Saturday Morning

Teams:

Mr. Red - Andel, Fasmire, Lux, Manion, Aceto, Santos
No Name - Jefferson, Hancock, Regenstein, Holmberg, Pollins, Benaloh, Miller
Southeast Corner- Naujok, Yu, Valentine-Brown, Jones, Soper, Burris, Ramos
Nautilus – Robinson, Syverson, Daviage, Smith, Johnson, Shacham, Joyce, Wagner

Team Discussions of Processes (as Yana wandered from table to table):

Team No Name

Jefferson – wants to do risks first, questions the whole premise behind risk discussion (bob's equation), wants an opportunity to question that, and that informs the rest of the discussion, believes the risk equation is totally wrong
Miller – also questions the equation
Benaloh – risk is simple, it's getting the wrong result
Jefferson – the more electronic votes are sent, the greater the risk, and Bob's arguments are dangerous at any but a negligible scale. Wants bob to say it's a bad idea but we're going to do a small demonstration

Southeast Corner

Ramos – Missing requesting a ballot (between registration and obtain/transmission)
Jones – UOCAVA context doesn't involve certifying and canvassing, the state should be able to apply their own state law in cases where voter sends in a paper ballot and electronic ballot
Soper – 2010 data shows that half the voter registration addresses were incorrect – need a process to update your address (Klaus – that's registration)

Nautilus

Shacham - audits are missing, it's more important than certifying and canvassing, it's following a process to make sure that the stated winner is in fact the winner (the winner we would get if we went back and looked at the paper ballots) – Syverson – that is certifying and canvassing
Johnson – it's a matter of state law, explains process of what election board does during canvassing in his state (counting the ballots, auditing the ballots)
Joyce – difference between audits and auditability

What are the Processes – Big Room Discussion

No Name

- added processes:
    - at beginning - standards/testing/requirements for voting systems, vote verification
    - at end - auditing needs

Southeast Corner

- registration separated into registration and ballot request,
- added a step called processing between return of ballot and certification

Nautilus

- agrees with Southeast Corner,
- adding in auditing as part of certification/canvassing,
- authentication and authorization called out specifically

Mr. Red

- request for ballot added, b/c obtaining a ballot is multi-tiered process;
- creation of the ballot itself (there's a process for paper balloting, but what about electronic),
- that got them to data standardization (allows broader participation by allowing jurisdictions to have it in their toolbox) – common data format for ballots (interoperability)

Big room discussion – ballot rendering versus ballot definition/assignment (ballot assigned to right individual); consensus – obtaining a ballot is too broad a step
- Soper – UOCAVA system needs process for updating address/jurisdiction, others in room talk about how to advertise this process to voters
-Syverson – privacy and anonymity not addressed in anything we've discussed
- Jefferson – list of processes, not properties, and properties cut across all of the processes (accessibility, privacy, etc)

<u>Team Discussions of Voter Attributes/Properties (as Yana wandered from table to table):</u>
No Name –having a hard time thinking to themselves
Benaloh – integrity/correctness, privacy/coercion, availability/survivability, usability/transparency
Jefferson - In most cases voters have more trust in systems than systems deserve

- Big divide b/w paper and online issues for registration
- Voter registration database

Southeast Corner –wrote to themselves
Registration – ease of registration, simplicity and usability, access; what info you have to provide to register (how hard is it to get what I need), how annoying it is to provide same information to different pieces of the government *(Klaus – that's the national ID card, a no no), had a discussion about NVRA databases, sidetracked discussion about barcodes*
Obtaining a ballot – efficiency, able to get it fast, easy to get
(free, simple and easy cut across all of these processes for voters)

Mr. Red
Ballot Marking – mistake mitigation (error trapping for over and under voting), ease of use/intuitive, clear interface
Return of Voted Ballot - Voter verification that ballot was delivered (proof of receipt)

Certifying – auditability, correctness of tally, with privacy,

<u>Big Room Discussion: Voter Perspective Attributes</u>

Southeast:

- Across the board: easy to use, simple, efficient, reliable, free
- Registration: access to website, need to be able to update the registration
- Ballot Marking: optional validation (over and undervote checking), secret/anonymous
- Return of Voted Ballot: secure, ease of use (somebody takes care of all details for you), error free
- Certifying: verification that ballot was received, information on what went wrong (if there was a problem), vote auditable by voter, timely error messages (fix before end of election day)

