case and stored along with the ballots until the ballots are destroyed. Confirming the chain of custody on the seals and the recorded numbers should be part of each step of the process and part of the 5% Audit.

5) A different color must be used for replacement seals in the ESC for use at the polling place. The use of these seals should be recorded in the judge's paperwork. Different seals (in appearance) provide a way to replace seals without compromising the integrity of the seals. This procedure must be accompanied by a documentation sheet that records when the seal is changed, by whom, and the reason for the change.

6) The Handbook should be changed to include information on the seals and their importance. There should be a section on security and there should be a FAQ that specifically pertains to seal issues. Seal training should be required for all election judges and PPAs.

7) CBE technicians and PPAs must replace seals when they repair equipment and include the new seal numbers in the judge's paperwork before the repair is considered completed. The recording of the change should be made in election judge paper work as described in #2.

8) When the CBE mails pay checks to the election judges, they should include blank polling place evaluation forms to allow for continuing opportunities to election judges to provide feedback on the polling place experience. Election judges need to have the opportunity to report polling place concerns after the election. This would help catch reoccurring problems and provide the election judges with an opportunity to confidentially report concerns.

9) Election judges and PPAs are given pinned badges. The paper adhesive ones do not last through the day and are hard to read.

IMPLICATIONS OF THE STUDY

Implications / Significance of the Study

This study should be published across the state and nationwide. Voters should understand that the Chicago Board of Elections issues reported here are not exceptions to the rule, but are the rule. 239 out of 700 precincts is a significant sampling providing indisputable evidence that, left on their own, election authorities do not necessarily provide adequate security.

Nationally, until we begin to measure security of voting procedures, the implication to the vote is literally immeasurable! Local groups should feel empowered by this result to audit election practices in their communities.

Conversations should be immediately initiated with election authorities across the state, seeking voluntary inclusion of audit procedures to assure the polling place maintains security.

The Illinois State Board of Elections should receive a copy of this report with a request to respond to its results. The Board is responsible under law to report to the State Legislature on election matters, and this report should be the basis of such a communication.

The State Legislature should be contacted with the purpose of launching a statewide investigation.

Building upon the depth of experience gained in conducting the Audit, Defend the Vote will now seek to create a citizen advocacy mechanism to audit the vote and advance ballot integrity across Illinois. Our next step is to perform a vulnerability assessment and security audit across the entire state of Illinois for the upcoming 2012 elections. We ask all interested parties to join our ongoing and upcoming efforts.

ACKNOWLEDGEMENTS

Funding Bodies: Champion News and Jack Roeser

Investigators: Defend the Vote

Auditors: Thank you to the many auditors who worked to make the audit happen!

Major Collaborator: Jack Roeser, Publisher of Champion News, and Steve Boulton General Counsel of the Chicago GOP.

Advice and Sharing of Expertise: Jack Roeser, Steve Boulton, Peter Bella, Carl Segvich, Jim Fuchs, Jim Leahy, and a special thank you to the auditors who came from various Tea Party Groups.

Roger G. Johnston, Ph.D., CPP, head of the Vulnerability Assessment Team (VAT) at Argonne National Laboratory, was invaluable for his advice and expertise on seal protocols.

Thank you to the peer reviewers with the Journal of Physical Security who helped to make this report stronger and who approved it for publication.

REFERENCES

The Judge of Election Handbook for the Feb. 22, 2011 Municipal General Election and the April 5, 2011 Supplementary (Run-Off) by the Chicago Board of Elections.

APPENDICES

SUMMARY DATA WORKSHEET

SUMMARY OF RESULTS- WARD 20

SUMMARY OF RESULTS- WARD 36

SUMMARY OF RESULTS- WARD 38

SUMMARY OF RESULTS- WARD 41

SUMMARY OF RESULTS- WARD 43

SUMMARY OF RESULTS- WARD 46

SUMMARY OF RESULTS- WARD 48

Summary Data Chart for the April 5th 2011 Chicago Audit

	Ward Audited	20	36	38	41	43	45	46	Totals	Percentage
	The number of precincts audited by 13 ques = total Items: Answers = Y, N, N/A	9 (x 13) = 117	42 (x 13) = 546	52 (x 13) = 676	33 (x 13) = 429	45 (x 13) = 585	38 (x 13) = 494	20 (x 13) = 260	239 (x 13) = 3107	Procedure Fail Rate % + ProcFR%
		Yes - No - N/A	Yes - No - N/A	Yes - No - N/A	Yes - No - N/A	Yes - No - N/A	Yes - No - N/A	Yes - No - N/A	(Yes + No) Yes - No - N/A	FR = % of No's (Yes + No)
1	2 Judges present when the ESC opened and poll set up. (Red Error)	6 3 1	29 8 5	39 12 1	26 6 1	42 0 3	28 6 4	20 0 0	(225) 190 35 14	35 No's is 11% of 225
2	Green Seal closed on ESC. (Red Error)	4 5 0	35 6 1	38 12 2	26 7 0	30 15 0	25 12 1	16 2 2	(233) 174 59 6	59 No's is 25% of 233
3	Judges have badges on. (Yellow Error)	4 4 1	32 4 6	42 0 10	25 4 4	36 3 6	29 3 6	9 6 5	(201) 177 24 38	24 No's is 12% of 201
4	PPA have badge on. (Yellow Error)	7 2 0	24 8 10	29 9 14	27 4 2	32 8 5	25 6 7	8 2 10	(191) 152 39 48	39 No's is 21% of 191
5	Judges took their oath. (Red Error)	7 0 2	31 0 11	48 2 2	29 2 2	41 0 4	29 5 4	13 5 2	(212) 198 14 27	14 No's is 7% of 212
6	Blue cones were at 100ft. (Red Error)	6 3 0	36 2 4	43 4 5	32 1 0	42 0 3	34 3 1	11 0 9	(217) 204 13 22	13 No's is 6% of 218
7	T/S scroll is sealed. (Red Error)	8 1 0	38 4 0	49 3 0	30 3 0	43 0 2	34 4 0	16 1 3	(234) 218 16 5	16 No's is 7% of 234
8	Red seal is on T/S Open/Close port (Red Error)	5 2 2	32 10 0	46 6 0	29 4 0	38 7 0	29 7 2	10 5 5	(230) 189 41 9	41 No's is 18% of 230
9	T/S Cartridge Port is sealed. (Red Error)	5 2 2	39 2 1	48 4 0	31 2 0	41 4 0	32 3 3	14 3 3	(230) 210 20 9	20 No's is 9% of 230
#	The Card Activator is sealed. (Red Error)	6 0 3	38 4 0	46 6 0	30 3 0	42 3 0	25 7 6	16 1 3	(227) 203 24 12	24 No's is 12% of 227
#	The Ballot Box is sealed. (Red Error)	4 3 2	16 26 0	33 19 0	16 17 0	12 33 0	13 25 0	3 16 1	(236) 97 139 3	139 No's is 59% of 236
#	Ballot Scanner is locked and the Red Seal is on the back. (Red Error)	5 1 3	24 13 5	30 19 3	30 3 0	34 4 7	31 4 3	14 3 3	(215) 168 47 24	47 No's is 22% of 215
#	Early Voter labels are on the ballot applications at 6am. (Red Error)	5 0 4	23 2 17	35 2 15	23 9 1	37 1 7	15 7 16	12 2 6	(173) 150 23 66	23 No's is 14% of 173
	Total = (Y+N) N/A not figured in FR % Yes No N/A	(98) 72 26 19	(486) 397 88 60	(624) 526 98 52	(419) 354 65 10	(548) 470 78 37	(441) 349 92 53	(208) 162 46 52	(2824) 2330 494 283 (484=18% Avg FR)	(ProcFR%)+ = 228% No's.
	ProcFR% is N% of (Y+N): On 13 ques, Avg FR of precs per Ward	27% Total 98: 26 No = 27% of 9 prec	18% Total 486: 88 No = 19% of 42 Prec	16% Total 624: 98 No = 16% of 52 Prec	16% Total 419: 65 No= 16% of 33 Prec	15% Total 548: 78 No= 15% of 45 Prec	21% Total 441: 92 No= 21% of 38 Prec	23% Total 208: 46 No= 23% of 20 Prec	20% - Avg FR per procedural item, city wide.	ProcFR Avg 18% 228% /13 = 18% AvgProcFR-18%
	239 Precincts audited CityProcFR By Ward, precincts results are tallied.	81% Red Errors 2 Perfect Precincts 0 Prec Yel Errors 7 Prec-Red Errors	91% Red Errors 2 Perfect Precincts 2 Prec-Yel Errors 38 Prec-Red Errors	91% Red Errors 5 Perfect Precincts 0 Prec-Yel Errors 47 Prec-Red Errors	83% Red Errors 5 Perfect Precincts 1 Prec -Yel Errors 27 Prec-Red Error	94% Red Errors 3 Perfect Precincts 0 Prec-Yel Errors 42 Prec-Red Errors	90% Red Errors 4 Perfect Precincts 0 Prec-Yel Errors 34 Prec-Red Errors	100% Red Errors 0 Perfect Precinct 0 Prec-Yel Errors 20 Prec-Red Error	90% of 239 Failed 215 with Red Errors 21 Perfect Precinct 3 Prec w/Yel Errors	90% CityPrecFR 215 Red = 90% 21 Perfect = 9% 3 Yellow = 1%

