Wheeler Trigg O'Donnell LLP

# PUBLIC COMMENT M E M O R A N D U M

**TO:** Secretary of State Scott Gessler

**FROM:** Myriah Sullivan Conroy and Jeffrey A. Sherman

**DATE:** December 8, 2011

**SUBJECT:** Comments Regarding Proposed Changes to Election Rule 43 and the Conditions of Use for Certified Voting Equipment

---

On November 9, 2011, Colorado Secretary of State Scott Gessler (the "Secretary") issued a Notice of Public Meeting to discuss proposed changes to Colorado Election Rule 43 and the Conditions of Use for certified Direct Record Electronic voting equipment (DREs). The notice indicated that a public meeting will be held on December 8, 2011 from 1:00 p.m. to 5:00 p.m. Wheeler Trigg O'Donnell LLP ("WTO") represents Myriah Sullivan Conroy and Jeffrey A. Sherman (the "Electors") and submits these written comments as invited by Section IV of the Notice of Public Meeting. If you have any questions or would like to discuss the Electors' concerns that are discussed below, please do not hesitate to contact either Mr. Paul Hultin or Mr. Matthew Johnson.

## I. INTRODUCTION AND HISTORICAL PERSPECTIVE

### A. In 2006, the Denver District Court Ordered the Secretary of State's Office to Establish New Requirements for Certification of DREs and to Adopt Stringent Security Procedures for the Use of DREs.

*Conroy et al. v. Dennis*, Case No. 06-CV-6072, Denver District Court ("*Conroy*"), marks the point in time when the Electors first became concerned about the dubious actions of the Secretary of State's office regarding the security vulnerability and ease of hacking into DREs. In *Conroy*, the Electors, along with others, formed a group of non-partisan plaintiffs who sued then Secretary of State Ginette Dennis ("Dennis") in her official capacity to require Dennis to comply with applicable law in certifying DREs for use in Colorado elections. *See* Opinion of the Denver District Court (the "Opinion"), Exhibit 1 hereto, at p. 1. After a three-day trial, the District Court ruled in favor of the Electors on a number of key issues.

Most importantly for purposes of these Public Comments, the proposed changes to Election Rule 43, and the proposed changes to the conditions of use for DREs, the District Court ordered as follows:

1. The Secretary was to promulgate a rule containing minimum security standards for DREs as required by C.R.S. s. 1-5-616(1)(g).

2. The Secretary was to retest previously certified systems or any new systems, using the revised security standards to be promulgated by the Secretary, prior to the next primary, general or statewide ballot issue election following the November 7, 2006 general election, whichever comes first.

3. Prior to the November 7, 2006 election, the Secretary was ordered to require county election officials to implement security standards governing the use of DREs. County security standards were required to be developed immediately with input and cooperation from Plaintiffs, and were ordered to be designed to reduce the significant risks of tampering, to increase the security relating to handling and use of DREs, and to provide for secure and proper handling and storage of the paper record of votes cast on DREs in a controlled environment.

*See* Opinion at pp. 7 – 8. The Opinion was not appealed and remains binding on the current Secretary. The county security standards and procedures were ordered because of overwhelming scientific evidence that the DREs are notoriously insecure and can be easily hacked and reprogrammed to change votes.

The retesting of the four existing DRE systems then in use in Colorado resulted in decertification of three of the four DRE systems. In light of the emergency created by this not-unexpected result, interim legislation was passed and stringent security procedures and conditions of use were developed by the Secretary of State to minimize the substantial risks associated with the use of these dubious DRE voting systems.

It is these 2008 security rules and conditions of use that the Secretary now proposes to relax or eliminate entirely. He offers no reason for this other than the self-serving and conclusory statement that he is considering "possible amendments to the election rules in order to improve the administration of Colorado elections law." Notice at page 1.

**B. The Election Reform Commission**

Following the ruling in *Conroy*, and as a result of Senate Bill 08-243, an 11-member Election Reform Commission was created. Secretary Gessler was a member of the Election Reform Commission, and Mr. Hultin was also a member. Following a series of meetings between November 2008 and February 2009, which included: (1) the taking of public testimony; (2) hearing presentations from experts and stakeholder representatives in the fields of elections and voting technology; and (3) deliberating on issues related to reform of Colorado's election system and the use of DREs in Colorado, the Election Reform Commission created a Final Report. The Election Reform Commission's Final Report was submitted to the members of the

Colorado House and Senate State, Veterans, and Military Affairs Committees. *See* Final Report of the Election Reform Commission dated February 27, 2009, Exhibit 2 hereto.

Importantly, of the 20 recommendations the Election Reform Commission approved, nos. 7 and 8 relate directly to DRE security and auditing. *See* Final Report of the Election Reform Commission, Ex. 2, at pp. 5 – 7.