Nautilus: similar to above, also:

- convenience (different from easy to easy to use) – more like available everywhere (ie, kiosk is easy, but maybe not available everywhere like online voting)
- track registration, ballot return, if vote is counted
- advertising/outreach/education for voters

Mr. Red:

- Registration: privacy and ease of use
- Obtaining: security and availability (having correct ballot style being delivered), correctness of content on ballot (ballot integrity), ease of access
- Marking: error trapping (over/under vote, mistakes), prevention of miscast of ballot
- Return: confidentiality, availability (time period allowed to return ballot), assurance of receipt of ballot
- Certifying: vote verification – did it get received, correctness of the tally

No Name:

- 4 basic properties that election system of any kind should have:
    - integrity or 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)
- Minority perspective – software should not be involved in ballot marking

Around the room discussion – are those 4 categories a framework we would all use;
Lux – likes it because everything that was listed could be assigned to those 4 categories
Burris – agrees, but likes the word 'efficient' as another category
Andel – agrees, that's what's in the literature (scientific and technical)

Jeffereson – agrees, wants to add transparency/observability of process (Benaloh – that's under usability from voter perspective)
Other discussion – add education/outreach/training for voters
Soper – 2 properties I want to see : fair and accurate (from the room: that's under Benaloh's integrity)
Smith – completeness of the ballot (being able to vote for local things, not just president) – everything that I'm eligible for, I get to vote on
Santos – is security a 5th category? (josh – security falls under the different categories, depending on what type of security you mean)

Room consensus – the framework is useful when presenting things to Bob Carey

<u>Team Discussions of Voter Attributes/Properties (as Yana wandered from table to table):</u>

Mr. Red

Problem for election officials is explaining to different vendors at each iteration of internet voting. Would be much easier if the same vendor did each demo project.
Hardest to figure out election official perspective for: obtaining a ballot and ballot marking; mostly just getting the right ballot to the right voters – need data integration system to deliver right ballot, and make sure system is secure and does error trapping for voters

Southeast

Across the board: recoverable and redundant
Registration: integrated with federal databases, easy, scalable,
Ballot Marking: unambiguous marking, simple words, easy to read, no questions of interpretation, no overvotes, no undervotes
Return of Voted Ballot: easy to determine whether it should be counted or not

<u>Big Room Discussion: Election Officials Attributes/Properties</u>

No Name:

- Registration: doing more with less (online registration b/c election officials and staff aren't doing the data entry, the voter is – so staff time isn't involved and data is more accurate), ease of assigning voters to correct districts, duplicate registration (not having multiple records for same citizen), transparency (ability to provide info to public about who is on the rolls)
- Obtaining ballot: efficient distribution (budget issues – more efficient distribution is cheaper, electronic is cheaper), ensuring the ballot is correct in terms of content and correct ballot style for that voter, more efficient is better for previous
- Marking: eliminate ambiguity as much as possible, hard to figure out voter intent for EOs, making sure that voters understand ballot so they can mark it correctly and eliminate need for EOs to guess what voters intended
- Return: ability to track ballots, ability to verify that you processes all returned ballots
- Certifying: ability to provide information that assures public trust

Mr. Red:

- overall – security and usability
- Obtaining ballot: making sure that ballot has been delivered
- Return: being able to make sure ballot has been returned

Nautilus:

- across the board:
    - Flexibility within system to make sure you can integrate with other technologies, accessibility aids, etc (ie, interoperability)
    - Sustainability – system can be maintained (cost and logistics) over it's lifecycle
    - Accuracy – info that's provided/received is accurate,
    - Scalability – if voter base expands, system has to keep up
    - Avoiding having to remake or resend ballots
    - Being able to demonstrate that you as the EO did your job, evidence of due diligence, CYA abilities (if that's auditability, then it was covered, but it's slightly different)

Southeast:

- across the board, want everything to be recoverable and redundant
- Registration: integration with larger voter registration interchange, scalable to size of voter reg rolls, automated with reporting capabilities
- Obtaining: ballot development, making sure correct ballot goes out to voter
- Marking: easy for voter to mark, cover over/under voters, ambiguity
- Certifying: Easy to determine if it can be counted, auditable

Saturday Afternoon

Teams:

Mr. Red Team - Andel, Fasmire, Lux, Manion, Aceto, Santos
Team No Name - Jefferson, Hancock, Regenstein, Holmberg, Pollins, Benaloh, Miller
Southeast Corner- Naujok, Yu, Valentine-Brown, Jones, Soper, Burris, Ramos
Nautilus – Robinson, Syverson, Daviage, Smith, Johnson, Shacham, Joyce, Wagner

Team Discussions of Outside Observer Attributes/Properties (as Yana wandered from table to table):

Mr. Red

No training process for poll watchers.
Statistical analysis that shows anomalies, instead of physical checking of everything.