Summary of Results for Ward 20

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
20	9	MA Only	No	No	No	N/A	No	No	No	No	N/A	No	N/A	N/A	Wasn't able to complete inspection of election equipment due to Election Judge refusing access
20	7	BB Only	No	No	No PPA	N/A	No	Yes	No	No	N/A	N/A	N/A	N/A	Wasn't able to complete inspection of election equipment due to Election Judge refusing access
20	3	All - PPA set up	Yes	No	Yes	Yes	No	Yes	N/A	N/A	Yes	No	Yes N/A	N/A	Ballot counter was locked no access didn't let me proceed
20	2	SC Only	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	N/A
20	2	PPA ALL	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - No	Yes	N/A
20	2	All	No	No	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A	Didn't let me proceed
20	1	All - PPA	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A
20	0	All + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - N/A	Yes	Ballot boxes locked
20	0	All and PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	

Summary of Results for Ward 36

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
36	5	All	Yes	N/A	Yes	Yes	Yes	No	No	No	Yes	No	Yes- ?	No	No Label 3
36	5	S alone	No	Yes	Yes	N/A	Yes	Yes	Yel Seal missing	N/A	Yes	No	No	N/A	N/A
36	5	N alone	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	No	Yes -No	Yes	Broken seal reported to Tech
36	5	1 or 2 Judges	No	No	Yes	N/A	Yes	Yes	Yes	Yes	Yes	No	No	N/A	N/A
36	4	N/A	No seal	Yes	Yes	N/A	Yes	Yes	Yel Seal missing	Yes	Yes	No	No	N/A	N/A
36	3	A. alone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes -No	Yes	N/A
36	3	2 or 3 Judges	No	Yes	N/A	N/A	Yes	Yes	Yel Seal missing	Yes	Yes	No	N/A	N/A	Ballot Scanner Key is kept in EJ's pocket
36	3	All	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes -No	Yes	N/A
36	3	All	No	Yes	N/A	N/A	Yes	Yes	Yel Seal missing	Yes	N/A	No	Yes	Yes	N/A
36	3	S. alone	No	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes N/A	Yes	Green Seal was removed the night before, and not replaced. S. set the polls up.
36	3	All -	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	No	Yes	N/A	N/A
36	3	3 Judges	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	No	N/A	Yes	No cones when I arrived, in place when I left
36	3	DA alone	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	N/A
36	3	All	Yes	Not all	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	Yes	Did not observe seal on ballot scanner.

Summary of Results for Ward 36

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
36	2	All	Yes	Yes	Yes	Yes	Yes	Yes	Yellow	Yes	Yes	No	Yes	Yes	N/A
36	2	J. alone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes -No	Yes	N/A
36	2	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	
36	2	C. alone	Yes	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes	Yes	Yes -No	Yes	N/A
36	2	S. alone	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes- No	Yes	One Judge set the polls up alone and self reported the green seal was present.
36	2	N/A	N/A	Yes	N/A	N/A	Yes	Yes	Yel Seal missing	Yes	Yes	No	Yes - N/A	Yes	There was no yellow seal, but a red seal was put on. - Did not see locks on ballot machine -
36	2	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	N/A	Refused access to Ballot Box Back
36	2	All	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes - ?	Yes	N/A
36	2	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes -No	N/A	N/A
36	2	S. alone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes -No	Yes	N/A
36	2	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No Labels	Labels were not delivered.
36	2	3 Judges	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes -No	Yes	N/A
36	2	All	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	N/A	Missing Republican judge
36	2	All	Yes	Not all	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No - yes	Yes	Not all judges wore their badges
36	1	All -	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Seal on card activator broken on table
36	1	All	Yes	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes	No	Yes - Yes	N/A	N/A
36	1	3 out of 5	Yes	Yes	N/A	Yes	N/A	Yes	Yes	Yes	Damaged Seal	Yes	Yes -?	Yes	N/A

Summary of Results for Ward 36

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
36	1	2 out of 3	Yes	Yes	N/A	Yes	N/A	Yes	Yes	Yes	Yes	No	Yes	N/A	N/A
36	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	N/A	Refuse
36	1	All	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	N/A	N/A
36	1	All	Yes	N/A	N/A	N/A	Yes	Yes	Yel Seal missing	Yes	Yes	Yes	N/A	Yes	N/A
36	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - ?	N/A	Refused to show back of ballot counting machine
36	1	All	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	No	N/A	N/A	N/A
36	1	All	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A	N/A
36	1	All	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A	N/A
36	0	All	Yes	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes - Yes	N/A	Refused to show back of ballot machine
36	0	A & F (2)	Yes	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes	
36	0	All	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A

Summary of Results for Ward 38

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's ?	Notes
38	6	V.	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes -No	Yes	N/A
38	6	B.	No	Yes	No	Yes	Yes	No	Yes - No	Yes	Yes	Yes	Yes -No	Yes	N/A
38	6	C and J	No	Yes	No	No	N/A	Yes	Yes	Yes- damaged	Yes	No	Yes - Yes	N/A	N/A - Key was discarded and they had to fish it from the trash
38	5	J.	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes -No	No	N/A
38	5	CK	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes -No	Yes	N/A
38	5	All	No	Yes	No	Yes	Yes	No	Yes	Yes	Yes	No	Yes - No	N/A	N/A
38	5	EG, CG	Yes	Yes	N/A	Yes	No	Yes	open yellow	Yes	Yes	N o	Yes -No	Yes	PPA not around and no one knew her name
38	4	B	Yes	Yes	N/A	Yes	Yes	Yes	No	Yes	Yes	No	Yes -No	Yes	Seal was laying on top of the machine- opened
38	4	CK	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No - No	Yes	Red O/C seal was unused, laying in the case.
38	4	P & M	No	Yes	N/A	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes -No	Yes	The PPA was not around, EJ's complained. They did not have PPA's name either.
38	4	BJ	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes	No	No	Yes -No	Yes	No PPA showed up
38	4	All	No	N/A	Yes	Yes	No	Yes	Yes	Yes	No	No	Yes - N/A	N/A	No cones in the ESC . The ESC was locked but did not have a seal.
38	4	All	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	Yes	When EJ showed the seal, it was so flimsy it broke - No Extra Names List.
38	3	S	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes -No	Yes	N/A
38	3	All	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes -No	Yes	N/A

Summary of Results for Ward 38

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's ?	Notes
38	3	All	Yes	N/A	N/A	Yes	Yes	Open seal	Yes	Yes	No	No	N/A	Yes	PPA was sleeping - EJ's put up stands last night as a team. Card Activator seal was missing, seal on Scroll for T/S open.
38	3	GF	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes -No	Yes	N/A
38	3	All	Yes unlocked	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	Yes	N/A
38	3	N/A	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes - Yes	Yes	Seal added at PW request
38	3	All	Yes	Yes	No	Yes	Yes	Yes	Yes	Damaged Seal	Yes	No	Yes - Yes	Yes	N/A
38	2	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes - Yes	Yes	Placed seal on at PW request. Also, M.was concerned that the PPA was not doing anything .
38	2	All	N/A	N/A	N/A	N/A	N/A	Yes	No - EJ failure	Yes	Yes	No	N/A	N/A	EJ's mishandled putting the open/close seal on
38	2	All	Yes	Yes	N/A	Yes	No	Yes	Yes	Yes	Yes	No	Yes - Yes	N/A	N/A
38	2	W & J	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes -No	Yes	N/A
38	1	All	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No One	Yes - Yes	N/A	Ballot box was replaced.
38	1	All	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No - No	Yes	N/A
38	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - ?	N/A	N/A
38	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - ?	N/A	Refused to open Ballot Scanner
38	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No - Yes	Yes	N/A
38	1	All	Yes	N/A	N/A	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes -No	Yes	N/A
38	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	Yes	Ballot box seals off until requested. Said they couldn't find the seals.

