the turnout

UOCAVA Electronic Ballot Transmission

Recommendations to Mitigate Security Risks

Authored by The Turnout, LLC[1]

[1] This project by The Turnout, LLC was supported by the Democracy Fund.

Background

U.S. military and overseas voters have special absentee voting rights for federal elections. These rights are governed by the 1986 *Uniformed and Overseas Citizens Absentee Voting Act* (UOCAVA), and are colloquially referred to as UOCAVA[2] voters. This group faces unique challenges when registering to vote, and receiving and returning their ballots to their local election offices for tabulation. While the nation is comprised of different jurisdictions, each with their own unique election laws and processes to conduct elections, enabling military and overseas voters to register to vote, receive a blank ballot, and cast a completed ballot while away from their place of residence is an important duty of election officials throughout the nation.

Although UOCAVA helped to established the initial legal framework for assisting military and overseas voters to participate in elections, it did not completely remove the burdens associated with successfully returning a ballot. For instance, ballots were not always getting to voters in a sufficient time frame for voters to properly complete the ballot, and return it via mail. In 2010 Congress modernized and expanded UOCAVA by passing the *Military and Overseas Voter Empowerment (MOVE) Act*. MOVE mandated that election jurisdictions use modern technologies to distribute validly-requested absentee ballots to voters within 45 days. Over the first few years after its passage, a number of new election technologies came to fruition that are still heavily utilized today such ballot tracking and electronic blank ballot distribution systems.

This report provides security recommendations for the current practices surrounding electronic blank ballot delivery and voted electronic ballot return within U.S. states and jurisdictions. These recommendations aim to be actionable for election officials, related intragovernmental agencies, and other related stakeholders. The recommendations contained here are not solely technical recommendations, as many procedural and operational safeguards are also suggested that can be implemented by election officials to help secure the election process.

It is clear that many election jurisdictions make extensive use of email, fax, and web portals for UOCAVA ballot transmission and return. The suggestions within this report are provided In the interest of improving the security of these UOCAVA voting methods that are already in place in some election jurisdictions, without actively encouraging their expanded use in other jurisdictions. These range from methods to ensure the physical and electronic security of fax systems, to mitigating the threats facing email and web portals. It is important to keep in mind that even by following the suggestions outlined below, there is no guarantee that any existing mode of electronic ballot transmission or return can be made completely secure.

These recommendations should not be considered an argument for any particular method of UOCAVA electronic ballot return, nor a blueprint for fully-securing any of these modes. In fact,

[2] Uniformed and Overseas Citizens Absentee Voting Act https://www.fvap.gov/info/laws/uocava.

the National Institute of Standards and Technology (NIST) concluded that there are unresolved computer security and voting technology issues around endpoint security (e.g. securing voter-owned and State-owned devices against attack), voter authentication, and ballot auditability for remote electronic voting.[3] Ways and methods of securing online voting is an active field of research and there is not a clear solution at this time.

Steps taken to increase the security of ballot transmission and return may conflict with accessibility and usability for voters or may produce administrative complexity for election officials. For example, this report does not discuss securing the remote voter's device, application, or network. States and jurisdictions may not desire or need to implement all of these recommendations; rather this summary offers considerations for election officials to improve the security of this important aspect of their state's or territory's balloting process in 2019 and beyond. With these disclaimers, there are valuable and actionable items to protect election offices and voters that should be implemented whenever possible.

Technical and procedural recommendations

This report is not the first effort in providing guidance for securing technology designed to assist UOCAVA voters. NIST has published *Interagency Report (IR) 7682 - Information System Security Best Practices for UOCAVA Supporting Systems,*[4] *NISTIR 7711 - Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters,*[5] and *NISTIR 7700 - Security Considerations for Remote Electronic UOCAVA Voting.*[6] Although these documents were published in 2011, they still offer useful security recommendations and provide an in-depth treatment of the subjects.

This report's recommendations begin with ways to secure the voter themselves while engaged in UOCAVA voting activities, followed by individual discussions on the various technologies used within UOCAVA voting: fax, email, blank ballot distribution, and remove electronic voting systems.

