



THE COUNCIL OF STATE GOVERNMENTS

USING TECHNOLOGY TO ENHANCE MILITARY & OVERSEAS VOTING VOL. 1:

RECOMMENDATIONS FOR USE OF THE COMMON ACCESS CARDS
AND DIGITAL SIGNATURE VERIFICATION & UNREADABLE OR
DAMAGED BALLOT DUPLICATION METHODS.



The Council
of State
Governments

I. INTRODUCTION

In September 2013, The Council of State Governments, or CSG, entered into a cooperative agreement with the Federal Voting Assistance Program, or FVAP, launching the four-year, \$3.2 million Overseas Voting Initiative, or OVI.

The goal of this collaboration is to improve the voting process for citizens covered by the *Uniformed and Overseas Citizens Absentee Voting Act*,¹ or *UOCAVA*, specifically by improving the return rate of overseas absentee ballots. This effort augments FVAP's ongoing efforts to engage its stakeholders—especially state and local election offices—and improves the voting process for individuals covered under *UOCAVA* and for the election offices that implement its provisions.

The *Uniformed and Overseas Citizens Absentee Voting Act*, or *UOCAVA*, covers U.S. citizens who are active members of the Uniformed Services—the Army, Navy, Air Force, Marine Corps, and Coast Guard, the commissioned corps of the Public Health Service, and of the National Oceanic and Atmospheric Administration—and their eligible family members, members of the Merchant Marine and their eligible family members, and U.S. citizens residing outside the United States.

The Military and Overseas Voter Empowerment Act,² or MOVE Act, enacted in 2009, promoted the use of technology to address some of the long-standing issues that faced military personnel, dependents and overseas citizens covered by *UOCAVA*. Among other provisions, the MOVE Act required states to:

- Transmit ballots no later than 45 days prior to a federal election;
- Provide *UOCAVA* voters with the option to request and receive voter registration and absentee ballot applications by electronic transmission; and
- Give *UOCAVA* voters the option of receiving a blank absentee ballot via an electronic transmission method.

MOVE also required states to work to ensure that electronic transmission procedures protected the security of the balloting process and the privacy of voters who used these electronic transmission processes.

The Military and Overseas Voter Empowerment Act, or MOVE Act, expanded *UOCAVA* significantly in 2009, when Congress passed the law to provide greater protections for service members, their families and overseas citizens. Among other provisions, the MOVE Act requires states to transmit validly-requested absentee ballots to *UOCAVA* voters no later than 45 days before a federal election, when the request has been received by that date, except where the state has been granted an undue hardship waiver approved by the Department of Defense for that election.

Since the enactment of the MOVE Act amendments, there has been a need and desire to assist *UOCAVA* voters and the election officials who serve them, especially through the use of new technology solutions. Technology solutions include the implementation of U.S. Department of Defense Common Access Cards, or CACs, with digital signature verification for voter registration and absentee ballot requests, and methods for duplicating or resolving unreadable or damaged paper ballots that are mailed by *UOCAVA* voters back to their local election office. Improving these specific situations for *UOCAVA* voters will also help lower the risk of *UOCAVA* ballot rejection and optimize these voters' opportunity for success.

The U.S. Election Assistance Commission, or EAC, administers the biennial Election Administration and Voting Survey, or EAVS, to collect state-by-state data on the administration of federal elections. The EAVS reports include data on the ability of civilians, military members and overseas citizens to successfully cast a ballot and contain the most comprehensive, nationwide data about election administration in the United States. It is a survey of all states, the District of Columbia, Guam, Puerto Rico, American Samoa and the U.S. Virgin Islands.

CSG OVERSEAS VOTING INITIATIVE: TECHNOLOGY WORKING GROUP

One major component of CSG OVI was the creation of a technology working group to study ways technology could be used to enhance the voting process for military and overseas citizens. CSG and FVAP recognized that election officials across the country were incorporating innovative technologies to improve the voting process, including improvement of the *UOCAVA* voting experience, and set forth to draft best practices in this area based on this group's work.