Summary of Results for Ward 38

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's ?	Notes
38	1	All	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes -	Yes - Yes	Yes	N/A
38	1	All	Yes	N/A	Yes	N/A	N/A	Yes	Yes	Yes	Yes	No	N/A	N/A	N/A
38	1	All	Yes	N/A	N/A	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - ?	N/A	Refused to open the back
38	1	All	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes -N/A	Yes	N/A
38	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - ?	Yes	No seals for the ballot box in the ESC - Judges refuse to open back of the ballot scanner.
38	1	3 judges	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes N/A	N/A	refused to place seals on Ballot Boxes
38	1	All	Yes	Yes	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes	No - No	Yes	N/A
38	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No - No	Yes	Voting booth open to judges (see paper for picture)
38	1	All	Yes	N/A	N/A	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes - Yes	Yes	N/A
38	1	MK	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - N/A	Yes	N/A
38	1	DD	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - Yes	Yes	N/A
38	1	PPA + 2 judges	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - Yes	No	EJ's report they did not receive stickers for early voting/absentee. EJs explained they have been checking list as votes come in.Key Judge no show - PPA has key
38	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- ?	Yes	They do not have the seals to seal it - Refuse to open the back of the memory pack seal.
38	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes - Yes	Yes	C/P was on, but it was open
38	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	N/A	N/A

Summary of Results for Ward 38

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's ?	Notes
38	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	N/A	N/A
38	0	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - Yes	N/A	N/A
38	0	All	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A	N/A
38	0	All	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - Yes	Yes	N/A
38	0	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - Yes	Yes	Advised them to turn electronic polling so screen isn't visible to crowd
38	0	All	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - Yes	Yes	Poll watchers present checking names

Summary of Results for Ward 41

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
41	5	All	No	No	N/A	Yes	Yes	No	No	Yes	Yes	No	Yes - Yes	N/A	N/A
41	4	No	No	Yes	N/A	N/A	No	Yes	Yes	Yes	Yes	No	Yes - Yes	Yes	Green Seal -No seal last night, A green seal was put on last night and it was there this morning - Booths set up last night by K. - Alone
41	4	All	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes - Yes	Yes	Put seal on upon request - said had to remove seal to start machine - Seals missing in 3 locations
41	4	No	No	N/A	Yes	N/A	Yes	Yes	Yellow Seal only	Yes	Yes	Yes	Yes	No	WM opened the ESC alone and set the poll up alone. Not done with the EV stickers when the PW left
41	4	All	Yes	Not All	Fell off	Yes	Yes	Yes	Yes	Yes	No	No	Yes - Yes	Yes	The PPA had a badge that fell off. The team put card activator seal on upon request at 5:47
41	4	All	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes-Yes	Yes	
41	3	B. Only	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes - Yes	Yes	N/A
41	3	All	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	Yes	Took down touch screen prior to my arrival. Tags were off. Said no one used it all day. The PPA reported she left the envelope at home with badges.
41	3	3 judges	Yes	Not All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No - No	No - not all	120 stickers - most were done before open - 20 left. 1 extra name - was checked and inserted.
41	3	All	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	Yes - No	Sticker not completely applied - Voter not in book per Rachel M.
41	2	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes -No	Yes	N/A
41	2	No - Key Judge only	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	KW (key judge) set up poll alone (Double check this) Card Activator was not sealed. PW request caused for it to be sealed.
41	2	3 judges	No	Yes	Yes	Yes	Yes	Yes	Yes-Seal Damaged	Yes	Yes	Yes	Yes	Yes	Set up evening of 4/4/11 Mr. C. reported there was no green seal, they did not call
41	2	All + ppa	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	N/A

Summary of Results for Ward 41

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
41	2	3 judges + ppa	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Judges report no EV stickers received.
41	2	D.E & PPA alone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	Yes	N/A
41	2	BS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	BS openned ESC alone, BS and JJ set up the poll - at 6:50 the EV stickers still had not been started
41	2	All	Yes	N/A	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Scroll Seal - Not present, but was placed on while pollwatcher was present. - EV Stickers were not completed until 6:45 am
41	2	3 judges	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No - Broken	Yes	Judges reported the Ballot Scanner had to be replaced. New unit came about 6:45am. Judges stowed ballots in ESC until new came per instruction
41	1	3 judges	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	Yes	N/A
41	1	All + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	Yes	N/A
41	1	All + ppa	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	Yes	N/A
41	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	N/A
41	1	All	Yes	N/A	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	EV not finished when the polls opened
41	1	All	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - Yes	Yes	N/A
41	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Not at 6:35	Electronic ballot box allows visibility beyond voter visibility. The EV stickers were not completed when the PW left at 6:45 am
41	1	3 Judges	Yes	N/A	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	HS opened precinct 21 ESC with key from precinct 22 (ward 41) because AC (key judge for precinct 21) was late. HS stated "all the keys for the ESC are the same."
41	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	T/S broken in the morning.
41	0	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - Yes	Yes	N/A
41	0	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - Yes	Yes	N/A

Summary of Results for Ward 41

Ward	Prec ER	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
41	0	3 judges	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - Yes	Yes	DS noted that one early voter sticker did not have corresponding page on applications for ballot. DS called board regarding this
41	0	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - Yes	Yes	N/A
41	0	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - es	Yes	N/A

Summary of Results for Ward 43

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
43	4	All + PPA	No	N/A	Yes	Yes	Yes	Yes	Open Red Seal	No	No	No	Yes - N/A	Yes	N/A
43	4	All + PPA	No	Yes	No	N/A	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	N/A	The Judges would not disclose if they had the stickers on.
43	4	All + PPA	No	Yes	No	Yes	Yes	Yes	No	Yes	Yes	No	Yes - N/A	Yes	N/A
43	3	3 judges PPA	Yes	Yes	Yes	Yes	Yes	Yes	Open Red Seal	No	Yes	No	Yes- Yes	N/A	N/A
43	3	All	No	Yes	N/A	N/A	N/A	Yes	Yes	Yes	Yes	No	No - No	Yes	N/A
43	3	2 + PPA	Yes	Yes	Yes	Yes	Yes	N/A	Machine Broken	Machine Broken	Yes	No	Yes- Yes	Yes	
43	3	All + PPA	No	N/A	Yes	Yes	N/A	Yes	Yes	Yes	Yes	No	Yes - No	Yes	N/A
43	3	N/A	No	N/A	No	N/A	Yes	N/A	Yes	Yes	No	Yes	N/A	N/A	Judge refused to the ballot scanner and called Election Central
43	2	4 + PPA	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
43	2	All + PPA	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No - No	Yes	N/A
43	2	All	Yes	Yes	N/A	N/A	Yes	Yes	No	Yes	Yes	No	Yes - ?	Yes	Yellow Seal was on, no Red Seal (T/S O/C)Locked did not show me
43	2	All + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes- Yes	Yes	All signature papers w/ labels were removed from the binder and placed on the spindle before polls opened and were not numbered.
43	2	All + PPA	No	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	Yes	N/A
43	2	All + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Open Yel Seal	Yes	Yes	No	Yes- Yes	Yes	N/A

