Realistic Mitigations for UOCAVA Voting

Jared Marcotte, The Turnout
About The Turnout

● Consultancy focused on a variety of election technology issues
  ○ Voter registration data interoperability and interchange
  ○ Cybersecurity aspects of electronic voting methods
  ○ Application usability analysis
  ○ Custom development (where applicable)
Acknowledgements

● People
  ○ R. Michael Alvarez, PhD
  ○ Magenta Sage Strategies
  ○ John Dziurlaj
  ○ Joshua M Franklin

● Organizations
  ○ Democracy Fund
  ○ FVAP
  ○ NIST
Agenda

- Purpose
- Securing the Voter
- Fax Security
- Email Security
- Election Portal Security
- Conclusion
Disclaimer

● Multiple technologies are used to return ballots (e.g., fax, email, apps)
● NIST concluded that unresolved computer security and voting technology issues exist for electronic ballot return:
  ○ Endpoint security
  ○ Voter authentication
  ○ Ballot auditability
● Securing online ballot return is an active field of research
● No clear solution at this time

NIST Activities on UOCAVA Voting
https://www.nist.gov/itl/voting/nist-activities-uocava-voting
Securing the Voter

- Remote voters are advised to plan how they will cast their ballots
- Ensure a private and independent method of voting
- Helps to avoid voter coercion and intimidation
  - Shoulder surfing
  - Monitored systems and networks (e.g., library, schools, coffee shops)
  - Cameras in public areas
- Many election jurisdictions already provide great guidance for helping voters to secure themselves while voting
  - Officials should continue to ensure voters have this material available

From the Attorney General of the State of Minnesota

https://www.ag.state.mn.us/Consumer/Publications/HowtoProtectYourselfAgainstHackers.asp
Just The Fax

- Fax technology is a conglomeration of *implicitly trusted* protocols, networks, and systems
  - Both ends cannot verify how, where, or from whom a fax originated
- Fax machines should be dedicated to election activities, in a locked room, and disconnected from the internet or local WiFi network
- Firmware updates and security patches should be applied to all-in-1 devices
- Avoid cloud faxing, iFaxing, or other similarly-named services
- To the extent practical, authenticate and encrypt transmissions
- FVAP provides guidance and makes DoD Fax Service available
We’ve Got Mail

- Similar to fax technology - designed for interoperability, **not security**
- Encryption and authentication are not the default by most email providers
- Use DMARC to prevent fake emails and message spoofing
- Use email providers that support STARTTLS
- Disable loading of certain email content
- PGP or GPG can be used to encrypt and sign emails
  - Viable alternative but difficult to explain and distribute keys
- Many voters are already on end-to-end messaging platforms (e.g. WhatsApp, Signal, Threema)
  - Can be used to send and receive encrypted ballot images
Election Portals

- Portal is a catch-all term to enable blank ballot delivery, online ballot marking, and remote ballot return
  - Can also be co-located with online voter registration
  - Ballots selections can be sent as data or images
- These internet facing systems must withstand a variety of attacks
- NIST published security recommendations
  - NISTIR 7700 - Security Considerations for Remote Electronic UOCAVA Voting
Web App Security

- Portals should undergo a cybersecurity development process similar to other critical infrastructure areas
  - Secure systems engineering
  - Risk assessment
  - Static and dynamic code analysis
- Use two-factor authentication, if possible, to access apps and underlying infrastructure
- Trusted digital certificate
- Establish relationships with EI-ISAC & DHS
- Ensure responsible vulnerability disclosure from whitehats, if possible
- Obtain outside security assessments, but vet the assessors
Conclusion

- A discussion of specific threats is included within the written report
- The written report contains links to guidance from other organizations
  - We updated and brought it all together
- Realistic mitigations exist for common security concerns facing UOCAVA voting methods
- The recommendations included here can reduce the risk of compromise
  - Recommendations do not alleviate all of the risks associated with online systems
Thank you

Jared Marcotte, The Turnout
jared@turnout.rocks
References

- NISTIR 7700 - Security Considerations for Remote Electronic UOCAVA Voting
- FVAP Fax & Email Guidelines
  [https://www.fvap.gov/oe/overview/sending-ballots/fax-email](https://www.fvap.gov/oe/overview/sending-ballots/fax-email)
- Internet Safety: How to Protect Yourself Against Hackers
  [https://www.ag.state.mn.us/Consumer/Publications/HowtoProtectYourselfAgainstHackers.asp](https://www.ag.state.mn.us/Consumer/Publications/HowtoProtectYourselfAgainstHackers.asp)
- A Tutorial for Beginners to PGP
  [https://www.pitt.edu/~poole/PGP.htm](https://www.pitt.edu/~poole/PGP.htm)
- NIST Auditability Working Group