Southeast

Transparency, adherence to policies across all categories. Voting machines must go through certification that machines are fair. Outside observers should be able to see that machines go through this process (open). But code is not open for review. Discussion about open source issue.
2nd monitor for tabulation of votes, visible by observers.
Elections in U.S. are chaotic, different rules for different counties, so international observers don't like to observe us. Because U.S. doesn't live up to treaty obligations for observers, bad countries say they don't need observers either.

No Name

Integrity is the overarching issue. Different types of observers – Jimmy Carter type vs. Dems and Republicans. Minority perspective: open source, ability to view code, could be part of transparency. Hancock: verifying that what jurisdiction certified is what they are running, or actually looking at the code. But not many people are qualified to look at source code, plus intellectual property rights.

Big Group Discussion – Outside Observers Attributes/Properties

Mr. Red:

- Hard to look at electronic system from outside observer standpoint – how can we make it transparent for an outside observer. What's a perception of what happened? How do we define a poll watcher in an electronic system.
- Observation of the registration process – people who are ineligible signing up
- Observer in the front and back ends only – registration/ certifying

Nautilus:

- system has to have easy verification;
- integrity;
- availability - outside observer needs to be able to see all parts of process;

- usability – outside observer should be able to understand how the system works and what they are looking at;
- auditability
- Kiosk style system might be similar to polling place, but electronic system is much more difficult

No Name:

- accessibility – have to have access to all aspects of the process;
- Registration – observers should know requirements, demographics
- Certifying – observe that jurisdiction can correct mistakes, confirm that jurisdiction is using the certified system
    - Should the process meeting international standards for observation?
- Ability to view source code? Or just compare input and output of system, and treat source code as black box? --- this is a debate that UOCAVA guys will have to resolve
    - Burden of source code audit – million lines of code. Might be un-necessary (Benaloh). Don't trust black box testing (Klaus)

Southeast

- Breakdown by registration etc is not useful, did not address. Basic principles
- Transparency – observes must be able to tell that law is being observers, that technology is the advertised technology, and that testing/certification process is there and was used
- Disclosure – disclosure of standards to which equipment is tested
- Openness – transparency is not to some class of observers, but that anyone can enquire and get answers

<u>Team Discussions of Saboteur Attributes/Properties (as Yana wandered from table to table):</u>

Nautilus

Syverson - Social engineering is a better hack than the crypto. If I can prevent you from using the system, I'm in. CAC card would prevent this.

No Name

Registration – potential target for wholesale attack
Obtaining ballot – potential target for localized attack
Ballot marking – potential target for localized attack
Return of voted ballot – potential target for localized attack
Certifying – potential target for wholesale attack
Verification/auditing – potential target for wholesale attack
Jefferson – I can't support any electronic system unless they have Benaloh's properties. Paper is the alternative, and it's hard to remotely attack and tinker with on a large scale except at the LEO, and that's the best defended spot. Benaloh – paper doesn't have verifiability (whether it was counted properly) – end to end systems prevent this. End to end is an auditing method – I can tell something went wrong, but I can't prevent it. Also, tradeoff with paper is that you make small scale attacks easier but large

scale attacks harder. Hackers want it to be obvious where the ballot is at every stage. Jefferson – voters waiving their right to privacy is not okay, voters don't have the right to waive their own right to privacy because you are endangering the entire election. Benaloh – taking fringe opinion, doesn't want vote by mail at all, only at a kiosk or polling place. Disagrees with Bob's premise that the level of risk should be the current level of risk. Jefferson – also disagrees with Bob's premise.