Summary of Results for Ward 43

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
43	2	All	Yes	Yes	Yes	Yes	Yes	Yes	T/S Broken	Yes	Yes	No	Yes- Yes	Yes	N/A
43	2	N/A	No	Yes	Yes	Yes	N/A	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
43	2	3 Judges	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A	N/A	N/A
43	2	All	No	N/A	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A	N/A	N/A
43	2	All + PPA	No	N/A	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes	N/A
43	1	All PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	Lots of pages of signature book doesn't contain any signature for long time voters
43	1	All and PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - N/A	Yes	N/A
43	1	3 Ej's + PPA	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
43	1	5 EJ's + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
43	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	N/A	Yes	N/A
43	1	All + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
43	1	All PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
43	1	All + PPA	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
43	1	All	Yes	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	Yes	N/A
43	1	3 Judges + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
43	1	All + PPA	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
43	1	All + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes- Yes	N/A	N/A

Summary of Results for Ward 43

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
43	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No - Yes	Yes	N/A
43	1	3 Judges + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
43	1	All	No	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes- Yes	Yes	N/A
43	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - N/A	Yes	N/A
43	1	All	No	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes	EV stickers done last night -
43	1	All + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	N/A	N/A
43	1	All + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - N/A	Yes	Why are so many signatures missing from ballot application book?
43	1	All + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
43	1	All + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
43	1	All + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
43	1	All + PPA	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - N/A	N/A	N/A
43	0	3 Judges + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes- Yes	Yes	N/A
43	0	N/A	Yes	N/A	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes	N/A
43	0	All + PPA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes- Yes	Yes	N/A

Summary of Results for Ward 45

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
45	8	G. and S. did it alone the night before	No	No	N/A	No	Yes - Signs were wrong	Yes	Yes	Yes	No	No	Yes- Yes	No Stickers placed on	Judge (S.)and the Janitor (G.) live there. They set up the polls night before in a Gym. S. was poorly trained yet considered the lead judge. He recently moved in to live there. The signage was incorrect out front. The EV stickers were not on at 6:30PM. I reported this to the EC at 6:49 PM. The Card Activator seal was missing. G. insisted we look at the kitchen he just finished painting,
45	4	N/A	No	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No	N/A	N/A	There was no sign on the front door. No seals on ballot box. - T/S Scroll was broken from the morning - When repaired the technician did not replace the seal.
45	4	All	Yes	Yes	Yes	N/A	Yes	No	Yes	No	No	Only 1	Yes - Yes	N/A	No seal on the Card Activator. T/S missing seal on scroll
45	4	T - Alone	Yes Broken	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes - Yes	Yes	The PPA fixed the invalid message by powering up and down the machine 5-6 times. They report the card activator does not consolidate properly (last 3 elections). They report the ballot counter got an error "wrong cartridge" they rebooted and it connected itself. They want the machines fixed - noteworthy because ESC label wasn't on. The TS had to be repaired 4 or 5 times. Judges felt the paperwork was confusing. (Green Seal Notes: T. reported seal was broken - she inspected the ESC alone and resealed it)
45	4	One judge set up alone on Sunday night	N/A	Yes	Yes	No	Yes	Yes	Open - Damaged Seal	Yes	Yes	No	Yes N/A	N/A	One Dem judge set up polling place alone on Sunday night - same judge placed EV stickers on the books - alone. EC had a phone check. The PPA was very adamant she was not trained in seals. (Green ESC Seal Notes moved: Reported yes but no seal was there.)

Summary of Results for Ward 45

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
45	4	C. only one	No -	N/A	N/A	Yes	Yes	Yes	No	Yes	Yes	No	Yes - Yes	Yes	M. was the Dem judge at the table. Literally building the poll list for a pollwatcher who was not there. Missing ballot box and TS/OC seals - C. set up alone - unsupervised - Dem judge (Green Seal Notes C set up booths alone, then he applied a seal for the morning - no seal from factory.)
45	4	N/A	No	Yes	No	Yes	N/A	Yes	Yes	Yes	N/A	No	Yes - No	N/A	This poll had several Garrido pollwatchers out front and inside. They were missing 1 judge and couldn't take the time
45	4	All	Yes	Yes	No	Yes	on 1 side	Yes	Yes	Yes	Yes	No	Yes - No	N/A	Investigator 5x
45	4	All set up Mon night	Yes	Some	Yes	Yes	Yes	Yes	Yes- Damaged	Yes	Yes	No	Yes - Yes	N/A	Ballot box won't transmit to consolidator. Last two elections.
45	3	All	Yes	Yes	Yes	Yes	Yes	No seal & broken machine	No	No seal - Broken	Yes	Yes	Yes - N/A	N/A	Experienced team. Report that the last 5 elections the same TS was sent to them broken (placed a small mark on a label to ID the same machine). No seals on TS. This team gets an error message (001445). This team set the polling place up the night before.
45	3	All	Yes - broken	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes - N/A	Yes	Sign announcing the polling place was inside the door, not outside. EV stickers were placed on. D. reported she called in that the ESC had a broken seal on it when she arrived - she was very concerned about it. Young man repeated they did not take the oath. No ballot box seals. D. reported the Green Seal was broken when she arrived
45	3	All	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes -N/A	Yes	Taught Judges how to put seals on Ballot Box. There was no sign out front. V. called EC to check if she had to show the back of the ballot machine
45	3	All	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes - Yes	N/A	

Summary of Results for Ward 45

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
45	3	Team	Yes - Unsure	Yes	N/A No PPA	Yes	Yes	Yes	No	Yes	Yes	No	Yes N/A	Yes	I was unclear if ESC had a seal but did not want to press the judge who did not want to show it. Touch screen did not have the open/close seal. Ballot box unsealed.
45	3	All	Yes	Yes	PPA asleep	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes -See Notes	N/A	When this team arrived the ballot scanner was out on the table. The judges were upset about this because it was not there the night before. They all state they did not leave it out. No seal on ballot box.
45	3	All	Yes	N/A	No	Yes	Yes	Yes	Yes	No Seal Open	Yes	No	Yes - Yes	N/A	The seal on the T/S Cartridge Port was open.
45	3	All	Yes	No	No	Yes	Yes	Yes	N/A	N/A	Yes	None	Yes ?	N/A	Could not read seals on the T/S
45	2	All	No	Yes	N/A	Yes	Yes	Yes	Yes - Strange seal from U-Line	N/A	N/A	Yes	Yes - Yes	N/A	When they take ballots to transfer station - officials seal them there (big box of them). - The T/S open/close seal was an unrecognized seal from "U-Line"
45	2	All	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes - Yes	Yes	The location lacked the cone - there was a large group (10 - 12) of people outside the poll, too close - electioneering - Asked the Ejs to put the cone out. They walked outside but were not too concerned - we did not remain to see it resolved.
45	2	All	Yes	Yes	N/A	Yes	Yes	No	Yes	Yes	Yes	No	Yes - Yes	Yes	Mature EJ team - did not have ballot seals on - they had a tech for the broken seal. The T/S Malfunctioned. - Technician did not replace the seal. The T/S Scroll seal is open and damaged.
45	2	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes -N/A	No	No Ballot Box Seals - Added the seals - They forgot to add the EV stickers and added them in the mornings.
45	2	J - Alone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	N/A	N/A	N/A
45	2	All	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	Yes	No seals on the ballot boxes.