The CSG OVI's Technology Working Group was comprised of state and local election officials from across the United States, who came together to identify ways in which the election experience for *UOCAVA* voters could be improved in the specific area of technology. Working together, the group identified three primary areas where state and local governments can use technology to improve the *UOCAVA* process: digital signing using the DOD CAC, duplication of damaged or machine unreadable ballots, and the standardization of data collection.

II. DEPARTMENT OF DEFENSE COMMON ACCESS CARDS AND DIGITAL SIGNING

The U.S. Department of Defense Common Access Card (CAC)

A DOD CAC is only issued to individuals who have completed a background check process.³ The card serves as identification for both in-person and digital interactions and contains:

- Information about the person, such as demographic data (e.g., gender, date of birth), personnel information (e.g., military branch or contractor role, pay grade), and biometrics (e.g., fingerprints, a photo of the CAC holder's face);
- The appropriate PKI Certificates for identity, signature, encryption and personal identity verification authority; and
- The individual's credential data (i.e., the card holder's unique identifiers).

Much like with an ATM card, a CAC is a form of multifactor authentication. It requires something you have (the CAC itself) and something you know (a personal identification number, or PIN) for authentication to occur. The PIN is selected by the user when he or she receives a CAC. When the CAC is inserted into a computer, the user enters his or her PIN, which authenticates the user to the system.

To illustrate, a CAC allows a soldier (Mike) to digitally "sign" a document. Mike would like to register to vote and is absent from his voting residence. He could use his CAC's digital signature certificate to sign his FPCA form with his private key. Because Mike's public key is attached to his registration when he signed with his digital signature, Mike's local election official, or LEO, can determine it has not been modified since it was digitally signed.

The LEO can make this assumption because the document received was automatically validated by a trusted Certificate Authority. If the validation fails, it tells the LEO that Mike did not send the document or that it has been altered since being digitally signed. Once a state or local election office receives a digitally signed document, the software that is used to open the document (e.g. Adobe Acrobat Reader) will validate the digital signature certificate with the trusted Certificate Authorities.⁴ This automatic validation provides the recipient(s) with the ability to authenticate whether a document signed using a CAC was valid (sent by a person with a valid certificate)—or invalid (sent by someone with an expired or revoked certificate) in addition to whether the document has been modified since it was signed with a digital certificate.

TREATING CAC SIGNATURES LIKE "WET" SIGNATURES

The OVI Technology Working Group noted that the current process of signature verification uses a wet, or handwritten, signature given by an individual in an official capacity to a government representative (e.g., at the Department of Motor Vehicles or at a polling location). Once on file, this becomes the reference signature for subsequent interactions between the voter and the election office. Because the U.S. DOD issues a CAC, it has many of the same qualities as a wet signature. States must treat the CAC digital signature like a wet signature.

Several federal laws support the use of electronic signatures. The key concern with accepting any signature—an electronic signature or digitized signature—relates to challenges to the enforceability of the signature. The likelihood of these challenges can be evaluated using risk analysis that takes into consideration: (1) the likelihood of a successful challenge to the validity and enforceability of the signature, and (2) the adverse impact that would result from a successful challenge. These risks can be substantially reduced by using the DOD as the trusted credentialing authority.

