

Sunday Session

Summary Slide Show

Supporting Concepts/Quotes Slide

Carey: From perspective of voter, it's not 2x, it's equivalent.

Jefferson: Completely disagree. Voter would prefer to be disenfranchised rather than having the vote flipped.

EOs in Room: Voters don't want to see either case.

Walker: Voters intend to cast a vote, and if it doesn't happen, it doesn't matter whether it was flipped or not. I would be pissed off either way, whether it was flipped or destroyed.

Carey: Impact of changing vote is greater than impact of losing vote. But don't dismiss the lost vote because it's only half as bad. Don't dismiss disenfranchisement.

Simons: From my voter's perspective switching vote is far worse. It's a binary math issue.

Carey: For the voter, it might be more like 20% risk of switching, and 80% risk of vote cast as intended. Compare that to 100% risk of vote not counting at all.

Keller: Everyone agrees that disenfranchising military voters is bad. We can't equate that to actual fraud. (applause in room). Second issue is related to auditing. Risk limiting audits – factor of 2 is important: losing a vote has half the potency in this type of audit than switching a vote. Let's focus on enfranchisement and figure out where the pitfalls are and fix in priority order with the most effective first.

Lux: Math of this being a factor of 2 can't be denied. But the difference between flipping and disenfranchisement is that I don't get to vote on any race on my ballot if I'm disenfranchised, and not just the race that got flipped.

Jefferson: Group was assembled to do quantitative estimates, and that's what we're trying to give you. And it's actually more than a factor of 2, because it would not be a random sample of the population (ie: flipped votes not equally divided between candidates).

Soper: I want to see everyone be able to exercise their right to vote. Recently saw 2 bills in California: email voting (which got defeated) and procedural changes (as long as its postmarked on election day, voters have 10 days to get it back). The procedural changes part is important. I don't want to see us enfranchising the Chinese. That's the worst case, and we have to cancel the election. And that's not an option in the United States. Let's not open up our election system to hacking, ala Washington D.C. That proved that we can't protect this in real life.

Kaplan: We should have multiple channels and be able to verify both channels. Vote by web on secure network AND submit signed votes by mail. That would be a study, and you could compare results like in a clinical trial and do auditing.

Facilitator: Let's move on, trust the facilitator to bring out some of these issues later on in the slide show.

Properties EO Slide

Lux: More concerned about ability to integrate data, not the systems. Election management systems should stand alone to be protected, but data and results need to be integrated.

Benaloh: Explains his 4 properties:

Integrity (correctness of the tally).

Privacy (protection from coercion, vote selling, etc).

Availability of system (won't crash, lack of disenfranchisement).

Usability (ease of use, transparency, see what's going on and understanding that things are going properly)

Properties Saboteur Slide

Peterson: Wholesale vs. retail: in current system massive fraud is very difficult. In electronic system, the opportunities are there for big changes if you can get in at all.

Epstein: Register Mickey Mouse x 1000, that's a pain in the neck for EO, but doable to sort out the bad eggs. But once you can do it electronically, you can do a million, and EOs have to look at each one.

Jefferson: You can also do wholesale attacks without getting into the system.

Andel: If EOs not accurate in registration, you don't need to do anything else.

Carey: Does taking registration out of electronic mitigate these risks?

Patrick: But taking away online registration doesn't maintain the level of rights for UOCAVA/FPCA voters as other voters in CONUS.

Carey: More DMZ is a plus for the saboteur?

Burris: Yes. Because people don't know how to use DMZ well.

McBurnett: Closed source posted on the internet is worse than open source to start with.

Risks Slides

Rothschild: Broader view of risk is more of an issue for Congress than for FVAP.

Franks: Controlling expectations is going to be very important for FVAP.

Myung: FVAP needs to communicate the slippery slope.

Keller: Look at lessons of ADA(?). Language that was developed for specific project, but once it existed, there was pressure to use it for more things.

Carey: Demonstration project was mandated by NDAA 2002/2005, and MOVE Act mandated pilot projects to support the demonstration project.

Keller: How do you distinguish between what is demo and what is pilot?

Rothschild: Demo is internet voting, pilots lead up to that.

Carey: The final project is the demonstration mandated by 2002/2005. Everything else we do is classified as pilot.

Keller: Demos in vendor world are not in a live election. If that's what you plan, you won't get too much objection from the room.

Hancock: Don't assume that Congress knew that when they wrote those two different words – it's semantics.

Carey: We just took labeling from the law. Pilot projects are not live, but demo project is return of ballots in a regularly scheduled general election.

Carey: Regarding a more narrow context/architecture slide. Having difficulty understanding slide.