Summary of Results for Ward 45

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
45	2	N/A	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes N/A	N/A	EV stickers were on. They did not have seals on the ballot box. This team has a card activator that has had trouble transmitting in the past.
45	2	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A	N/A	No	Yes - Yes	Yes	2 broken seals were besides the machine - red and yellow - PPA/Judge reported the red one came broken so they replaced it.
45	2	All	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes -N/A	Yes	Yes	Yellow seal on O/C was broken before they arrived and there was o Red Seal. (T/S - O/C)
45	1	All	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes	Yes - No	N/A	N/A
45	1	Alll	No	N/A	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes	Yes - Yes	Yes	No ESC Seal
45	1	All	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes -?	Yes	Judges placed blue seals on after I arrived
45	1	All	Yes	Yes	N/A	N/A	Yes	Yes	Yes	Yes	No	Yes	Yes - Yes	N/A	No seal on the card activators
45	1	All	Yes	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes	No	Yes -Yes	Yes	They worked together for a long time. No seals on ballot box.
45	1	All	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes -Yes	N/A	N/A
45	1	Team	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes - Yes	Yes	EV stickers were on. The EJ reported the ballott scanner was broken. The technician came out to repair it and he did not place seals on the machine. I viewed the work order proving he came out. No ballot box stickers.
45	1	N/A	Yes	Yes	N/A	N/A	Yes	Yes	Yes	Yes	No	Yes	N/A	N/A	N/A
45	1	R. alone	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - Yes	N/A	N/A

Summary of Results for Ward 45

Ward	Prec FR	Who was present when the ESC was opened and the	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal	Are the EV labels placed on the ballot app's?	Notes
45	0	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - N/A	Yes	This team loved their PPA, who set the poll up for them in the morning (they were all present). This team worked great together - they had the judges table with 8 people on it (too many) but otherwise this was a well run team
45	0	All	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes	N/A	Yes	Yes - Yes	N/A	[illegible] the serial #s on the touch screen unit and printer - also wanted us to make sure metal
45	0	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes - Yes	N/A	N/A

Summary of Results for Ward 46

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
46	6	All	Yes	No	No	Yes	Yes	No	N/A	No	Yes	No	Yes -No	Yes	The T/S machine was broken. Seals were removed.
46	5	All	Yes	Most	No	Yes	Yes	Yes	No -	Yes	Yes	No	Yes -No	Yes	Yellow Seal is open on the T/S Open Close Port.
46	5	All	No	No	Yes	Yes	N/A	Yes	No	N/A	Yes	No	Yes- Yes	No	N/A
46	4	All	No	Yes	Yes	No -	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	No	They were checking lists and judge said they did not have stickers. After asked, another judge found stickers. - PPA showed ballot scanner seal - Election Judges 5-40 years experience, skipped swearing in.
46	3	All	Yes	Yes	N/A	Yes	N/A	Yes	Yes	Open Seal	No	No	N/A	N/A	Broken scroll on the Card Activator The tape broke and they had to break the seal and did not replace it.
46	3	All	Yes	No 4/6	N/A	Yes	Yes	Yes	No - Seal broken	Yes	Yes	No	N/A- N/A	Yes	Additional list of names not marked in book, said they were checking but list was buried under activator at the time…
46	3	All	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes- Yes	N/A	N/A
46	2	All	Yes	Yes	N/A	No	Yes	N/A	Yes	Yes	Yes	No	Yes- Yes	Yes	Checking extra list? Yes- Touchscreen display visible to everyone entering polling location (see paper for drawing) Veteran judges skipped swear in.
46	2	All	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes -No	Yes	N/A

Summary of Results for Ward 46

Ward	Prec FR	Who was present when the ESC was opened and the poll was set up?	Was the Green Seal closed on the ESC?	Did the Judges have their badges on?	Did the PPA have their badge on?	Did the judges take the oath?	Are there blue cones at 100ft?	Is the T/S Scroll Sealed?	Is there a red seal on the T/S polls Open/ Close port?	On the T/S is the Cartridge Port sealed?	Is the Card Activator sealed?	Is the Ballot Box Sealed?	Is the Ballot Scanner locked and the Red Seal on the back?	Are the EV labels placed on the ballot app's?	Notes
46	2	All	Yes	Yes	Yes	No	N/A	Yes	Yes	Yes	Yes	No	N/A	Yes	N/A
46	2	All	N/A	Yes	N/A No PPA	N/A	N/A	N/A	N/A	N/A	N/A	No	Yes	N/A	PPA was not present
46	2	G and G	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
46	2	All	Yes	No	N/A	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
46	1	All	Yes	Yes	N/A	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes - N/A	Yes	Could not see Ballot scanner seal, Judges wouldn't open it until polls close
46	1	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes- Yes	Yes	N/A
46	1	All	Yes	N/A	N/A	No	N/A	N/A	N/A	N/A	N/A	N/A	Yes - N/A	N/A	1 judge difficult - question re: opening ballot box seal door.They called Election Central.
46	1	All	N/A	N/A	N/A	Yes	N/A	Yes	N/A	Yes	N/A	No	Yes	N/A	N/A
46	1	All	Yes	N/A	Yes	No	N/A	Yes	Yes	Yes	Yes	Yes	Yes- Yes	Yes	N/A
46	1	All	Yes	Yes	N/A	N/A	N/A	Yes	N/A	Yes	Yes	No	Yes- Yes	N/A	Judges volunteered to unlock and show seal
46	1	All	Yes	N/A	N/A No PPA	Yes	N/A	Yes	Yes	No	Yes	Yes	Yes N/A	Yes	N/A

Journal of Physical Security 5(1), 73-77 (2011)

Viewpoint Paper

Suggestions for Better Election Security*

R.G. Johnston and J.S. Warner
Vulnerability Assessment Team
Argonne National Laboratory

Summary of Common Security Mistakes

1. Electronic voting machines that fundamentally lack security thought and features, including an ability to detect tampering or intrusion, or to be reliably locked or sealed.

2. Failure to disassemble, inspect, and thoroughly inspect (not just test) a sufficient number of voting machines before and after elections in order to detect hardware or software tampering.

3. Assuming that tamper-indicating seals will either be blatantly ripped/smashed open, or else there is no tampering. In reality, even amateurs can spoof most seals leaving (at most) subtle evidence.

4. Inadequate seal use protocols and training of seal installers and inspectors. Failure to show examples of blatantly and subtly attacked seals to seal inspectors.

5. Over confidence in use of a voter verified paper record (VVPR). A VVPR is an excellent security countermeasure, but it is not a silver bullet, especially for an election organization with poor overall security.

5. Little or no insider threat mitigation.

6. A poor security culture, including denial and no *a priori* procedures for dealing with security questions or concerns.

About These Suggestions

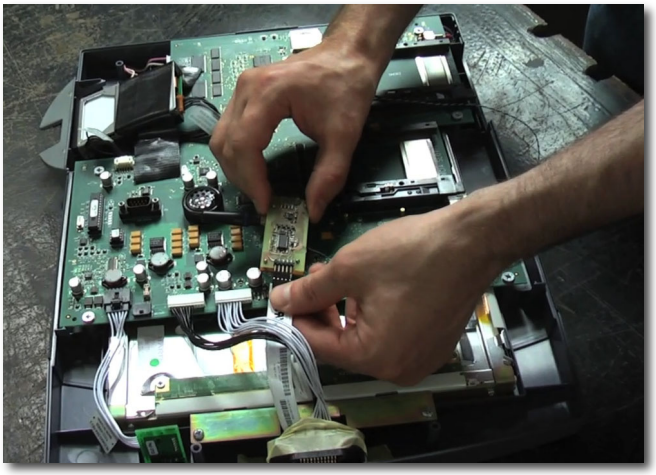
The following suggestions for better election security are provided by the Vulnerability Assessment Team (VAT) at Argonne National Laboratory. The suggestions fall into two categories, "Minimum", which are security features that are essential in our view, and "Recommended", which are needed for the best security. (For more information on the VAT see http://www.ne.anl.gov/capabilities/vat.)

Hardware & Software Inspection

Recommended: Prior to the election, at least 1% of the voting machines—randomly chosen—should be removed from the polling places and tested, then disassembled, inspected, and the hardware examined for tampering and alien electronics.

The software/firmware should also be examined, including for malware. It is not sufficient to merely test the machines in a mock election, or to focus only on cyber security issues! This analysis should be completed prior to the election.

