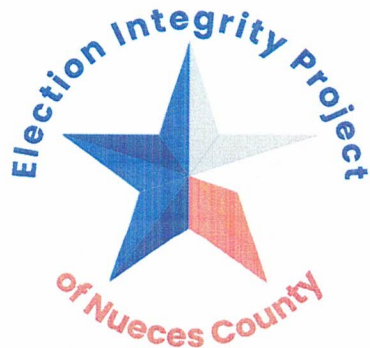


## **ACTIONS NECESSARY TO SECURE OVERSEAS VOTING**

- **What can the States do**
- **Suggestions for proof of overseas status of non-military**
- **Summary of security risks of online registration and electronic registration**
  - **Risk areas and risk matrix**
  - **Recommendations**



# WHAT IS LEFT TO THE STATES TO DECIDE?

| State Legislative Options         | More Secure                                                                          | Avoid               |
|-----------------------------------|--------------------------------------------------------------------------------------|---------------------|
| Separate Military v. Non-Military | Military Only Privileges                                                             | Combined            |
| FPCA Receipt Deadline             | 30 Days Prior to Election                                                            | No Deadline         |
| Residency Requirement             | Prior Residency                                                                      | Never Resided in US |
| Military ID Requirement           | DL, Military ID, SSN4                                                                | No ID               |
| Non-Military ID Requirement       | US Passport/DPOC /<br><i>TAX RETURN</i>                                              | No ID               |
| Non-Military Proof of Address     | Utility Bill, Lease<br><i>BANK RECORDS</i>                                           | No Proof of Address |
| Method for Return of Voted Ballot | <i>NEAREST EMBASSY / OTHER OFFICIAL</i><br>Return by Mail /<br><i>GOVERNMENT BAG</i> | Electronic Return   |
| Deadline for Return of Ballot     | Election Day in Office                                                               | Extended Deadline   |
| Ballot if Pending Verification    | Provisional Absentee                                                                 | Standard Ballot     |

# Security Risks in UOCAVA Online Registration and Electronic Ballot Transmission

## Executive Summary

Electronic services for UOCAVA voters improve access for military personnel, their families, and overseas citizens, but they also introduce significant cybersecurity and privacy risks. Online registration, electronic ballot requests, email delivery of blank ballots, and email return of voted ballots may be vulnerable to unauthorized access, interception, alteration, identity exposure, and service disruption. The highest-risk activity is the email return of voted ballots because it can compromise ballot secrecy and ballot integrity. Jurisdictions should apply layered security controls, provide clear voter notices, and preserve paper-based return methods whenever feasible.

## Background and Legal Context

UOCAVA was enacted by Congress in 1986 to protect the absentee voting rights of members of the uniformed services, certain family members, members of the Merchant Marine, and U.S. citizens residing outside the United States. The law requires states and territories to allow covered voters to register and vote absentee in federal elections, while many jurisdictions also extend related procedures to state and local elections.

A central feature of UOCAVA is the Federal Post Card Application, which allows eligible voters to register and request an absentee ballot through a single form. UOCAVA also provides for the Federal Write-In Absentee Ballot as a backup option when a voter has timely requested but not received a regular ballot. These tools are intended to reduce barriers caused by distance, deployment, unreliable mail service, and compressed election timelines.

The Military and Overseas Voter Empowerment Act of 2009 amended UOCAVA and strengthened federal requirements for serving military and overseas voters. Among other requirements, states must provide electronic options for UOCAVA voters to request and receive voter registration and absentee ballot materials, and states must transmit validly requested absentee ballots at least 45 days before a federal election when the request is received by the applicable deadline.

Federal law requires electronic transmission procedures to protect the security of the balloting process and, to the extent practicable, the privacy of each voter's identity and personal data. However, UOCAVA and the MOVE Act do not create a uniform national rule

for the electronic return of voted ballots. Methods for returning completed ballots, including whether email, fax, online portal, mail, or other methods are permitted, are generally determined by state law.

The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) protects the voting rights of eligible military personnel, their family members, and U.S. citizens residing outside the United States. To support timely participation, many jurisdictions provide online voter registration tools, electronic ballot request options, electronic delivery of blank ballots, and, in some cases, electronic return of voted ballots. While these services improve accessibility for voters who may face unreliable postal service or time constraints, they also introduce cybersecurity, privacy, and election-integrity risks that require careful management.

## Risk Areas

Online registration and electronic ballot request systems may be vulnerable if identity verification, account access controls, system monitoring, and data-protection practices are insufficient. Potential threats include unauthorized access, fraudulent requests, disruption of services, manipulation of voter information, and exposure of personally identifiable information.

The electronic delivery of blank ballots, including delivery by email, can also present risks to integrity and availability. A voter could receive an altered or delayed ballot if systems are compromised, email accounts are breached, or transmission channels are not adequately protected. Although electronic delivery of blank ballots is generally considered lower risk than electronic return of voted ballots, it still depends on secure systems, accurate voter authentication, and reliable communications.