### C. House Bill 09-1335 Becomes Law And Reforms Election Law In Colorado.

As a result of the Election Reform Commission's Final Report, the Sixty-Seventh General Assembly of the State of Colorado passed House Bill 09-1335 that was signed into law by Governor Bill Ritter, Jr. The provisions of House Bill 09-1335 are now found in the Colorado Election Code, C.R.S. s. 1-1-101 *et seq.* There were many critical and much-needed changes to Colorado's election laws in House Bill 09-1335, which included a prohibition on further purchases of DREs, the requirement of a paper record for votes cast on DREs, and the adoption of risk-based audits to mitigate the risk of election fraud that arises from the use of DREs. For all Coloradans who want fair, transparent, and secure elections, House Bill 1335 was a significant step forward.

## II. ELECTRONIC VOTING CONTINUES TO BE UNDER ASSAULT ACROSS AMERICA. ANY CHANGES TO COLORADO ELECTION RULES SHOULD REQUIRE GREATER SECURITY, NOT WEAKER SECURITY POLICIES SUGGESTED BY THE PROPOSED CHANGES.

Electronic voting became much more prevalent following the passage of the federal law known as the Help America Vote Act of 2002 ("HAVA"), P.L. No. 107-252. However, in the massive expansion of electronic voting associated with HAVA, the development and widespread use of DREs resulted in compromises of voting security that were widespread, and that became a matter of great public concern both in Colorado and throughout the entire country. Since *Conroy* and the passage of House Bill 09-1335 in 2009, computer scientists and security experts have continued to demonstrate the woeful lack of security in electronic voting.

For example, in one of the most egregious examples of voting security being easily compromised, national security experts from the Argonne National Laboratory, which is now part of the Department of Homeland Security, recently demonstrated how easy it was to make a "man in the middle" hack into a Diebold DRE.[1] Amazingly, the Argonne computer scientist and security experts demonstrated that it was easy to remotely hack into a Diebold DRE with materials that cost less than $26.00 . *See Researchers Hack Voting Machine for $26*, Sept. 30,

---

[1] A copy of the full Argonne National Laboratory report titled *Suggestions for Better Election Security From the Vulnerability Assessment Team at Argonne National Laboratory*, October 2011, is attached as Exhibit 3 hereto; *see also Diebold Voting Machines Can Be Hacked By Remote Control*, September 27, 2011, at http://www.salon.com/2011/09/27/votinghack/.

2011, at http://www.foxnews.com/scitech/2011/09/30/researchers-hack-voting-machine-for-26/. The Diebold DREs are used in many counties in Colorado. Diebold's voting machine business is now owned by Dominion Voting Systems, a Denver-based company. *See id.* Over 22 states use Dominion Voting Systems' DREs. *Id.* The Argonne researchers were able to hack into the Diebold machines from up to a half-mile away and change a voter's vote immediately after the vote was cast. *Id.* A potential hacker could of course be a Republican, a Democrat, or a foreign person motivated to simply disrupt or destroy the accurate results a given election. This is why the Argonne scientists consider DRE voting systems a national security risk.

In another disturbing example of electronic vote hacking, the Washington D.C. Board of Elections and Ethics was forced to suspend an internet voting trial after the system was successfully hacked by a group of University of Michigan computer science students. *See Hacker Infiltration Ends D.C. Online Voting Trial*, October 7, 2011, at http://voices.washingtonpost.com/debonis/2010/10/hacker_infiltration_ends_dc_on.html. The online voting system was designed to allow military service members living abroad the opportunity to vote online. In fact, a member of the D.C. Board of Elections and Ethics invited would-be hackers to "give it your best shot," at hacking into the system. *See id.* The University of Michigan students did just that. The students hacked into the internet-based system and rigged the system such that after a voter cast his or her vote, the University of Michigan fight song, *The Victors*, immediately began playing for the voter. *See id.* While Colorado currently does not have online voting, long standing and widely documented threats to the primitive security of DRE electronic voting are real and problematic. As a result, states such as Colorado should be amending their election rules and conditions of use for DREs to make them more rigorous and tighter, not weakening and loosening them as Secretary Gessler proposes to do with his changes to Election Rule 43.

## III. THE PRELIMINARY DRAFT OF POTENTIAL REVISIONS TO ELECTION RULE 43 WILL MAKE COLORADO ELECTIONS LESS SECURE, LESS UNIFORM AND LESS TRANSPARENT TO THE POINT THAT THE PROPOSED CHANGES INVITE VOTING FRAUD.

### A. Proposed Changes to Colorado's Election Rule 43

There are several major areas of responsibility and accountability that are absent from the proposed revisions to Election Rule 43 circulated by Secretary Gessler. These changes show a lack of concern for the integrity of the voting process, and if implemented, the revisions make it easier for vote tampering to go undetected.