Minimum: It is completed less than 6 weeks after the election.



Inserting alien electronics into an electronic voting machine in a classic (non-cyber) "man-in-the-middle" attack.

Minimum: Within 4 weeks after the election, at least 1% of the voting machines actually used in the election—randomly chosen—should be tested, then disassembled, inspected, and the hardware examined for tampering and alien electronics. The software/firmware should also be examined, including for malware. It is not sufficient to merely test the machines in a mock election, or to focus only on cyber security issues!

Recommended: The voting machines for the above reverse engineering (or trial bribery discussed below) should be randomly chosen based on pseudo-random numbers generated by computer, or by hardware means such as pulling numbers or names from a hat. No

*Editor's Note: This viewpoint paper was not peer-reviewed.

individual should make the random choices without the aid of hardware or software.

Insider Threat

Minimum: All election officials, technicians, contractors, or volunteers who prepare, maintain, repair, test, inspect, or transport voting machines, or compile "substantial" amounts
of election results should have background checks, repeated every 3-5 years, that include a criminal background history, credit check, and (when practical) interviews with co-workers.

Minimum: Prior to each election, all poll workers, election judges, election officials, and relevant contractors and technicians should take an oath to protect election integrity. They should be warned of the legal penalties for vote tampering and fraud, and reminded of their patriotic and ethical responsibility to help guarantee fair elections. They should also be thanked for taking on this important responsibility, and being vigilant of election security.

Minimum: Before each election, the U.S. citizenship of every poll worker and election judge should be verified in a reliable manner.

Recommended: On a regular basis, try bribing a small subset of poll workers, election judges, election officials, technicians, clerks, and personnel who transport voting machines and other election materials. Let them keep the money and hail them publicly as honest heroes if they decline the bribe. (Allow at least 36 hours for the bribe to be reported or declined.) There are legal entrapment issues here, but the point isn't so much to identify and fire dishonest individuals as it is to make bribes untenable by creating publicity and uncertainty about whether an apparent bribe is some kind of test.

Recommended: A written policy should be in effect and periodically communicated to all employees and contractors that bribery attempts must be reported immediately, and where or to whom they should be reported.

Locks

Minimum: Locks on voting machines should not all open with the same key.

Minimum: Opening of a lock on a voting machine or container should be accompanied by a careful examination of the exterior of the voting machine or container in order to try to determine if the integrity of the voting machine or container has been compromised without disturbing the lock. This includes looking for evidence of cosmetic repair of the voting machine or container walls after they have been breached. Election officials, judges, and technicians should be trained on how to inspect the relevant voting machines or containers, including the underside.

Tamper-Indicating Seals

For information on tamper-indicating seals, see *American Scientist* **94**(6), 515-523 (2005); *ACM Transactions on Information and System Security*, 14, 1–29 (2011); http://www.cs.princeton.edu/~appel/voting/Johnston-AnalysisOfNJSeals.pdf and http://www.ne.anl.gov/capabilities/vat.

Minimum: Avoid the assumption that tamper-indicating seals will either be blatantly ripped/smashed open, or else there is no tampering. In reality, even amateurs can spoof most seals leaving (at most) subtle evidence.

Minimum: Prior to each election, all poll workers and election officials who inspect seals (including tamper-evident packaging) need to have a minimum of 10 minutes of training per kind of seal used. This training will include information as to how to install (if appropriate) and inspect the seal. This should include multiple samples, photos, or videos of that specific kind of seal that has been attacked subtly and samples, photos, or videos of that specific kind of seal that has been attacked blatantly, e.g., by being ripped open or smashed.

Minimum: Personnel who inspect seals that protect "large" numbers of election results should have an additional 10 minutes per kind of seal. This should include hands-on practice in spotting sample seals that have been opened subtly and those that have been opened blatantly.

Recommended: Only a small number of election officials should be authorized to order tamper-indicating seals, and the seal manufacturer or vendor should contractually agree to refuse orders not placed by those individuals or by anyone who does not know the secret password required for seal purchases for a given election district, and to report failed attempts to officials of that election district.

Recommended: The vendor or manufacturer of seals used for election purposes should contractually agree not to provide 2 or more seals with the same serial number (including at a later time) to anyone.

Recommended: A two-person rule should be in effect when a seal is applied to critical election assets. Each person should verify that the correct seal was correctly

applied, and that its serial number is correctly entered into the database of seal serial numbers.

Minimum: Only tamper-indicating seals with unique serial numbers should be used.

Recommended: Signing or initialing seals offers little effective security and should not be done.

Minimum: All seal inspections require checking the seal serial number against the secured data log of seal serial numbers. Each seal must also be carefully examined for evidence of both subtle and blatantly obvious opening, counterfeiting, damage, or removal.

Minimum: The list of seal serial numbers for seals applied to voting machines and containers or packages of sensitive election materials must be carefully protected from tampering, theft, or substitution.

Recommended: Seals should not be used in sequential order based on serial number (so that an adversary cannot predict a seal serial number in advance).

Minimum: Seal inspectors must not be fooled by a seal of the wrong kind or color that has the correct serial number—a common mistake.

Minimum: Seals must be inspected alongside an identical (except for serial number), well-protected unused seal of the same kind. There must be a comparison of size, morphology, color, surface finish, and serial number font, digit spacing, and digit alignment/orientation.

Recommended: Minimize the use of (pressure sensitive) adhesive label seals (because these tend to be easy to counterfeit or to remove, then replace without leaving easily detectable evidence, plus they require an inordinate amount of training and inspection time to be effective).

Minimum: With adhesive label seals, prior to installing the seal, the surface the seal is to be applied to must be cleaned and checked for evidence of oil or other substances that can reduce surface adhesion.

Minimum: With adhesive label seals, the way the seal behaves when it is removed is often a critical method for checking for tampering. To be effective, however, the seal inspector must know how the seal is supposed to behave when removed.

Minimum: Any checking of a seal for evidence of being broken or tampered should be accompanied by a careful examination of the container or package or voting machine the seal is attached to in order to try to determine if the integrity of the container or package or voting machine has been compromised without disturbing the seal. This includes looking for evidence of cosmetic repair of the container/package/voting machine walls after they have been breached. Seal inspectors should be trained on how to do this inspection for each kind of container, package, or voting machine.

Minimum: All used seals should be preserved until at least 3 months after the election for possible examination, then thoroughly destroyed (not just discarded in the trash) so that the parts cannot be used by adversaries to practice or execute seal attacks.

Minimum: All unused seals should be protected or guarded prior to use from theft or unauthorized access. Seal installers must be required to protect and turn in any unused seals.

Secure Transport

Recommended: Escort the voting machines to and from the polling place if at all possible. Use *pro bono* volunteers if necessary.

Recommended: Do not allow technicians to work on a specific voting machine without authorization and oversight.

Recommended: Personnel or contractors who transport voting machines to or from the polling places should be bonded.

Minimum: Some individual or group should be responsible for accepting voting machines and sensitive election materials delivered to the polling place before or on election day, sign for them, and be responsible for providing oversight to the extent practical. (This can include students at a school, for example.) It should be possible to determine if there was an unexpected delay in delivery of any such voting machines or election materials, and this delay must be investigated immediately. Similarly, any delay in receipt of the voting machines back at the storage warehouse after the election should be detectable and immediately investigated.

Chain of Custody

A chain of custody is a process that helps to secure voting machines, ballots, records, memory devices, seals, keys, seal databases with serial numbers, and other election materials. We henceforth refer to these items needing protection from theft, tampering , copying, or substitutions

as "assets". (Note: A "chain of custody" is not a piece of paper that multiple people sign or initial.)

Recommended: An effective chain of custody starts by checking that everyone to be involved in handling the assets in question is trustworthy. This is best determined by periodic background checks.

Minimum: An effective chain of custody requires procedures to make sure that each person handing off the assets to another is sure of the identify of the person they are handing the material to, and that this person has been authorized to receive the assets.

Recommended: Each individual in the chain of custody must know the secret password of the day or the election before being allowed to take control of the assets.