The return of voted ballots by email creates the highest level of concern because the completed ballot may be exposed to interception, alteration, malware, spoofing, or unauthorized access during transmission or processing. Email-based ballot return can also weaken ballot secrecy because a voter's identity and ballot selections may be transmitted together or stored in systems not designed to preserve anonymity. These risks can affect confidentiality, integrity, availability, public confidence, and, in a large-scale incident, election outcomes.

## Risk Matrix

| Risk Area | Threat Scenario | Likelihood | Impact | Overall Risk | Mitigation Measures |
|-----------|-----------------|------------|--------|--------------|---------------------|
|-----------|-----------------|------------|--------|--------------|---------------------|

|                                 |                                                                                                                    |        |        |          |                                                                                                                                                   |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------|--------|--------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Online voter registration       | Unauthorized access, fraudulent account creation, or manipulation of voter information.                            | Medium | High   | High     | Strong identity verification, access controls, monitoring, audit logs, and routine vulnerability testing.                                         |
| Electronic ballot request       | Fraudulent or spoofed ballot requests submitted through insecure portals or compromised credentials.               | Medium | High   | High     | Multi-factor authentication, request validation, anomaly detection, and secure confirmation procedures.                                           |
| Email delivery of blank ballots | Ballot files delayed, intercepted, altered, or delivered to a compromised email account.                           | Medium | Medium | Medium   | Encrypted transmission where feasible, secure ballot download portals, voter verification, and delivery tracking.                                 |
| Email return of voted ballots   | Completed ballots intercepted, altered, exposed, or associated with voter identity during transmission or storage. | High   | High   | Critical | Limit use to voters with no practical alternative, provide clear risk notices, apply secure intake procedures, and preserve paper-return options. |
| Election system administration  | Administrative accounts compromised through phishing, weak passwords, or                                           | Medium | High   | High     | Phishing-resistant authentication, least-privilege access, administrator training, logging,                                                       |

|                   |                                                                                              |        |      |      |                                                                                                                                |
|-------------------|----------------------------------------------------------------------------------------------|--------|------|------|--------------------------------------------------------------------------------------------------------------------------------|
|                   | inadequate role separation.                                                                  |        |      |      | and incident-response planning.                                                                                                |
| Public confidence | Real or perceived weaknesses in electronic ballot systems reduce trust in election outcomes. | Medium | High | High | Transparent policies, public communication, post-election audits where applicable, and documented chain-of-custody procedures. |

## Security and Policy Implications

Election officials should treat electronic ballot services as high-value election infrastructure and **apply layered safeguards**. These include strong voter authentication, multi-factor authentication for administrative accounts, encryption in transit and at rest, secure logging, routine vulnerability testing, phishing-resistant email practices, incident-response planning, and clear chain-of-custody procedures for any ballot received electronically. Jurisdictions should also provide transparent voter notices explaining the privacy and security limitations of email ballot return.

Where electronic return is permitted by law, its use should be limited to voters who have no practical alternative for returning a ballot in time to be counted. **Paper return methods should remain the preferred option whenever feasible because they provide stronger auditability, better preservation of ballot secrecy, and a more reliable basis for post-election verification.**

## Recommendations

1. **Prioritize secure ballot return methods.** Jurisdictions should encourage paper-based ballot return whenever feasible and reserve email return for voters who have no practical alternative for meeting statutory deadlines.
2. **Strengthen voter authentication and request validation.** Online registration and ballot request systems should use robust identity verification, secure account access, anomaly detection, and confirmation procedures to reduce the risk of unauthorized or fraudulent activity.
3. **Protect electronic ballot delivery systems.** Election offices should use secure ballot delivery portals where available, encrypt ballot materials in transit and at rest,

monitor delivery activity, and maintain procedures for detecting altered, delayed, or misdirected ballot files.

4. **Apply strict controls to electronically returned ballots.** When email return is permitted, officials should implement secure intake procedures, segregate access to returned ballots, preserve chain-of-custody records, and minimize exposure of voter identity and ballot selections.
5. **Provide clear voter risk disclosures.** Voters who choose email or other electronic return methods should receive plain-language notices explaining the potential risks to ballot secrecy, confidentiality, and integrity before submitting a voted ballot electronically.
6. **Harden administrative systems.** Election offices should require multi-factor authentication for administrative users, apply least-privilege access, maintain secure logs, conduct phishing-awareness training, and routinely test systems for vulnerabilities.
7. **Maintain incident-response and continuity plans.** Jurisdictions should prepare for cyber incidents, service disruptions, and suspected ballot-transmission failures by establishing escalation procedures, backup communication channels, and documented recovery steps.
8. **Promote transparency and public confidence.** Election officials should publish clear procedures, document security controls, conduct post-election reviews where applicable, and communicate openly about how UOCAVA ballots are protected.

## Conclusion

UOCAVA electronic services play an important role in ensuring that military and overseas voters can participate in elections despite distance, deployment, and limited access to traditional mail. However, the same technologies that improve access can also create meaningful risks to ballot secrecy, system integrity, voter privacy, and public confidence. The return of voted ballots by email remains the most significant concern because it may expose both voter identity and ballot selections to interception, alteration, or unauthorized access. A balanced approach should preserve voter access while prioritizing secure ballot return methods, strong authentication, transparent voter disclosures, resilient election infrastructure, and documented safeguards that support both election integrity and public trust.