#### *1. Relaxed Security Plan Requirements*

Under both the current version and the proposed version of Rule 43, counties are required to file a security plan with the Secretary of State annually. Although the components of this report remain generally the same, in Secretary Gessler's proposed version of Rule 43, some

important changes in the proposed version of Rule 43 would allow counties to provide a much less rigorous analysis of their security issues. The current version of the rule states that a security plan must "provide a point-by-point detailed response with a proposed solution to each of the requirements set forth in this rule." *See* Proposed Changes, Section 43.2, p. 2. The proposed version deletes this specific requirement, and simply states that a plan must be submitted, apparently with whatever information a County Clerk decides is relevant for whatever reason.

There is no reason articulated by Secretary Gessler as to why the Annual Security Plan submitted by the County Clerks should not "meet or exceed the standards set forth in [the] article." Removing this requirement simply extinguishes the reasonable bar that is currently set for the County Clerks' Annual Security Plan.

2. *Relaxed Physical Security Requirements*

Both the current and proposed versions of the rule involve the use of serial-numbered, tamper-proof seals on DREs and other voting equipment. But the proposed version compromises how security is to be maintained using these seals.

First, the version proposed by Secretary Gessler states that "[i]f a seal is inaccessible and cannot be removed, then it is not necessary to verify that seal serial number." Proposed Changes, Section 43.2.2, p. 3. This cryptic instruction is likely to result in compromised security. Who decides that a seal is inaccessible and cannot be removed? County election officials or a creative hacker doing his best to beat the system? And if the seal is not verified, then what is the purpose of even having it placed on the machine?

Second, in the current version of the rule, at least one seal is to be placed on all four sides of the seam connecting the two sides of the case containing the electronic components of the voting machine. Proposed Changes, Current Section 43.8.24(a)(iii), p. 4. In contrast, the proposed version requires that "[s]eals shall be used at <u>either</u> the seams of the case <u>or</u> at key entry points such as screw access points." Proposed Changes, Section 2.2(A)(3), p. 4 (emphasis added). Rewriting the rule in this disjunctive and subjective way, and with no requirements regarding mandatory requirements for placement of numbered seals, could lead to a significant decrease in security. For instance, what if seals are placed only over screw access points, but a hacker simply compromises the lock to open the case? If there are no seals on the seams, such tampering would go undetected. This is contrary to the minimum standards published by the scientists and security experts for the Argonne National laboratory. *See* Exhibit 3 attached hereto.

Additionally, <u>both</u> versions of this rule only require these tamper-proof seals if the "firmware or software hash value" cannot be verified. The type of hacking recently demonstrated was accomplished remotely and was only detected because the hackers reported what they had done. It seems that even the current version of the rule does not offer adequate

protection against remote, wireless hacking, which is clearly a real and credible risk. In light of the undisputed and widespread evidence (including evidence from computer scientists from Rice University and the University of Iowa presented in open court in the *Conroy* trial) that DREs are vulnerable to hacking, the Secretary should be focused on tightening the security measures in Rule 43, not loosening them.

Third, the current version of Rule 43 contains stringent security measures relating to which county employees can access the storage area for voting equipment and the mail-in ballot counting area. Proposed Changes, Current Section 43.8.3.3, p. 6. While the proposed revisions on page 6 contain largely the same security measures regarding access to voting equipment, a county may now simply "request" from Secretary Gessler an "exemption" from all of the requirements in the event of "extreme circumstance." Proposed Changes, Section 2.3(C)(2), p. 6. There is no explanation of what an "extreme circumstance" might be, and there is no reason given for providing the counties and the Secretary with the unfettered right to arbitrarily and capriciously declare that so-called "extreme circumstances" exist, or how any concerned member of the public could be made aware that an exemption had been requested. This is a giant potential loophole.

Fourth, on page 7 of the Proposed Changes, the requirement that video surveillance be "continuous" is deleted. The definition section, on page 1 – 2, elaborates that "non-continuous" recording is acceptable, so long as the "detector response" is evaluated every 15 seconds. We need to understand why this change is proposed and the practical security implications of, and reasons for, this dubious change.

*3. Relaxed Inspection Requirements*

Several of the proposed changes would eliminate important responsibilities of the Secretary with respect to monitoring the integrity of Colorado's voting system.

The current version of Rule 43.8.6.1(e) states that "[t]he Secretary of State shall be required to inspect the counties' maintenance records" for a small percentage of randomly-selected voting devices. Proposed Changes, Current Section 43.8.6.1(e), p. 9 (emphasis added). The proposed version makes this affirmative requirement permissive: "The Secretary of State may inspect a county's maintenance records . . . ." Proposed Changes, Section 3.2.6(E), p. 9 (emphasis added). Apart from changing a requirement from a mandatory requirement to a mere grant of permission, the current wording requires random inspections, which motivate County Clerks to keep careful maintenance records. The proposed wording arguably eliminates all inspections by the Secretary, which is a clear signal to the counties that the current mandatory requirement, like much of Rule 43, has been relaxed, if not practically eliminated.