Securing the voter

First, a piece of general advice for UOCAVA voters is to ensure their own physical security when performing election-related activities. A voter should feel safe, secure, and free to cast their ballot without fear of coercion—due to someone physically intimidating or threatening the voter to vote a particular way—or by sacrificing secrecy—due to nearby cameras or people looking over the voter's shoulder.

[3] https://www.nist.gov/itl/voting/nist-activities-uocava-voting
[4] https://www.nist.gov/sites/default/files/documents/itl/vote/NISTIR-7682-Sept2011.pdf
[5] https://www.nist.gov/sites/default/files/documents/itl/vote/nistir7711-Sept2011.pdf
[6] https://www.nist.gov/sites/default/files/documents/itl/vote/NISTIR-7700-feb2011.pdf

There are many variables across various platforms, systems, and devices, which are outside of the control of the jurisdiction or local election official (LEO), and potentially beyond the ability or comfort-level of the voter to improve. However, it would still be useful for all levels of government, including jurisdictions, to provide voters with educational resources or guides to protect themselves. The specific concerns for the use of certain services may be different from state to state, but several have good examples to follow. The office of the Attorney General of the State of Minnesota, recommends these general steps for online/cyber safety:[7]

- Make sure your computer security software is up-to-date;
- Install and use antivirus and anti-malware software on your computer;
- Create a strong PIN or passcode for your mobile or cell phone;
- Only install trusted applications on your mobile or cell phone;
- Keep your mobile or cell phone software up-to-date;
- Create unique passwords for all electronic communication devices;[8] and,
- Use multifactor authentication on your accounts.[9]

Verify reception of electronic ballot

Some electronic ballot transmission modes provide built-in methods to confirm to the voter that their election office has received their ballot. Election offices should proactively inform voters of the status of their ballot via transmission report (fax) or a read receipt (email). For voters who want to confirm receipt and disposition of the returned ballot, election offices should also provide a method that UOCAVA voters can use to check the status of their returned ballot, such as a phone number, an email address, or a look-up tool.

Fax

The term “faxing” has become muddled in recent years due to changing technology. Faxes can be sent over physical fax machines, through traditional phone lines, digital lines, online services and websites, or mobile phone applications. At times faxes can be received through any combination of these methods. Because of the multiplicity of ways that a fax can be sent, it can be exceedingly difficult to ascertain from where a fax is coming and through what medium. This is in part why fax data are unencrypted as the fax system is designed to ensure that nearly any system or machine can receive and interpret it. This makes securing ballots transmitted by fax complicated.

[7] The recommendations, originally at the following link, have been altered slightly in this report for clarity: https://www.ag.state.mn.us/Consumer/Publications/HowtoProtectYourselfAgainstHackers.asp
[8] The Center for Democracy and Technology (CDT) released a guide on passwords https://cdt.org/insight/election-cybersecurity-101-field-guide-passwords/
[9] The Center for Democracy and Technology (CDT) provides a guide on multifactor authentication https://cdt.org/insight/election-cybersecurity-101-field-guide-two-factor-authentication/

The Federal Voting Assistance Program (FVAP) is the U.S. government agency charged with assisting military and overseas voters with election-related activities. FVAP provides guidance to assist jurisdictions using fax machines for election-related activities.[10] Additionally, FVAP makes the U.S.Department of Defense (DoD) Fax Service available to election officials to transmit and receive election materials via a toll-free fax to and from Service members, their eligible family members and other eligible overseas voters.

Examples of risks associated with the use of fax machines for returning ballots include:

- Loss of ballot secrecy due to lax physical security at the receiving fax machine;
- Intentional modification of the ballot at the receiving end if the ballot is not physically safeguarded;
- Loss of ballot secrecy due to network eavesdropping while transmitting the ballot image;
- Accidental modification of the voter's ballot selections when the faxed image of the ballot is transcribed onto a proper ballot of the appropriate paper stock; and,
- Loss of ballot secrecy and/or modification of ballot selections due to a compromise of the fax machine itself.

Ensure faxes are physically secured

Assuming that ballots sent by fax are received by a physical fax machine or printed before being manually transcribed and duplicated for tally, the machine used for this process should be kept in an area or room with limited or controlled access in the same fashion as any other live, voted ballot. Only individuals trusted with handling ballots should have access to the machine for the entire duration that it is being used for election activities. This helps to keep the pool of authorized individuals small to minimize risk that the received ballot is damaged or manipulated. Access to the area or room with the physical fax machine should be logged or monitored to minimize and track unauthorized access.