Rocket to moon analogy. Want to get there and back safely is one context. Other alternative is take

what I currently have and see how far that will take me safely. In the military we take best practices and use them because we have to achieve our mission. I don't think this falls into that category. I'm willing to wait until I know I can get there and back safely, rather than take what we have and try.

Walker: That doesn't absolve you from the considerations on the slide.

Carey: First define the problem, and then figure out courses of action that will meet it. At some point we're going to launch. Do you do this after you define the risk?

Walker: It's an imbedded process. There are risks from start to finish, and you need to identify those risks. Slide is saying this needs to be done no matter what stage you are in. Need to assess the risks with goals and objectives, and that requires architecture.

Carey: Measure numerous architectures against risks?

Walker: We can't measure risks against future tech that exists tomorrow.

Carey: But can you say what level of risk you're willing to accept.

Walker: That's not a concrete risk assessment, it's pulling it out of the sky.

Carey: Do properties change based on level of risk you're willing to accept.

Franks: Getting a wing of aircraft would change your risk assessments in the military, if previously you only had tanks.

Walker: It's a cyclical process, new tech changes your risk profile.

Hancock: Goals of law are to enfranchise military voters.

Carey: Goal is to test internet voting.

Hancock: But why? Congress asked you to take out a sniper at a 1000 yards with a muzzleloader instead of a 50 caliber. They dictated your tech.

Carey: Commander says to company "take out the sniper, I want it done." Or Commander says "we're not going to move until we can guarantee 0 casualties."

Walker: Risk profile changes with MacGyver and a butter knife vs. Gomer Pyle with a butter knife.

Keller: If we define the goal as to enfranchise every military voter, then everybody agrees.

Benaloh: That's hopeless.

Keller: Real goal should be to raise the number – to make as many military vote as is feasible. Problem is that Congress has decided on a particular mechanism. Goal is to go to moon, and Congress told us what rocket to use. Where we are is that the community wants to help military vote. We all agree with the goal. It's possible for FVAP to say: we will do what we can with the best available technology, but remove the requirement for that to be electronic ballots. Risks were not that well known in 2002 – we should advise Congress to change the law, and some of us want FVAP to tell Congress that.

Simons: Estonia vs. D.C., were people saying Estonia is secure?

Epstein: No. Subtle difference between the 2 systems in the details. But the result is that Estonia is less insecure.

Simons: I'm not convinced of that.

Takeaways Slide

Carey: Next steps before demo project, or after?

Franks: Next steps after today

Open Discussion

Carey: Impressed with level of work, detail, and energy. Appreciates everyone's efforts and commenting. Regarding timeline: March 12th. Looking to use EAC's and NIST's risk assessment tools to do risk analysis of current system (electronic transmission of black ballot, 45 day return window, etc). Question regarding alternative proposed risk equation (damage/cost). Does the EAC tool/NIST tool provide sufficient capability to do that type of risk assessment? We need a method to compare risk between current and future systems – we're not wedded to any specific method. But we need a risk assessment of current system to compare, it's a key first step we need to have to evaluate future systems, and we don't have it.

3 key questions that need to be answered from today:

1. Do EAC/NIST risk assessment systems properly integrate the damage/cost model?
2. Is it a widespread belief that we need to have specific architecture to develop high-level guidelines or assess risk? (Carey thinking risks →guidelines→architecture)
3. When does the internet stop becoming the internet? Data from JWIGS transmits over open internet lines, but is very highly encrypted. Is that still the internet? If we establish DZN, is that still the internet?

Regarding question 1 (EAC/NIST risk assessment tools and the alternate risk equation)

Miller: EAC tool is a probability tool, and I was dismayed to see it.

Carey: Is there an applicable tool that uses alternative risk analysis?

Regarding question 2 (need for specific architecture):

Walker: There's a difference between guidelines and risk. We need to consider risk tolerance of user/voter as well. When you talk about democracy/freedom/voting and compare against banking online, people are more likely to do the latter, because there are remedies for getting money back, but not for getting vote back. So risk tolerance for voting is lower.

Jones: EAC came out to with guidelines that don't have architecture. But there are always implicit assumptions before you have anything testable. Need to know how info flows through system before you can evaluate risk. So need architecture for a useful risk assessment.

Carey: TGDC don't put standards against variables?

Jones: No. You need guidelines in order to frame development of architecture, because they give you goals to aspire to. Standards are an end point, you have to produce them before you build the architecture.

Carey: Does the architecture change with the level of risk you're willing to accept? So should you define acceptable level of risk in the high level guidelines?

Walker: Yes. It's an iterative, circular process.

Jones: Guidelines don't currently set acceptable risk.