*4. Relaxed Reporting Requirements to the Secretary of State*

Beyond trying to reduce the Secretary's duty to inspect and ensure the integrity of the voting process, Secretary Gessler's proposed changes eliminate the security reporting that he would receive from the counties.

For example, in the current version of the rule, Section 43.8.11.1, Remedies, requires that if an election judge notices that a seal has been broken or if there is a serial number discrepancy on the voting equipment, the judge is to immediately alert the County Clerk and then that person "shall investigate and report the incident to the Secretary of State...." Proposed Changes, Current Section 43.8.11.1, p. 15. The proposed revision eliminates the reporting of the potential security breach to the Secretary of State and instead the County Clerk must conduct an "internal investigation" and only if the County Clerk "is unable to determine why a seal was broken or why a discrepancy exists in a chain-of-custody log" must the clerk file an incident report with the Secretary. Proposed Changes, Section 3.2.11(A) and (B), p. 15. Therefore, if the County Clerk is notified of a broken seal, and learns that the machine was potentially hacked, he or she would not need to report that incident to the Secretary and instead would only need to conduct an internal investigation. This would leave discretion as to whether a security violation had occurred to the counties who do not necessarily have either the resources or expertise to perform such an investigation. Any potential hacking incident would not be reported to a central location. This, of course, makes no sense and should not be the new version of Rule 43.

Further, Rule 43 currently requires specific actions be taken if suspected tampering occurred before, during, or after the voting period. But in each of these sections the proposed changes, the requirement that a report be submitted to the Secretary is deleted. With no mandatory reporting or oversight, the use of the dubious DREs is essentially unsupervised and unchecked and any acts of local, systemic, or statewide fraud would easily go unreported and undetected.

Additionally, in the current version of the rule, each county is required to submit a written report "addressing the existence or absence of any security issues related to the implementation and operation of the voting system" to the Secretary before that county can submit certified voting results. Proposed Changes, Current Section 43.8.11.4, p. 18. The proposed changes simply delete this provision. Like the other changes proposed, this is a blatant relaxation of provisions designed to protect the integrity of Colorado elections.

Under the current version of Rule 43, if serious equipment failure occurs, a polling place must contact the Secretary of State to obtain authorization for the use of provisional or mail-in ballots. Proposed Changes, Current Section 43.8.8.2, p. 12. If the proposed changes take effect, a polling place must simply notify the Secretary that they are going to use these replacement ballots—thus relieving the Secretary of any responsibility while leaving all decisions in the hands of the County Clerks. This change also diminishes a key source of state-wide data on the performance, or lack of performance, of the dubious DREs because the County Clerk may never explain to the Secretary why the county is suddenly switching to provisional or mail-in ballots.

### B. Conditions of Use of DREs

Secretary Gessler's Notice also included a preliminary draft of "revised Conditions of Use" for each of the four types of DREs currently in use in Colorado. In contrast to the changes to Election Rule 43, changes to these documents are not indicated in any manner that we could discern (i.e., there are no additions in SMALL CAPS or deletions in ~~strikethrough~~). Moreover, after reviewing the four sets of proposed changes on the Conditions of Use and comparing the proposed versions with the versions currently in place, the proposed versions are approximately half as long and seemingly far less stringent. The current versions contain diagrams, photographs of proper procedure, etc., while the proposed changes to the Conditions of Use contain nothing of the sort. Further, there is no explanation as to why the changes to the Conditions of Use are needed, or why the content is now suddenly half of the current Conditions of Use.

The Conditions of Use documents are technical in nature and address the specific configuration and capabilities of the four DREs in use in Colorado. The Conditions of Use were adopted by the 2008 Testing Board and were mandatory to protect against "significant weakness in security, auditability, integrity and availability of the voting system" for each of the four DRE voting systems.

For these reasons, we are not able to analyze the effect of any proposed changes to the Conditions of Use at this time. Nonetheless, even with a limited understanding of these machines, and of what changes, if any, are proposed in these new and drastically shortened proposed versions, it is troubling to see the Secretary apparently relaxing and, in some cases, eliminating security Conditions of Use for DRE electronic voting systems that were mandatory and required by the Testing Board operating under a legislative mandate in 2008.

## IV. CONCLUSION

Vote tampering and DRE hacking risks have increased, as proved by a group of scientists from the Nuclear Engineering Division of the Argonne National Laboratory. DRE technology that was substandard in 2006 has not kept pace with other advances in computer science and invasive technology. It is naive in the extreme to assume that there will be no games played with our elections. A hacker could be a Republican, a Democrat, a third party activist, a teenager having fun on election day, or a member of a terrorist group seeking to wreak havoc with a cornerstone of our democracy—the right to vote in a fair and democratic election.