Fax machines used for ballot transfer should be disconnected from the local network

Ideally, the fax machine used for ballot transfer should exclusively receive faxes. In smaller offices, where the fax machine may be a multi-purpose printer that performs additional functions such as faxing and scanning, the machine is likely tied to the overall network and should be disconnected during the entire UOCAVA voting period. Dedicated fax machines are fairly inexpensive, often available for approximately $50. Other departments in local governments may be able to provide a dedicated fax machine temporarily for this purpose. To the extent practical, this includes all wired connections—typically ethernet—and wireless connections (e.g. Bluetooth, WiFi). Printers with wireless capabilities may open the jurisdiction to potential

[10] https://www.fvap.gov/eo/overview/sending-ballots/fax-email

document leaks,[11] and multi-purpose fax machines with local network access can be a danger to the overall network.[12]

Take advantage of network security

For jurisdictions that use IP telephony (i.e. VoIP), work with your provider to investigate encrypted fax transmission. Even with encrypted transmission, only the network of your provider is guaranteed to be secure. Once the fax data exits the provider's network, the transmission is likely unprotected.

Ensure proper configuration of fax machines

Newer fax devices, especially those that are part of multifunction devices (MFD)—which may act as an office copy machine, printer, and fax machine—may store received faxes for later retrieval. Prolonged storage of the voter's transmission (i.e. how they voted) increases the chance that stored ballots may be viewed or manipulated. Use of multifunction devices with strong security controls, such as Common Criteria certification, and configuration to federally-tested, secure settings is essential.[13] Election offices using fax machines which allow fax storage should develop procedures for removing stored ballots from the machine's memory and storage, and for logging this process.

Printers with faxing capabilities often contain multiple web servers and fail to be updated on a frequent and regular schedule. In addition to a properly configured device, it is important to ensure the machine is regularly updated, especially in the time before an election.

Fax machines should make contemporaneous paper records

If the machine is configured to store received faxes in memory, the machine should also make a contemporaneous hard copy of each ballot the jurisdiction receives. This reduces the chance of loss due to forgotten encryption keys, deletion, or machine failure. This policy necessitates the previous recommendation on physical security be followed as well.

Use real-time faxing methods only

Some third parties offer cloud faxing, iFaxing, or other similarly named services. These services often provide what is called "store and forward" faxing, where the fax is stored in the cloud and later forwarded to its eventual destination. This relies on a third party to secure the endpoint against attacks—which, if not properly protected, may result in violations of ballot secrecy—and jurisdictions should avoid the use of these services for UOCAVA ballot transmission.

---

[11] https://www.wired.com/2015/10/drones-robot-vacuums-can-spy-office-printer/
[12] https://www.wired.com/story/fax-machine-vulnerabilities
[13] U.S. Government Approved Protection Profile - U.S. Government Protection profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™ 2009), https://ieeexplore.ieee.org/document/5422058

Additionally, because the voter is talking to a middleman, not the jurisdiction's fax machine, the transmission reports may give a false sense of security.

Email

Similar to fax machines, email was designed for interoperability over security. It too faces significant procedural and technical hurdles in secure implementation and usage. Yet solutions exist that can make it a much better option than fax. There are tools that local election offices can use to encrypt the data or mode of transmission, but there are still vulnerabilities to be mitigated. While encryption can prevent unknown individuals from reading ballot contents while being transmitted, it does not verify that the individual sending the ballot is actually the registered voter, nor that the ballot hasn't been modified during transmission. This is a process known as authentication. A holistic email solution authenticates both sides of an email transaction and prevents unauthorized third parties from reading confidential information. The solution should also encrypt the email and prevent it from being modified in transit. Some of the solutions presented below accomplish these goals.

Examples of risk scenarios associated with the use of email for returning ballots include:

- A fake ballot is delivered to the voter who is subsequently disenfranchised by returning the fake ballot;
- Voted ballots containing malware are returned to the election official;
- Loss of ballot secrecy due to an intermediate party reading ballot selections;
- Loss of ballot secrecy due to malware on the voter's computer system; and,
- Loss of ballot secrecy as voter is coerced into sending a ballot by a physically present party.