Epstein: You need a threat model for acceptable risk.

Jefferson: Any electronic voting system that does not exceed in risk the current system – let's set that as ground rule. So look at costs to swing 1000 votes in current system, and use that as the metric for

comparison for proposed architectures, and look at the lowest cost it would take to do the same amount of damage. If there's a lower cost to swing those 1000 for the electronic system, reject it, if there's a higher cost, accept that electronic system.

Benaloh: Goal of any security-based system is to make the cost to an attacker less than the monetary benefit derived by the attacker (cost of hack/monetary benefit of hack). If equation total is less than one, probability of an attack is basically 0, if the cost is more than 1, then probability of an attack is basically 100%.

Carey: So is the proposed risk analysis equation going about it the right way, and will it provide us adequate data to assign values to high order guidelines?

Benaloh: If you modify the earlier presented equation to what we've been discussing, then yes, you will be able to assign values.

From the room: But what's cost of buying an election official. That's a hard number to assign.

Benaloh: You can't do it precisely enough to submit to an expense report.

From the room: Then how do you assign numbers?

Epstein: There's a paper this week by Joe Hall, myself, etc, that measures value by number of people.

Walker: This argument is based on limited sample space. But you have countries that have military units set up to hack, and their resources are unlimited.

Benaloh: But we can still make it that the cost is higher than the benefit.

Carey: We can do it by time, not cost.

Jefferson: If another state wants to attack the US, they will succeed, and that's why it's so dangerous to do it at all.

Franks redirects conversation: Should we be moving to architectures before we've defined guidelines?

Carey: Can we take high level guidelines and assign high order values to them?

Finely: We need to measure risk in current system, and we keep forgetting that. The definition of the current voting system has been widely inaccurate. EAC's risk analysis tool didn't define the starting and ending points of electronic voting system as the same places as the paper-based/DRE systems. So let's be honest about what it is we are comparing. The return of the voted ballot is a very precise point, and including other steps in the current process is intellectually dishonest.

Carey: I see why you want an architecture to compare now. Could we just do a complete end to end risk assessment of the current voting system with the MOVE Act requirements (blank ballots, 45 days, returning by express mail, no electronic return of voted ballots)? Take that level of risk, and apply that against high level guidelines to get some values in order to influence the architectural development?

Walker: That makes sense from the perspective of arguing your case to the powers that be. But from a more purest perspective, you want to look at the two separately, compare the risks, and decide which you want to tolerate more.

Carey: That's a decision point, and I'm talking about the process level.

Franks: We don't know where we can enter the circle. Once we're on the circle we can get moving, but we need to decide where we enter the circle.

Walker: Congress has suggested the architecture. So we can work backwards to suggest guidelines.

Finely: But FVAP has been arguing that we should only accept the electronic system if it doesn't have a higher level risk than the current system. Military postal system has published their results, and that

shows that for ballot return, 92% percent of overseas ballots in express military mail were delivered within 7 days. If we compare than to the 45 day window to deliver ballots – only 7 ballots from CENTCOM were delivered after 30 days.

Carey: But it takes 1-30 additional days to get from FOB/ship at sea to military post office.

Finely: 30 days plus 7 is still under 45.

Carey: We should define rough order guidelines to do architecture, but then we need to go back and reassess the architecture for better numbers afterwards.

Regenscheid: We don't know how to do it.

From the Room: We don't have baseline numbers of what's wrong with current system either. It's all speculative.

Jefferson: You don't have to estimate cost of all attacks, just the cheapest attack. So forget about the fact that expensive attacks are not estimatable.

Keller: Distinction between detectable and undetectable attacks. Risk factors on those are different. Need to compare costs to other ways that give you the same benefits. Slippery slope – in a military environment a system would have different risks in the outside world. You need an architecture to do an architectural risk assessment. Is it possible to identify all the risks associated with a completely fleshed out architecture. (group – you can't do that with any system ever). But if you can't identify all the risks, you can't quantify them. You can compare risks to existing internet systems and their intrusions. Comparison by analogy. Qualitative assessment, not quantitative.

Walker: The government scrapped a project to build the most secure system ever, because cost was too prohibitive. We can quantify costs to us, instead of quantify risks. Then compare to benefit of providing such a system.

Simons: I'm uncomfortable with quantifying risk. Because it's the presidential U.S. election. There's no cost figure on something like that. We're talking about expectations. Given how insecure the internet is, I don't see how we can move forward with sending voting ballots.

Regarding question 3 (when is the internet not the internet)

Carey: JWICS uses the internet but is secure – is that still the “internet” for purposes of voting?

From the room: Yes, JWICS is the internet.