In these uncertain technological times, and with DREs in use in Colorado until at least 2014, the Secretary should be strengthening Election Rule 43 and the conditions of use of dubious DRE voting systems. The Secretary should be taking on more responsibility for overseeing free, fair, secure, and safe elections in Colorado. However, Secretary Gessler's proposed changes to Election Rule 43 ignore the security risks that exist, and propose to abrogate many of the Secretary's duties while relaxing and eliminating security measures under the

current version of Rule 43 and the Conditions of Use for DREs. One can only speculate what is behind the proposed changes.

The proposed changes to Election Rule 43 should be immediately discarded and any future proposed changes should bolster DRE and overall election security, not diminish it.

# Problems With Secretary Gessler's Proposed Revisions to Election Rule 43 and Conditions of Use for DREs

Electors: Myriah Conroy and Jeffrey Sherman

Submitted by Counsel: Paul Hultin and Matt Johnson

Wheeler Trigg O'Donnell LLP

1801 California Street | Suite 3600 | Denver, Colorado 80202-2617 | P 303.244.1800 | F 303.244.1879 | wtotrial.com

# Secretary Gessler's Office Claims it is Committed To Security of Dubious DREs

- December 6, 2011 email from Andrea Gyger of Secretary Gessler's office stated:

*… we are committed to maintaining the same level of security as currently exists, and believe the proposed changes will do so while making it easier for all counties to understand and follow the procedures…*

*Thank you,*
*Andrea*

# Contrary to the Self-Serving 12/6/11 Email, the Proposed Rule 43 Changes Compromise and Eliminate DRE Security

WheelerTriggO'Donnell LLP

# History of Security Problems with DREs in Colorado

- Ms. Conroy, Mr. Sherman and others filed suit against Secretary of State Dennis in 2006.
- Secretary of State's Office was ignoring its statutory duties to protect the integrity of Colorado's elections.
- After 3-Day Trial: Denver District Court Rules in favor of Plaintiff Electors.

# Denver District Court Order

- Secretary did not follow law relating to certification of DREs.
- Secretary ordered to promulgate minimum security standards for DREs.
- Secretary ordered to retest DREs using revised minimum security standards.
- Secretary ordered to require counties to implement minimum DRE security standards and procedures (Rule 43).

# Three of Four DRE Systems Decertified

- After adopting minimum security standards and retesting pursuant to Court Order, the Secretary decertified three of the four DRE systems in late 2007.

# Election Reform Commission is Created in 2008

- Following *Conroy,* S.B. 08-243 set up the Election Reform Commission (ERC) in November 2008.
- Secretary Gessler and Mr. Hultin were members.
- After many public hearings, ERC Recommends 20 changes to election laws in Colorado in its final report.
- Recommendations Nos. 7 and 8 address DRE ERC Security Problems (relevant excerpts attached).

# House Bill 09-1335 Becomes Law in 2009

- Following the ERC's Final Report, HB 1335 Becomes Law Enacting Certain Recommendations from the Commission.
- DREs to be phased out of elections in Colorado by 2014.
- Voter verified paper audit required for use with DREs.
- Risk-based audits of DREs required to mitigate risk of election fraud because of easily hackable DREs.

# Scientific Evidence that DREs Are Unsecure Continues to Mount

- Argonne National Laboratory Scientists Complete "Man in the Middle" hack of DREs from half-mile away with $26.00 of off-the-shelf equipment.

- University of Michigan students hack into Washington D.C. internet voting system and program electronic voting machines to play *The Victors* (U of M Fight Song) when a voter registers vote.

- Argonne National Lab has proposed minimum DRE security standards which proposed Rule 43 will not meet (copy of Argonne report attached hereto).

# Examples of Rule 43 Changes Which Compromise Election Security and Integrity

| | |
|---|---|
| **Current:** Counties Must Provide Point-By-Point Annual Security Plan to Comply with Rule 43. | **Proposed:** Eliminates Requirement that Annual Security Plan Comply with Specific Requirements of Rule 43. |
| **Current:** Tamper-proof "seals" placed on all four sides of the DRE seams containing electronic components. | **Proposed:** Tamper-proof "seals" used on seams OR on screw access points (allows for lock tampering, etc. if no seal on all seams). |

# Examples of Rule 43 Changes That Compromise Election Security and Integrity

| | |
|---|---|
| **Current:** Secretary of State ***shall*** inspect counties' maintenance records regarding DREs. | **Proposed:** Secretary of State ***may*** inspect counties' maintenance records regarding DREs. |
| **Current:** If an election judge notices a seal is broken or serial numbers don't match up, Clerk ***must*** report incident to Secretary. | **Proposed:** If an election judge notices a seal is broken or serial numbers don't match up, Clerk not required to report incident. |