Preventing email address spoofing

It is often surprising to individuals when they learn how easy it is to send emails from an address they don't own. Often times, it's as easy as navigating to a website that offers a service that allows users to manually specify both the sender and the receiver addresses. In part due to the implicit trust built into the email system, addresses can unfortunately be spoofed, and this issue is affecting organizations throughout the world. It's worth noting that this simple method of spoofing doesn't always work and is most successful when companies or individuals are running their own misconfigured email server. Certain top level domains (TLDs) such as .gov are rarely susceptible.

A new system has been devised to help alleviate this issue, known as Domain-based Message Authentication, Reporting and Conformance (DMARC). DMARC can help local and state election officials spot phishing emails by highlighting impersonation attempts. Depending on the policies chosen for a domain, jurisdictions can quarantine emails that don't properly validate, or simply refuse to show them. DMARC does not require a purchase of software or hardware to

utilize and is experiencing rapid adoption across all sectors of IT. DMARC does not work in a vacuum and typically leverages the Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to assist in determining the authenticity of an email message.

Support STARTTLS[14]

As email is transmitted from a sender to a reader, the message has to pass through mail servers. The sender's mail server contacts the reader's mail server to transfer the message. Normally, one server would send the data unencrypted to the other because email is often made up of text. However, if both servers have STARTTLS enabled—a command will allow both the sender's and reader's servers to agree to upgrade their connection to support something called transport layer security (TLS) encryption—when this happens messages will be transmitted over an encrypted connection, which is much more secure.

However, enabling STARTTLS only allows mail servers to support more secure encrypted connections. If the STARTTLS command is missing from the sender's mail server or there is no response to the STARTTLS command from the receiver's mail server—either scenario could be potentially due to an attack or other limiting factor—the server will transmit the message over an unencrypted protocol as MX servers prioritize deliverability over security.

Email providers, whether email is provided through government IT agencies or vendors, should be able to answer questions on STARTTLS configuration, including if an office server is STARTTLS enabled. The Electronic Frontier Foundation (EFF) created a campaign, STARTTLS Everywhere—hosted at https://www.starttls-everywhere.org/—to promote safer email and a service to check email domains for an existing STARTTLS policy.[15] Individuals can visit the campaign site to check a domain name against EFF's service and provide the result to the email provider to start a conversation about email security.

Support end-to-end encryption

End-to-end encryption, a term for email text or information being encrypted at a starting point and decrypted when it is received, allows for encrypted email to travel over unencrypted channels (which are the most common). Voters and election officials may use one of the following end-to-end encryption programs or standards: Pretty Good Privacy (PGP), GNU Privacy Guard (GPG),[16] or Secure/Multipurpose Internet Mail Extensions (S/MIME). When up and running the processes and email clients used by the jurisdiction should allow verified voters

[14] STARTTLS refers to the server command and is always capitalized. STARTTLS is an implementation of the concept of "Opportunistic TLS," which outlines using extensions in plain-text communication protocols, like the ones email uses, to upgrade the connections to be encrypted.
[15] https://www.starttls-everywhere.org/
[16] GPG, PGP, and S/MIME use public-key cryptography. Public-key cryptography, put simply, describes a system requiring two keys: a public key—used to ensure the message came from an assumed source—and a private key—used to decrypt the messages encrypted with the matching public key. While each uses public-key cryptography, the implementation of each of these end-to-end encryption programs and, in the case of S/MIME, standards vary greatly and is beyond the scope of this report to cover.

to send and receive encrypted mail with an election official. The University of Pittsburgh hosts a comprehensive tutorial on setting up PGP.[17] Election offices would likely need to provide step-by-step guidance to voters to set up end-to-end encryption for themselves. It may involve specific training on email client plugins or functionality and an understanding of how to create, get, and install keys and/or certificates, which is a non-trivial task for most users. It is also not without other risks. Encrypted emails prevent network-level antivirus scanning, since the contents of the emails are encrypted, this requires the emails to be scanned by the receiver. This method increases the risk to the office network because the first time the contents will be scanned for viruses is at the time of delivery.