Jones: Concerned that by connecting LEOs to secure DoD systems, you compromise the DoD system.

Carey: Does establishing VPN between client server and LEO system – is that outside the realm of the internet?

Jones: Link is secure, but end point isn't.

Carey: We could buy LEOs a server (for several jurisdictions, 3000-5000 UOCAVA voters each). It will be NIPRnet only.

Back to question 2 (talking about abstracts or specifics)

Wallach: We're talking about individual pieces, not how we would design a whole system that would incorporate them. It's hard to have these discussions in the abstract. We're going about this discussion the wrong way – We have to know what the overall design is, or we have no idea what we're talking about in terms or risks.

Carey: We need to define *something* first.

Wallach: You can't have discussion in the abstract, we keep going around in circles – here, Chicago, etc, and we don't get anywhere.

Carey: So what do we need to do?

Benaloh: Create requirements and ask people to submit proposals.

Syverson and Sherman: Run a competition. Open process with standards, and any expert can come and comment on it. Gradually move forward from there.

Wallach: Process wherein people are trying to design and present and defend entire architectures against adversarial review.

Franks: We need an initial set of assumptions to start that submission to an open process. That's the guidelines.

Walker: That's the function of the working group here, I think. We need to produce some semblance of guidelines.

Sherman: People are unnecessarily fervent about anti-internet. Yesterday's discussions were maybe excluding good solutions.

Jefferson: Intermediate steps: actual demo should be the last of several steps not held in real election. Architecture competition should be completely open as it goes along – let the security community criticize, then vendors revise, and so on – no proprietary claims. And run demo only on systems that survive that and non-live tests. Most critical piece of instrumentation would be end to end so that we can verify that the demo election was conducted correctly. A process like that is the best that I can offer if you feel compelled to do a demo at all.

Carey: What about security through obscurity? Can the same level of analysis be done if we put folks in this room under government employment to allow for proprietary protection? Or is open source a necessity?

Walker: don't need open source. Obscurity can make an otherwise secure system more secure.

Santos: Employ the best scientists here, we don't need open source. Use the best resources at your disposal, and you need a field test. Set a cost equal to current means. Have a backup channel of mail to protect against risks while we're testing electronic.

Hall: Keep in mind that this is a political decision, not just a technical decision. Make sure each step of the process meets political and public opinion aspect.

Carey: Does it need to be open source?

Benaloh: Design needs to be open, sources don't.

Wallach: Company can have patents/copyrights, but not trade secrecy.

Benaloh: With some systems, at least some of the code does not need to be open to be verified as doing the right thing. End to end systems can verify correct functioning of code without looking at the code.

Simons: Software needs to be available so people can test it during the testing period. Independent testing by Halderman, etc. for non-commercial use.

➔ Group wants disclosed source, not necessarily open source

Carey: Do we need standards to know if the winner is good enough?

Room: We'll know it when we see it. **First determine what the best is, then determine if it's good enough.** Several systems may be best, it could be that none of them are good enough.

Process from the room:

- Demo proceeded by multiple non-live assessments.
- Open competition (X project) that gets many architectures assessed.
- Competition survivors tested in a non-open source way to see how they operate.
- Final live demo is a small controlled experiment with end to end verification technology (not optional).

Regenscheid: AES process: draft criteria were high level guidelines. But voting systems algorithms are more complicated than crypto algorithms. Not sure if we need to set benchmarks, but should set evaluation criteria (posted for comment, then updated). Then each year have a conference, get papers that attacked algorithms. NIST was independent party evaluating attacks, and continued to weed down numbers, went from 63 to 5.

McBurnett: End to end is key. Allows you to have a sense of the quantity of possible attacks. End to end should be lowest bar. Could a system without end to end have lower risk than current system?

Jones: In our room there was consensus that we wanted auditable system, and that any pilot project needs to be measurable to draw conclusions about its success. And an end to end measure is necessary. But there are many end to end measures. But ends have to be well defined. One can be voter intent. And the other end should be when the ballot is turned over into tally in old election management systems. But we can't get to that end because of election law.

Final Thoughts: Vendors/EOs

Lux: 2000 election busted our project, and created a lot of concerns. SERVE got cancelled, but they offered to keep it as a pilot. States said they didn't have time to do that and real election. Voters feel the same way – they don't want to do both paper and electronic. And participation will be minimal in demo projects that aren't live.

From the room: We'll be able to get enough volunteers.

Rothschild: Thanks for coming. Conversation was valuable to FVAP. Put suggestions down on Reflections sheet, or call/email me. Is there a good time for this next year?

EOs – this time next year is bad for us.

Everyone else – this time next year will be good.