## Proposed Changes to Conditions of Use Make No Sense

| | |
|---|---|
| **Current:** Each of the four sets of Conditions of Use were created by the 2008 Testing Board of Experts who developed the new security standards and re-tested DREs. | **Proposed:** Unclear which "experts," if any, drafted new Conditions of Use and what testing, if any, was done. |
| **Current:** Each DRE has approximately 10 pages of Conditions of Use which are highly technical security provisions. | **Proposed:** Cuts Conditions of Use down to 3 to 5 pages – no reason given. No explanation of what was eliminated and why certain conditions were eliminated. |
| **Current:** Diagrams, photos, explanations, etc., included for better understanding by County officials of security requirements. | **Proposed:** Text only, no visual guidance for Conditions of Use – more confusing, less helpful. |

## Proposed Changes to Conditions of Use Not Explained

- No red-line provided which shows changes from current Conditions of Use.
- No description of any testing or other scientific work justifying changes to current Conditions of Use provided.
- In the absence of this information the proposed Conditions of Use are unintelligible.

# Conclusion

- Colorado Secretary of State's Office has a five year history of ignoring security risks created by defective DREs.
- Secretary Gessler's proposed changes exacerbate this long-standing problem.
- DRE hacking is a real and present national security threat as Argonne National Laboratory Scientists recently demonstrated.
- Secretary Gessler should be strengthening Election Rule 43 to mitigate the risks of hacking of vulnerable DREs, not weakening Rule 43.
- Election Integrity is put at risk by proposed Rule 43 Changes.

# Election Reform Commission

## Members of the Commission

Senator Ken Gordon, Chair
Bill Hobbs, Deputy Secretary of State, Vice-Chair

Bob Balink, El Paso County Clerk
Mark Baisley, President/CEO, Slipglass
Scott Doyle, Larimer County Clerk
Scott Gessler, Attorney, Hackstaff Gessler
Paul Hultin, Attorney, Wheeler, Trigg, Kennedy
Scott Martinez, Attorney, Holland and Hart
Sally Misare, Castle Rock Town Clerk
Patti Nickell, Bent County Clerk
Stephanie O'Malley, Denver County Clerk

## Legislative Council Staff

Bo Pogue, Research Associate
Kurt Morrison, Senior Legislative Assistant

**Recommendation #4 – Assisted Living Facilities**

The commission recommends that the General Assembly consider legislation to exempt persons living in assisted living or nursing care facilities from identification requirements for voting. In addition, the commission recommends the use of the Secretary of State's rules to ensure consistent application of regulations pertaining to identifying residents of assisted living or nursing care facilities for elections-related purposes.

**Recommendation #5 – Verification Period for UOCAVA and ID-deficient Voters**

The commission recommends legislation to expand the current eight-day post-election signature verification period to allow for continued receipt of ballots from overseas voters under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), while maintaining the requirement that the ballots be postmarked no later than 7 p.m. on election day, where postmarks are applicable. The commission also recommends providing identification to voters who are identification-deficient.

**Recommendation #6 – National Voter Registration Database**

A national voter registration database would eliminate the possibility of citizens registering to vote in more than one jurisdiction.

The commission recommends that Colorado participate in the implementation of a national voter registration database.

## Technology and Auditing

**Recommendation #7 – Voting system certification**

After the Secretary of State's December 2007 decertification of the electronic voting systems (EVS) used by the majority of Colorado counties, Governor Ritter signed into law House Bill 08-1155, which provided for retesting and interim re-certification of any decertified voting machines. Under current law, the provisions of the bill are repealed on July 1, 2009, resulting in the decertification of systems certified under the bill. Extending the interim emergency certifications allowed for in HB 08-1155 will provide financial relief to cash-strapped counties and ample time to phase in the next generation of technology.

The commission recommends legislation to amend the statutes on voting system certification as follows:

- ***House Bill 08-1155.*** Extend the interim emergency certifications provided for in House Bill 08-1155 through the 2013 election cycle. Under this recommendation, use of currently certified EVS would be allowed through the 2013 election cycle, subject to all conditions that attached to the 2007 and 2008 certifications of such EVS.

- ***Voter-verified paper audit trails (VVPATs).*** Repeal the requirement that all direct recording electronic (DRE) voting equipment have voter-verified audit trails (VVPATs) by 2010. Jefferson and Arapahoe counties will not have to perform expensive short-term retrofits on DREs not currently equipped with VVPATs.