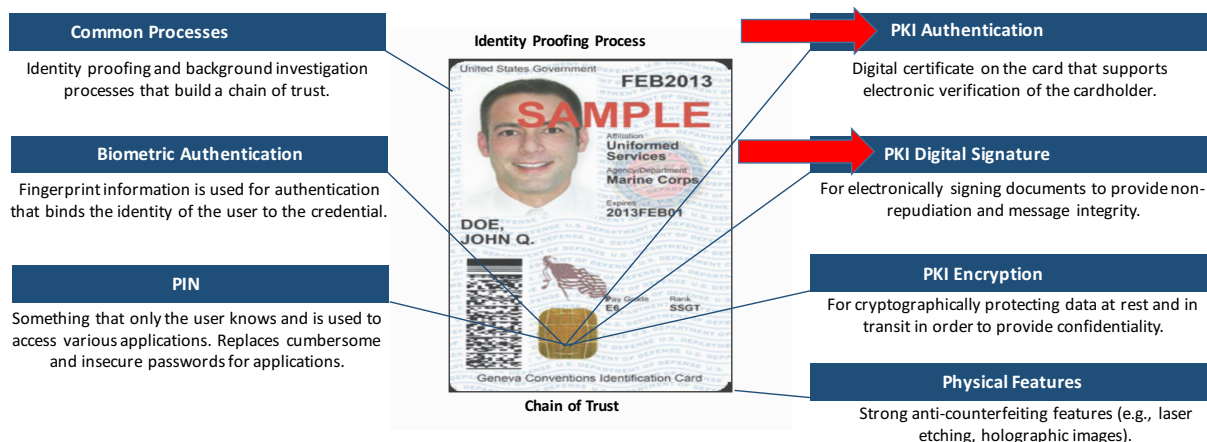


Figure 3 - The CAC contains a significant amount of data as is described in this visual from FVAP.

The primary issue with using a CAC as a signature mechanism in elections is that a state would have to make a digital signature, created by the signature certificate on the CAC, valid on election materials. As Vicki Renteria-Silva, a project manager in the Credentialing Division of the Defense Manpower Data Center, or DMDC, noted in her presentation to the OVI's CAC/Digital Signature Verification Subgroup,

“Any mark made with the intent to sign normally would be recognized by a court as a signature. ... The important issue... is how have you documented the signatory's “intent to sign” (usually addressed by a pop-up that says by proceeding to put in your PIN, etc. you will sign the document), and how secure the system is so that documents cannot easily be signed and changed, or signed by someone other than the intended person. ... It becomes a risk management decision.”⁵

The OVI Technology Working Group recommends that state laws address several key principles to best serve the *UOCAVA* population. First, laws related to the use of digital signatures should avoid being too specific. A law based on specific principles, instead of a current technology, will remain relevant over time as cryptographic methods and technologies change. Second, laws should treat signatures equally whenever possible. States that accept electronic signatures for some transactions should consider accepting electronic signatures on election documents.

The OVI Technology Working Group recognizes that state and local election offices play a central role in coordinating and providing services to their *UOCAVA* voters. Given that there is variation in states' acceptance of an FPCA signed with an electronic signature and how states process the FPCA, states will be in the best position to work in conjunction with local election offices to reconcile state requirements and help educate their *UOCAVA* population about their electronic signature options. FVAP, as a component of the DOD, is well positioned to assist with the education process and work directly with the states and local election offices as they consider the use of electronic signatures in the voter registration and absentee ballot request process.

ISSUES ASSOCIATED WITH USING CACS FOR SIGNATURES

The use of CACs is not without some limitations. As a part of its work on *UOCAVA* voting, FVAP has conducted studies examining the issues surrounding using CACs as a signature tool for elections.⁶ In 2015, FVAP issued a report on the use of CACs in the context of elections administration that discussed how an active CAC can be used to provide an electronic signature in the voting process without additional DOD involvement. This research found that use of only the CAC as a signature tool would likely rule out participation of non-DOD *UOCAVA* voters: U.S. civilians working, living or traveling overseas. There are also political

risks that may arise from integrating any voting process too closely with a given DOD system. If people view CAC infrastructure as playing a key role in transmitting ballot materials, then it could be seen as the federal government, in particular the DOD, being directly involved in conducting elections.

Another key limitation on the use of the CAC in elections is that it excludes all overseas citizens and military dependents who do not have a CAC. There are many individuals—such as federal employees with non-DOD agencies—who have a personal identity verification, or PIV, cards. Also, it is possible for a citizen to obtain a trusted online digital signature. However, it would be incumbent on the local or state election office to ensure that the issuing authority had a thorough process for validating an individual's identity. This could be mitigated, in part, by the state being able to match the voter to an existing driver's license file—as is done with online voter registrations. Such a match would also provide the local election office with a digital version of the voter's wet signature from a driver's license.