Southeast

Want system that's complex (more software is more likelihood that there's a door into the system). Don't want it to be redundant or recoverable (for DOS). Want it internet based, with open IPs on management side. Don't want it tested or certified. Want a centralized system with one database. Want it to be in the cloud (don't know where its hosted – no disclosure), or hosted overseas. Want it to be windows based. Want it to be electronic, no paper and no backups. Want full disclosure, open source, network diagrams. Want it to be built on technology that was good 20 years ago. I want it to be with an organization that has lack of standards, lack of discipline, with everyone in the building w/ admin access. Want no firewall between engineers, service group, etc. Want DMZ, because there's usually a hole from there back to main system. Want incompetent IT staff, with no promotion path from IT to management (so only people with any knowledge are at the bottom and disgruntled). Want system where engineers do live patching on production code from home. Organization without management procedures to review security. LEOs should outsource everything, and have no admin control.

Mr. Red

3 main attacks across the board: DOS, perception management/social engineering, manipulation of the result/votes

DoD has high assurance level, problem comes when it leaves the DoD. Risk is far higher outside the DoD.

Need way to say with 95% assurance that data was created here ended up over there.

Go with the most low tech approach to electronic transmission instead of the most high tech approach, because hackers aren't thinking of old old modems.

<u>Big Group Discussion – Saboteur Perspective</u>

Nautilus

- Auditability is the best defense against saboteur. Must be able to defend legitimacy of system if there are no problems, and detect problems if they occur. Auditable/verifiable systems defend the public trust.
- Software independence – when you use software, there needs to be some way to determine that outcome is correct, even if software is faulty or was hacked.
- Voting systems need to be designed with threat model in mind (Hovav wrote us notes for that). To be safe: online voting system must be disconnected between the tabulation system (print out ops scanable paper ballots).

Mr. Red

- All 5 categories deal with 3 or 4 areas. DOS attack. Perception management – hackers can create enough suspicion without actually hacking. Manipulation of votes – data at rest and data in transit.
- If you don't have good controls at end points, you're open to all traditional types of cyber attacks.

No Name

- Looked at weaknesses. Distinction between a small/localized attack and a wholesale attack. Paper usually has localized attacks, electronic have wholesale attacks.
- Registration – fraudulent voter registration in a large enough scale to impact election
- Insider vs. remote attacks. Electronic = remote attacks. Insiders have the ability to have a large impact (LEO, programmers). Perspective of a hacker: biggest bang for the buck.
- Two views in team: Paper advocated by some, end to end verifiability advocated by others as a potential deterrent and auditing mechanism (software independent mechanism) for electronic voting.

Southeast

- Looked at what saboteurs would want:
    - Internet-based, ip open, wireless access, standardized passwords, central system, cloud based, windows OS, no firewall, heavy DMZ, outsourcing everything, no version control, frequent changes
    - Registration – open registration with no internal controls, transparent board of elections
    - Obtain – normalized database rendering of ballot, PC based clients
    - Marking – on the fly ballot rendering
    - Return – clear text transmission, no check sums, electronic ballots
    - Certifying – no intermediate results, no logs

<u>Team Discussions of Risks (as Yana wandered from table to table):</u>

General group discussion about why we are here, whether we should focus discussion to only the type of demo project that Bob Carey brought up. Jefferson doesn't want to focus discussion on military only, because large other constituencies want to do internet voting. Jefferson wants FVAP to listen to things they don't want to hear. Report should distill and summarize experience of everyone in the room on the topic of military with CAC voting, but keeping in mind other constituent groups. Jones – need to define statistically significant number as some number that could make difference in election, and that fraud in that number of votes has an expected payoff (ie, motivation for fraud is there).

Southeast: looking at large enough scale for real risk
Worried about Google and other companies monitoring email.
If keep it to CAC cards, it's secure.

No Name:
Pilot should allow a live general election to demonstrate the real risk.

<u>Big Group Discussion – Focusing the Risk Conversation</u>

Nautilus

- How to best perform a credible risk assessment. With reference to a particular system, not in the abstract. One model is AES cryptographic selection process – involves public performing analyses. Procurement policies for FVAP – independent security analysis by experts, enabling other experts to perform their own security analysis to enable public debate.
- Public penetration testing, making design docs available so everyone can do security analysis to establish credibility. DC board of elections is a model for this. Concern: disclosing source code is enabling hackers, but security community says benefits of this outweigh the risks. Concern: vendor intellectual property. But vendors do cooperate, and have in the past, so it doesn't need to be a barrier.
- Quantitative risk analysis is beyond what we know how to do, because we don't know how to define the probability of attack. Also, skill level of attackers varies so significantly that we can't make that assessment either.