- ***Paper ballot/optical scan-based EVS.*** For all elections after the 2013 election cycle, and for all new electronic voting systems purchased and utilized before the 2013 election cycle, require all counties to utilize a paper ballot/optical scan-based electronic voting system that has been certified under the revised procedures recommended below.

- ***Certification of paper ballot/optical scan-based system and modification of EVS whose certifications have been extended.*** (applies to all new EVS and modifications to certified EVS)

  - repeal requirement that all EVS must be tested and certified as meeting current federal standards;

  - allow EVS whose certifications are extended through the 2013 election cycle to be modified subject to testing and certification by the Secretary of State that the systems, as modified, meet all Colorado testing and certification requirements;

  - change the testing and certification completion requirement in Section 1-5-617 (1)(c), C.R.S., from 90 days to 180 days; and

  - allow the Secretary of State to utilize and rely upon testing done by another state's secretary of state or chief election official, or by a federally certified testing lab, provided that the Colorado Secretary of State has complete access to all test documentation, test data, and test reports, and provided that the Colorado Secretary of State makes written findings and certifies that (1) he or she has reviewed the test documentation, data, and reports and finds that the testing has been conducted in accordance with state-of-the-art engineering standards and practices; and (2) the testing met each applicable Colorado requirement.

**Recommendation #8 – Post-election audits**

The commission recommends legislation to revise the statutory requirements for post-election audits in Section 1-7-514, C.R.S., to require a risk-based audit methodology instead of the current fixed-percent audit. All aspects of each election, whether mail-in voting, early voting, election day voting, or other, should be subject to the same audit requirements. In addition, the commission recommends the following:

- require all voting systems to report votes in auditable batches;

- define the confidence level required, e.g. 90 percent or some lesser confidence level;

- require audit units to be randomly selected;

- require the audit process to be transparent;

- require audit processes to be developed for each voting system in Colorado and accomplished in a way that is easily understood by public officials charged with completing the work;

- set out in statute the general requirements, standards, and procedures for a risk-based audit; and

- require the Secretary of State to implement risk-based election audits by notice and comment rule-making, resulting in a new election rule giving guidance to the counties as to the specific requirements, standards, and procedures to be followed.

## Uniformity and Simplification

The Election Reform Commission feels that certain areas within the elections environment are primed for uniform and consistent practices. While the commission recognizes the need for designated election officials to have flexibility in deciding how best to deliver elections in their respective counties, a need exists to have consistent practices where there is an opportunity to curtail voter confusion.

### Recommendation #9 – Mail Ballot Elections

The commission recommends legislation to allow counties the option to conduct primary elections by mail, if the legislation contains the following requirements:

- ***Minimum threshold.*** Before an all-mail ballot election is allowed, the absentee voter participation in the county must exceed 50 percent of all active voters in the previous presidential or gubernatorial election.

- ***Service centers.*** Counties conducting elections by mail must include a sufficient number of service centers established by formula. The service centers must provide consistent services to the voting public, and each service center must have secured computer access, be Americans with Disabilities Act-compliant, include a sufficient number of DREs, include a sufficient number of voting booths, have the ability to distribute second original ballots, have the ability to distribute replacement ballots, serve as a ballot drop-off location, and provide the ability to register in an emergency manner. In addition, the legislation must:

  - require minimum hours of operation and number of days open prior to election day;

  - require service centers to be available during early voting; and

  - require designated election officials to determine the number, location, and manner of operation of service centers, including poll watching activities at service centers, in consultation with the chairpersons of the county central committees of the major political parties and representatives of the minor political parties, and after a public comment period of no less than 15 days and a public hearing held in accordance with the rules adopted by the Secretary of State.

- ***Election preparation.*** Designated election officials must meet with an election vendor to determine whether the vendor has the ability to provide sufficient mail ballots in a timely manner, and meet with the U.S. Postal Service to coordinate ballot mailing, receiving, and tracking.

- ***Voter eligibility.*** The legislation must include language specifically mandating who is to receive mail ballots. The language must include direction to the designated election official that he or she mail to all registered voters, mail to all active voters, or that the

Argonne NATIONAL LABORATORY | Nuclear Engineering Division

# Suggestions for Better Election Security

*From the Vulnerability Assessment Team at 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, examine, 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.

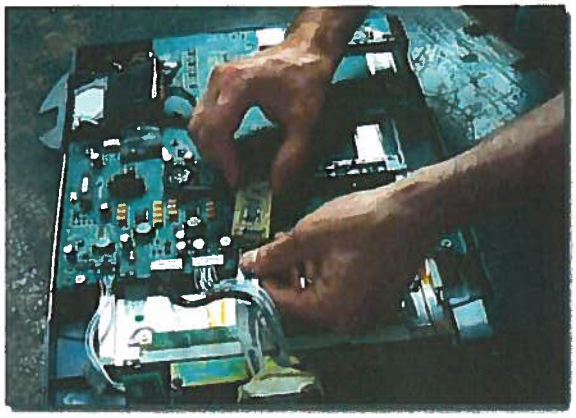
6. A poor security culture, including denial and no *a priori* procedures for dealing with security questions or concerns.