Disable the loading of remote content

Email has the ability to display embedded images, but many email clients also have the ability to download other types of types of content, such as images and files that affect the design of the message, that are stored on a remote server. Remote content decreases the size of the message in transit while allowing the visual aspects of the message to update after the message has been delivered.

However, the remote content can be detrimental to the privacy of the user. When the client starts to load the remote content, it sends a request to the server that can potentially expose information about the user and machine. Many commercial bulk emailing companies place tracking information within the emails to report on open rate and deliverability, but these same tactics can be used by bad actors to gain information about users and the network. Although emails without remote content may be less aesthetically-pleasing, jurisdictions can still create a functional, readable email with greatly improved privacy.

If you use end-to-end encryption loading remote content has the potential to break it. Earlier this year, security researchers uncovered vulnerabilities, dubbed EFAIL, that would allow an attacker to read the plain text of an encrypted message. In addition to privacy concerns, the researchers speculate that message content could potentially be manipulated and attachments could be injected with malicious code that could extend the damage to the greater network.[18]

For these reasons, jurisdictions should avoid using remote content in their email communications with UOCAVA voters, in particular email ballot transmission.

Alternatives to email

Using email may seem a generally accessible option due to its ubiquity, but given its security limitations, other encrypted communication platforms could be potentially safer and easier to use. Services like Signal,[19] ProtonMail,[20] and Threema[21] all offer free,[22] usable, end-to-end

[17] https://www.pitt.edu/~poole/PGP.htm
[18] https://efail.de/
[19] https://signal.org/
[20] https://protonmail.com/

encrypted messaging. These services could be used as an alternative to email ballot return. Assuming an election office had a confirmed Signal number, Threema ID, or ProtonMail address for a voter—and, likewise, the voter knew one for the elections office—the election official and voter could exchange messages and ballots with greater confidence in security and deliverability than end-to-end encrypted email. It may be worth exploring the legality of this option.

Electronic ballot delivery and ballot return portals

The term "portal" is a catch-all term for a web-based application that requires the voter to authenticate to the system in some manner to receive and/or submit a ballot. Besides enabling blank ballot delivery and electronic ballot return, jurisdictions may also operate other election systems within the same portal, such as voter registration or candidate filing systems. Depending on the implementation of the portal, this may involve filling out an online ballot or uploading a PDF. Regardless of implementation, these systems are internet-facing and use standard web-based technologies, which greatly increases the potential risk of attack.

Examples of risks scenarios associated with the use of electronic ballot delivery and returning electronic ballots include:

- Incorrect ballot provided to voter;
- Direct attacks on the election portal leading to full compromise of confidentiality, integrity, and availability;
- Loss of confidentiality and/or integrity of ballots in transit to, or sent from, the voter;
- Loss of ballot secrecy due to malware on the voter's computer system;
- Loss of ballot secrecy as voter is coerced into sending a ballot by physically present party;
- An improperly authenticated voter returns a ballot that they are not authorized to send; and,
- Attacks on the voting system.

States utilizing blank ballot distribution and ballot return portals should conduct the cybersecurity normal for critical infrastructure. For instance, states and jurisdictions should conduct a formal risk management process such as those detailed within *NIST Special Publication (SP) 800-30 Revision 1 - Guide for Conducting Risk Assessments*[23] or the *Center for Internet Security Risk Assessment Method (CIS RAM).*[24] Additionally, states and jurisdictions should participate in a secure systems engineering process such as those detailed with *NIST SP 800-160 Volume 2 - Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of*

[21] https://threema.ch/en
[22] Both Threema and ProtonMail have paid services or tiers, but still offer free accounts and services.
[23] https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
[24] https://learn.cisecurity.org/cis-ram

Trustworthy Secure Systems.[25] Regular scans should be run for vulnerabilities and misconfigurations within the infrastructure supporting the election applications. The software running the election application should frequently undergo analysis from static and dynamic analysis tools. Other experts in election security have suggested the following practices:

- Use two-factor authentication for all systems whenever possible;
- Maintain a trusted certificate;[26]
- Purchase common domains (e.g. register.state.gov);[27]
- Establish an ongoing relationship with the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) and U.S. Department of Homeland Security (DHS) to assist with threat intel and remediation;
- Obtain outside assessments, but vet cybersecurity product and service providers; and,
- Make it easy for external, well-meaning cybersecurity researchers from the public (i.e. whitehat hackers) to responsibly disclose vulnerabilities to election officials and the elections security operations team. The standard mechanism involves the use of the security@yourstate.gov.