Minimum: Each individual in the chain of custody must assume the individual responsibility of safeguarding the assets while in their custody, not letting the assets out of their sight to the extent possible, and securing the assets under lock or seal when not in sight.

Minimum except where noted: A chain of custody log should be kept with the assets. It must be signed by each recipient in the chain of custody when accepting the assets with a carefully signed signature (not initials) along with a printed, legible listing of their name, the date, location (Recommended), and time (Recommended). This log must also be protected from tampering, counterfeiting, or substitution.

Independent Security Review

Minimum: The majority of advice on election security should not come from vendors or manufacturers of voting machines or of tamper-indicating seals or other security products used in elections. It is necessary to seek out objective, independent security expertise and advice.

Minimum: Election officials will arrange for a local committee (*pro bono* if necessary) to serve as the Election Security Board. The Board should be made up primarily of security professionals, security experts, university professors, students, and registered voters not employees of the election process. The Board should meet regularly to analyze election security, observe elections, and make suggestions for improved election security and the storage and transport of voting machines and ballots. The Board needs considerable autonomy, being able to call press conferences or otherwise publicly discuss its findings and suggestions as appropriate. Employees of companies that sell or manufacture seals, other security products often used in elections, or voting machines are not eligible to serve on the Board.

Minimum: At least once every 3 years, the Election Security Board should oversee or conduct a comprehensive vulnerability assessment of the local election process, involving external consultants, volunteers, and security experts (including *pro bono*) to the extent practical.

Minimum: A Chief Election Security Officer (paid or unpaid) should be appointed who may have other duties as well. He or she is responsible for analyzing and overseeing election security issues and security training. The Security Officer also deals with and investigates security questions, concerns, and incidents on election day. He/she serves on the Election Security Board (discussed above) as a voting member, but does not chair the Board or appoint its members.

Recommended: The Chief Election Security Officer should maintain a publicly posted, frequently updated list of what he/she judges as the ten best suggestions (from the Board, or other internal or external sources) for potentially improving election security, and the prospects for implementing them. Public comments on this list should be encouraged.

Creating & Nurturing an Effective Security Culture

The key to good security is to have a healthy security culture. This requires everyone to pay attention to security issues, be thinking critically and continuously about security, to ask good questions, avoid denial, and to be free to raise concerns and be listened to about security issues.

Minimum: When election security is questioned, the first response of election officials and the Chief Election Security Officer must not be to deny the possibility of security vulnerabilities, but rather to seek to learn more and solicit advice from the person(s) raising these questions (and others) as to possible countermeasures or security improvements.

Recommended: Before each election, discuss in some detail with poll workers, election judges, and election officials the numerous ways that the voting process can be tampered with, and what to watch out for. Have them individually, or in groups suggest other ways they would tamper with votes if they were so inclined, including fanciful ways, using insiders or outsiders or insiders collaborating with outsiders. (The merits of the attack

scenarios they devise are less important that instilling a mindset of thinking like the bad guys).

Recommended: Poll workers, election judges, election officials, and other personnel involved in running elections should be warned and educated about techniques for misdirection and sleight-of-hand, perhaps by having these techniques explained/demonstrated by a magician, live or on video. (The sense of alertness to malicious acts that this engenders is actually of greater benefit than awareness of misdirection and sleight-of-hand *per se*, though the latter is not negligible.)

Recommended: Before each election, discuss with poll workers, election judges, and election officials the importance of ballot secrecy, and the importance of watching for miniature wireless video cameras in the polling place, especially mounted to the ceiling or high up on walls to observe voters' choices. The polling place should be checked for surreptitious digital or video cameras at least once on election day.

Recommended: Poll workers, election judges, election officials, and other personnel involved in running elections should be told how to accurately verify the identify of authorized election and law enforcement officials, as well as election workers who may be present on election day.

Recommended: Security must not be based substantially on secrecy, i.e., Security by Obscurity is not a viable security strategy, nor is secrecy conducive to observers, critical review, process improvement, feedback, transparency, or accountability. Somewhat counter-intuitively, the best security is security that is transparent. (Note: Some short-term secrecy may be warranted, such as short-term passwords or secrecy about the details of voting machine transport.)

Minimum: Security is hard work so expect it to be hard work. Any security device, system, procedure, or strategy that sounds too good to be true almost certainly is.

Minimum: There must be a convenient way for poll workers, election judges, election workers and contractors, election officials, and the general public to report security concerns, including anonymously on election day. There must be mechanisms in place to respond in a timely manner to these concerns, perhaps through the Chief Election Security Officer discussed above.

Recommended: Welcome, acknowledge, recognize, praise, and reward good security practice, as well as reasonable security questions and suggestions from any quarter, including from employees, contractors, poll workers, election judges, journalists, bloggers, and the general public.

Recommended: Election officials are often elected or are political appointees. It is important for a good security culture to attempt to differentiate and separate concerns, questions, and criticisms about election security from political attacks on those election officials.

Recommended: Security is difficult and involves complicated, value-based tradeoffs. Thus, security policy and practice is intrinsically a controversial topic worthy of debate and analysis, and should be viewed and treated as such. The existence of disagreement and dissent in regards to security must not be taken as a sign of weakness, but rather welcomed as a sign of a healthy security culture.

Other Suggestions

Recommended: Election officials should pressure manufacturers of voting machines to design them with better physical security, cyber security, and tamper/intrusion detection. Insist that manufacturers of voting machines design them with secure hasps that allow the use of locks and seals other than pressure sensitive adhesive label seals.

Minimum: Poll workers, election judges, and election officials should be able and expected to determine if a voting machine has been replaced by an unauthorized voting machine or counterfeit voting machine.

Recommended: A hash should be printed on each paper ballot on election day after each voter has completed the ballot. This hash should be generated from a secret algorithm that is different for each election, and possibly each polling location.

Journal of Physical Security 5(1), 78-82 (2011)

A Comparison of Cyber Attack Methods

Tyler J. Murphy
Lewis University
Romeoville, Illinois

Introduction

Have you ever seen the movie "Swordfish"? Do you remember when Hugh Grant was writing that "super worm" that was going to punch through the banks security systems and steal a whole bunch of money for John Travolta? What sticks out for me is that while he was writing his "super worm", there where graphical cubes floating around his 6 monitors, and every time something went wrong one of the cubes would shoot out of order. When he finished the hack, everything fit together like he was working on a jigsaw puzzle or something. Unfortunately, that is exactly how real world hacking doesn't happen.

There is an almost idealized view today of "hacking". In the media and in popular culture, they usually show a splash screen of some guy with earrings, or a bunch of donuts sitting in front of a computer staring at binary code, babbling about how he is going to bypass the firewall by cracking the encryption. Not very realistic!

While I was doing my undergraduate work at Lewis University, I wanted to do comparison of cyber attacks. In particular, I wanted to compare attack vectors. Which would be the best? Which would grant me access the fastest? So, I chose three attacks from the many different potential attack vectors—3 that typically receive much of the attention. The first is physical access. The second kind of attack is phishing or social engineering. The third attack is the famous attacking of the computer network.

All the attacks I explored and demonstrated were done on my own computer, or else on a computer and network with the full knowledge and consent of the owners (who offered me no assistance in actually executing the attacks).

If You Can Touch the Box, You Own the Box: Physical Attack

I setup a Windows XP system, a Macintosh OSX 10.5 system, and a Windows Vista Laptop for this experiment. The passwords were completely randomized and I had no idea what they were. As is well known, passwords do not represent a daunting hacker challenge. In the case of the Windows XP system, I used my own password cracker, but you can find them all over the Internet. Basically the cracker I used was a bootable ISO image. I simply rebooted the target system and dropped the ISO (in my case it was a UNIX BOOT OS) into the optical drive, and then followed the on-screen instructions. It has you mount the hard disk, select boot partition, etc. The actual cracking does not take place until the software locates the Windows SAM file. This file is where Windows stores a hashed version of your password. The problem is, the file is writeable. Most of these "crack disks" give you an option to change the password to something else. This, however, really isn't a good choice because the hacking victim is going find something is amiss when the password he/she has used for the past 6 months

doesn't work anymore. So the hacker should simply select "blank password" option. This basically deletes everything inside the same file effectively making the password blank.