## About These Suggestions

The following suggestions for better election security are from the Vulnerability Assessment Team (VAT) at Argonne National Laboratory (http://www.ne.anl.gov/capabilities/vat). 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.

## 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.



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

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

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 inspection (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 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

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Argonne National Laboratory, 9700 South Cass Avenue, Lemont, IL 60439

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).

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Argonne National Laboratory, 9700 South Cass Avenue, Lemont, IL 60439

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.

## About the Vulnerability Assessment Team

The Vulnerability Assessment Team (VAT) at Argonne National Laboratory has conducted vulnerability assessments on approximately 1000 different physical security and nuclear safeguards devices, systems, and programs. This includes analyzing locks, anti-counterfeiting tags, tamper-indicating seals, RFIDs, GPS, microprocessor systems, contact memory buttons, electronic voting machines, nuclear safeguards equipment, and biometrics and other access control devices. The VAT has demonstrated how all these technologies can be easily defeated using widely available tools, materials, and supplies, but has also devised and demonstrated simple and practical countermeasures.

In addition, the VAT has provided security consulting, training, R&D, specialty field tools, and novel security devices and approaches for more than 50 different companies, NGOs, and

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Argonne National Laboratory, 9700 South Cass Avenue, Lemont, IL 60439

government organizations, including DoD, NNSA, DHS, U.S. Department of State, the International Atomic Energy Agency (IAEA), Euratom, and intelligence agencies.

VAT personnel have given over 80 invited talks (including 6 Keynote Addresses) at national and international conferences.

The VAT is frequently interviewed by journalists and security bloggers about its work and its views on security. See, for example:

"Diebold Voting Machines Can Be Hacked by Remote Control", http://www.salon.com/news/2012_elections/index.html?story=/politics/elections/2011/09/27/votinghack

Bradblog.com, http://www.bradblog.com/?p=8785, http://www.bradblog.com/?p=8790, http://www.bradblog.com/?p=8818

"Most Security Measures Easy to Breach", http://www.youtube.com/watch?v=frBBGJqkz9E

"Roger Johnston on Election Security", http://www.opednews.com/articles/Argonne-Lab-s-Head-of-Vuln-by-Joan-Brunwasser-110329-968.html

"Getting Paid to Break Into Things: How Vulnerability Assessors Work at Argonne National Lab", http://www.techrepublic.com/blog/security/getting-paid-to-break-into-things-how-vulnerability-assessors-work-at-argonne-national-lab/5072?tag=mantle_skin;content

"Closing the Curtains on 'Security Theater'", http://www.smartplanet.com/technology/blog/science-scope/at-argonne-national-lab-closing-the-curtains-on-security-theater/5167/

"Digital Privacy: Are You Ever Alone?", http://news.medill.northwestern.edu/chicago/news.aspx?id=187163

"Six Rising Threats from CyberCriminals", http://www.computerworld.com/s/article/9216603/Six_rising_threats_from_cybercriminals

"Roger Johnston on Security Vulnerabilities of Electronic Voting", http://blog.verifiedvoting.org/2010/10/15/1131

"Phishing Attacks: Training Tips To Keep Your Users Vigilant", http://www.techrepublic.com/blog/security/phishing-attacks-training-tips-to-keep-your-users-vigilant/5402

Roger Johnston interviewed live on WTTW Public Television's "Chicago Tonight" program about electronic voting machines, http://www.wttw.com/main.taf?p=42,8,80&pid=BMeOsuVOgSUbQammoGQxMIIX00avS55H

"IT Security: Maxims for the Ages", http://blogs.techrepublic.com.com/security/?p=2435

"Security Maxims", *Security Now!* Podcast #215, http://www.grc.com/sn/sn-215.htm

"Vulnerability Assessment's Big Picture", CSO Magazine, http://www.csoonline.com/read/060107/fea_qa.html

*Argonne National Laboratory*

## About Argonne National Laboratory

Argonne National Laboratory, the nation's first national laboratory, is one of the U.S. Department of Energy's largest national laboratories for science and engineering research. It is located 25 miles from downtown Chicago. Argonne is managed by UChicago, LLC, for the United States Department of Energy.

Argonne has approximately 3,400 employees, including 1,100 scientists and engineers, three-quarters of whom hold doctoral degrees. Argonne's annual operating budget exceeds $738 million.

Since 1990, Argonne has worked with more than 700 companies, federal agencies, and other organizations.

Argonne NATIONAL LABORATORY

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Argonne National Laboratory, 9700 South Cass Avenue, Lemont, IL 60439