Southeast

- Failed to reach consensus. Except: likelihood of attack on military UOCAVA votes altering election is tiny. Conclusion: it doesn't really matter – if we disenfranchised all UOCAVA voters it wouldn't have much of an impact, so attack on their votes would only disenfranchise a few. So risk at the scale that is currently envisioned is actually very low.

No Name

- Metarisk issues discussed. Want to correct the record on the difference between risk of disenfranchising 1000 votes and switching 1000 votes. Difference is factor of 2. Disenfranchising random sample is one thing, choosing 1000 votes to switch is something else. Ability to switch votes is not comparable to disenfranchising.
- Definition of risk as articulated by Bob and Joel. Risk = probability*damage. Group agreed that this is not a good formulation of risk. A better framework is amount of damage divided by the cost. No way to rationally estimate probability of attack. Wants everyone to start thinking of that framework, ie, cost-benefit analysis. Can put a dollar value on damage caused. We need to raise the price of attacking electronic systems until it's a better value to buy ads on CNN. Others say that CNN is a red herring, and we should be comparing different illegal attack methods.
- Slippery slope argument. Investing $$ and time into these systems creates too much incentive to exaggerate success of first effort to spread costs over more voters in future elections. Arguments will be made that because this election was safe, other, larger elections will be safe also. FVAP should do this once and discourage electronic voting for other populations. M&M argument.

Mr. Red

- FVAP should try to emphasize in their documentation and reporting that the risk of failure inherent in the current system, and the proposed system, and neither will ever be 0. Emphasize that whatever they are proposing will be at least an equal and possibly lesser degree of risk than the current system.
- Risk vs. vulnerability and threat models, get a better idea of what kind of threats are out there, and thinking of attacking voting systems.
- Make sure we don't introduce reverse risk into DoD system by using CAC cards to vote.

Last Thoughts

Soper: Focus is on technology, but the ballots in 2010 get back in 10 days. The biggest problem is that half the ballots sent out are sent to the wrong address. Other procedures and solutions are not being addressed, and we need to discuss how we can improve the front end via procedures, and not via technology.

Burris: cost is going to be more than net gain. More emphasis needs to be put on the front end of military education, getting VAOs engaged, voters engaged. If they were engaged in the beginning, it would

Valentine-Brown: Agrees with above. Scheduled meetings with VAOs, and nobody shows up.

Benaloh: two separate cost benefits analyses. One is security side: cost of attack must be higher than benefit. From deployment side, we need to understand cost of that level, and what that achieves. Wand to avoid appearing as someone who is against internet voting. We have a status quo, and we have end to end tech that can make things better than the status quo. Internet voting can add many new risks. Internet voting without e to e is adding to risks by large factor. Monitored voting vs unmonitored voting is a big issue. Ie kiosks vs voting from home. Unmonitored voting has enormous risks of coercion, and has risks we don't know how to manage. Monitoring would be an important factor to consider to reduce risks.

Jefferson: if you must do internet voting demo, do it with end to end verification, either paper or electronic. Otherwise you get undetectable attacks.

Miller: conflicted as an EO because people with disabilities and people who can't get their ballots back in time are disenfranchised. Other perspective is that I'm concerned with slippery slope, and internet voting should not be available to everyone.

Lux: Regarding wrong registration addresses. Voters lie when its convenient, and they procrastinate, and their emergency becomes the EO emergency. Voters who don't update addresses who live locally has recourse, but those in foxhole don't. If we disenfranchise any other group like we do military, there would be riots in the streets.

Fasmire: not sure he agrees with cost benefit analysis. If you can get something to go viral, the cost is almost nothing. Cost model can't take that into account. Shacham: viral threat ie botnet has that kind of assumption. Fasmire: we need to get those guys on our side. Benaloh: even botnet doesn't have zero cost, and you can calculate it.

Johnson: echoes EOs. Outreach is important.

Smith: snacks were great, temperature control was great. Paper exists that quantifies risk by attack team size (Lazarus from last year's conference). Another formula for how to calculate risk. Rioting in the street can go the other way. We don't want to tell one group that they have to give up right to privacy, or that they should use systems with no auditability.