With all this in mind, obviously the proper running of these systems requires a skilled, dedicated and well-resourced team of cybersecurity professionals. The following are more specific discussions on technologies that can be implemented to help secure the blank ballot distribution or electronic ballot return system.

Auditability

Auditability is considered a core tenant of voting systems by the security community. Paper-based, electronic, and hybrid voting systems with strong auditability capabilities allow the following:

- Detection of errors (often through voter verification);
- Diagnosis of faults;
- Correction of errors;
- Disambiguation of voter intent;
- Preservation of records; and,
- Sampling in post-election audits.[28]

---

[25] https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf

[26] https://jfranklin.me/prez/DEFCON26-FINAL.pdf

[27] In his presentation, Franklin's example used a .com-based top-level-domain. Since anyone can apply for a .com domain, it opens the domain up to additional typosquatting risk, which is the act of registering alternate spellings of domain names to try to get users to land on the typosquatted site rather than the original. When users land on the typosquatted site, the attacker may set up a mirror of the original site to phish for user data or attempt to load malware onto unsuspecting users. Registering a .gov domain decreases the risk of typosquatting due to federal control of the .gov space and legal restriction on use, assuming users at least know the domain should end in .gov.

[28] https://www.nist.gov/document-7152

A class of voting systems exists known as end-to-end (E2E) cryptographic voting systems have a unique system architecture that helps push online systems towards desirable auditability properties. These systems generally ensure that voters can cast a single ballot and provides cryptographic evidence to voters that their ballot selections were included within the reported election totals. These systems have been implemented in General US elections in the past, and indeed throughout the world. With that said, these systems are generally still in the research phase and often provide difficult usability barriers for voters to overcome.[29]

Support strong encryption

Secure connections are not created equal. Even cryptographic protocols already discussed to secure internet traffic have fallen prey to a number of attacks. To mitigate these issues, all traffic should be encrypted by TLS v1.2 or higher. Email providers and website managers should know what version of TLS was implemented and, if necessary, how to upgrade.

Support HTTP Strict Transport Security

If an attacker acts as a relay between a user and a website—a man-in-the-middle (MitM) attack—the attacker may be able to strip the secure connection and spy on the communication. HTTP Strict Transport Security (HSTS) is a web server security policy that lets browsers, such as Firefox, Internet Explorer and Chrome, know that they should only interact with the server using secure connections. Assuming a user has previously browsed a site and received the HSTS policy directive, the browser should remember the policy and a MitM downgrade attack should fail.

The problem is a first-time visit to a site. If a MitM attack happens in this scenario, the attacker could remove the HSTS policy directive from the header and still downgrade the connection. To mitigate this problem, sites should apply to be on the HSTS Preload list.[30] Browsers ship with HSTS lists to ensure downgrade attacks fail even on first load.

Conclusion

These recommendations serve as best practices that election officials can adopt in the 2019 and 2020 election cycles to improve the security of ballots transmitted and returned. While these security recommendations will not fully secure any of the above-described return methods, following them will mitigate some of the many risks inherent in, and many of the most common attacks facing the technologies used to support the return of voted ballots for UOCAVA voters. With that said, risk mitigation is not a one-time proposition. As technology continues to evolve, so must the people, process, and technology involved in elections.

[29] https://www.usenix.org/system/files/conference/evtwote14/jets_0203-acemyan.pdf
[30] https://hstspreload.org/

Acknowledgements

The Turnout, in conjunction with R. Michael Alvarez, PhD, and Magenta Sage Strategies, is deeply thankful to the Democracy Fund for their generous support of this work. They would also like to thank their colleagues who collaborated in preparing this document. John Dziurlaj and Joshua M. Franklin provided valuable content, document review and editing assistance. Stacey Scholl, Lindsay Daniels, and Tammy Patrick of the Democracy Fund lent subject matter expertise and editorial advice.