The Macintosh 10.5 system similarly offered little resistance. In fact, all the hacker needs is a 10.5-operating disk. Macintosh supplies you with a password-reset utility, which basically does the same thing as the Windows "crack" disk. You can also boot the system in single sign-on mode and delete the initial set-up record. You will have to go through the annoying first time screens, but you get to create you very own admin account at the end.

Only slightly more difficult to hack was the BIOS password for the Vista laptop computer. The BIOS passwords (for most systems) are controlled by the C-MOS chip. To reset the password, all the hacker has to do is reset the chip. This can be done by removing the 3V lithium battery on the motherboard. The battery is easy to spot and is used in many other electric devices. The other way to reset it is a button located on the motherboard.

These attacks were based on having physical access to the computer systems. Even though there are many other ways to crack into an un-supervised computer, one of my favorites (which is often quite effective) is to look around the desk area for a sticky note with the password.

In my view, the best way to insure overall security against a physical attack is to deploy 2 pieces of technology that have been around for thousands of years, the door and the lock This is where physical and cyber security converge. In my experience, there has been a very intense focus on traditional cyber security measures, while physical security has been on the back burner since the 1980's. As a cyber security analyst, I have often seen a $50K Cyber Intrusion Detection System, or advanced firewall put into use in a room protected by an easy-top-defeat $2 lock. Time and time again, I have walked by server rooms where the door is wide open and nobody has even bothered to deploy the ineffective lock. This is a dangerous security practice that can lead to serious consequences. Physical Security is an integral part of Cyber Security: you cannot have a secure computer infrastructure without a physically secure facility to house it.

Gone Phishing and I Caught a Big One: Social Engineering Attack

Recently, social networking sites and their spin offs have become all the rage. This craze has lead to a dramatic increase in Social Engineering attacks. Social networking sites like Facebook, MySpace, and Twitter are making these types of attacks very easy to do. I view phishing attacks as a kind of network attack (with the exception of phone and mail scams) because they are operated from a remote location using the network as a conduit. On the other hand, phishing is ultimately about hacking a person.

For my social engineering attack, I decided to attack my brother (with his general knowledge and permission, but without his knowing any details of the attack). I lived in an apartment about 30 miles away from him, and had no internal knowledge of his network. Since many attackers like to target a specific person, I decided to go with a targeted phishing

attack. It's a bit like using a fish finder for real outdoors fishing. In my case, the fish finder was Facebook.

I did not create a fake Facebook account because doing so is a violation of Facebook's user agreement—not that a real hacker would much care about this!) I instead used a legitimate Facebook account of a friend of mine (with her knowledge and consent). It turns out that when a 17-year old boy (my brother, the target) gets an invitation from an attractive college-age blond female (my friend who's Facebook account I borrowed), to be his Facebook "friend", he is eager to accept.

Prior to this experiment, I had very little experience with Facebook, so I was surprised to learn how much information is just shot across the Internet. My brother had a privacy filter on, so only his friends could see details of his account, but out of what seems to be thousands of his Facebook friends, very few blocked anonymous users from viewing *their* content. I found the best bait for my brother was a free online game that he and his friends kept talking about. After figuring out the name of game, I did a quick recon on the games external website and got a feel for what the game was about. I even signed up for the free newsletter so that I could later simulate the look and feel of an email coming from the game site. After only about 20 minutes of detective work, I had a game plan.

I decided to spoof a fake e-mail address pretending to be the support staff of the game site. After that, I would slip him some code and presto I would have access to my brother's computer. Now the old adage is, "it is easier said than done". However, in this case, it was almost as easily done as said.

I thought about using an "smtp" hack in which I would brute force the password on a virtual "smtp" port, then spoof the index knowing he would not check. Alternately, I could use my already existent web-hosting client. I choose the web-hosting client. My fake email was decorated with the site's logo. and had the look and feel of the official newsletter.

The online gaming site was free, so I decided to attack my teenager brother where it hurts the most, his wallet. I wrote up an email claiming that the game was going to start charging for online services, however since he has been a loyal player he was going to be selected to receive the paid version for free. There was a catch, however: the fake email claimed that they wanted to run network tests and graphical tests to assess their users' computers. If he wanted to keep playing for free, he would have to install some software.

Now I could have written malicious code, and crafted it to his computer but I decided to go even simpler than that. I used totally legal and freely available software to take control of his system. I used a Virtual Network Controller (VNC) client network tunneling software and a few handcrafted batch files to shut off the pesky Windows firewall and start a background install. Within about 1 hour of sending off my bait to him, the fish bit down hard. As soon as he ran the batch files, the tunnel opened right up and I could use the VNC client to connect right to his system. Just like that, his system was under my control.

What I like most (as the hacker) and dislike most (as a computer security analyst) about this attack is its ease. It took little advanced knowledge of programming or network infrastructure. The attack was successfully completed with knowledge freely available on the Internet. If my brother had simply looked at the email address, or even the HTML index, he would have seen that it was coming from a bogus source. Unfortunately, he is not alone in this behavior. People and organizations fall victim to social engineering attacks all the time. In April of 2011, for example, The U.S. Department of Energy's Oak Ridge National Laboratory fell victim to the same type of attack as my 17-year-old brother did. (See, for example, Elizabeth Motalbano, "Phishing Attack Hits Oak Ridge National Laboratory", "http://www.informationweek.com/news/government/security/229402048).

Unfortunately for Network Administrators, there is no silver bullet to fix these kinds of phishing attacks. The only thing you can do is train your employees to be aware and vigilant. A good way to reduce the risk of becoming a target is to limit how much exposure you give yourself over social networking sites. As for the mass spam emails, remember these common sense rules: " NO ONE EVER GIVES AWAY ANYTHING FOR FREE" and "IF YOU DON'T REMEMBER SIGNING UP FOR THE SPANISH NATIONAL LOTTERY…. YOU PROBABLY DIDN'T".

Knock, Knock. Who's There?: Denial of Service (DOS) Attack

If I could go back in time to when I preformed this experiment and still retain the knowledge and experience I have now, I would do one thing differently: Only experiment with the first two attack vectors. The law got in my way more than any security feature did. DOS attacks are only effective if the hacker faces either attacking an extremely small target with limited bandwidth, or if he has a massive (illegal) bot net at his disposal to take on a larger network. Because I did not want to break any laws (though a real hacker might not be so constrained), I focused on attacking my parents network (again with their knowledge and consent).

I entered in through their wireless network, thankful as the hacker (but not pleased as the good son) that nobody had told my parents that WEP is not a secure protocol. So after some ARP relays, and a run through with KISMET, I was in. I used the network mapping tool NMAP to discover the location on the network. (Of course, any organization with minimal cyber savvy would black hole the ping sweep in a heart beat.) I found my target, my other brother who uses my parent's computer system.

Instead of using a crude ping bomb, I used an ARP bomb. Basically I simply asked his system about 10,000 times for his ARP tables. His system was so concerned with getting me this information that it locked up all other services. The systems network traffic came to a halt instantly and then he could not use any other network services. If you can imagine a large cluster of systems attacking at the same time, you can see how effective this method can be.

The DOS attack is quite easy to accomplish, but its effectiveness is limited to just being an annoyance. DOS attacks, however, are the majority of network-based attacks because they are

easy to do. Using IDS systems (or just about any other monitoring tool that tracks network traffic), administrators can prevent these attacks relatively easily.

Conclusion

All of these attacks are used every day out in the real world. The movies and media have painted the image of the hacker as someone staring at binary code or a scrolling through text file and spitting out random lines of code. The reality is much less romantic: hackers (or crackers) are going to use the path of least resistance. They are going to use the most effective attack at the lowest cost or level of effort. In this study, the cheapest and most reliable attack was the phishing attack. This is probably not surprising: social engineering is often the best way to compromise security.

Acknowledgement

Roger Johnston helped to edit this paper.