Many Service members face obstacles when they attempt to vote. Mail transit time is a critical challenge faced by individuals covered by the *UOCAVA* when registering to vote and casting their ballot. The time it takes for voting materials to go back and forth between an election office and a *UOCAVA* voter can sometimes be quite lengthy, from a matter of days to several weeks. This is because a voting transaction is the combination of the time it takes a voter to send a voter registration application and ballot request form (i.e., the Federal Post Card Application, or FPCA) to their local election office, or LEO, for the LEO to process the form, for the ballot sent by the LEO to reach the voter, for the voter to mark the ballot, and finally for the ballot to reach the LEO. Only then is a vote processed and counted.

The *UOCAVA* process is made more complicated for these voters when they have to return a document requiring a “wet” (handwritten) signature. The FPCA and state *UOCAVA* registration forms are most commonly accessed online and can even be filled out on a computer. However, the wet signature component requires the form to be printed, signed and then either mailed back to the LEO or scanned and emailed to the LEO. Many individuals living away from their voting residence lack access to printers and/or scanners, which makes it difficult to electronically return a document with a wet signature. Returning these documents by mail adds time to the application and ballot request process, which affects the voter's ability to meet legally established election deadlines.

DIGITIZED, ELECTRONIC & DIGITAL SIGNATURES


A **DIGITIZED SIGNATURE** is a handwritten signature that has been transferred into an electronic form—it is recognizable as a signature when examined visually. It is typically an image of a handwritten signature or a signature

captured from a signature pad.

An **ELECTRONIC SIGNATURE** is the term used for the electronic equivalent of a handwritten signature. It is a generic, technology-neutral term that refers to all the various methods by which one can “sign” an electronic record, including digital signatures, biometrics or personal identifying numbers. An electronic signature process authenticates the signer’s identity, binds the signature to the document and ensures that the signature cannot be altered after it is affixed.

A **DIGITAL SIGNATURE** is the term used to describe the encrypted data produced when a specific mathematical process involving a hash algorithm and public key cryptography is applied to an electronic record and is used to verify the veracity of an electronic signature. For the purpose of the OVI Technology Working Group, all recommendations assume the use of the CAC digital signature and the associated trust environment. Because the U.S. Department of Defense uses a digital signature technology to generate and authenticate electronic signatures, and the concern of the subgroup focused on both the signature and the authentication of the signature, the term digital signature is used in this section.

COMMON ACCESS CARD/DIGITAL SIGNATURE VERIFICATION

Digital Signature =  Signature + Digital Certificate

Digital Signature Security

- entirely electronic (no printer or scanner needed)
- encrypt document
- limit who can open document
- authenticate sender
- verify document has not been modified




Figure 1- The chip on the CAC contains the cardholder’s digital signature. A digital signature provides additional security and privacy when signing and transmitting documents electronically. This is accomplished by attaching a digital certificate to the document being signed. The addition of a digital certificate is what makes a digital signature different from an electronic signature, which is image of a signature. Additional security and privacy benefits include the ability to: sign documents electronically, without the need for a printer and scanner; encrypt documents; and limit who can open the document. Recipients of a digitally signed document can: authenticate the sender and verify document has not been modified since it was digitally signed.

Military personnel, DOD, civilian employees, eligible contractor personnel and certain other individuals can sign e-documents securely and electronically by using their CAC’s digital certificate to create a digital signature.⁷ A digital signature can be legally equivalent to a wet signature if states allow that use. States could make it far easier for CAC holders to register to vote when they are deployed or overseas by accepting and trusting the digital signature produced by the CAC.

The Common Access Card/Digital Signature Verification Subgroup studied the ability of military personnel, DOD civilian employees, eligible contractor personnel and certain other individuals to sign documents securely



Figure 2- The Common Access Card (CAC) is the standard identification for the U.S. Department of Defense. The CAC is a “smart” card and is also used to access to buildings, controlled spaces, as well as the DoD computer network and systems. It stores information on four layers: 1) the card itself, with readable information and images printed on the card, the barcodes and magnetic strip, 2) the RFID antenna embedded in-between the layers of the card, 3) the antenna provides contactless physical access, such as buildings and doors, and 4) the chip, which is used for computer login, two factor user authentication, and document signing.

and electronically using the CAC digital signature.⁸ The subgroup also considered the state of Nevada's pilot project where they allowed their LEOs to accept election documents that had been signed with a CAC digital signature. This pilot project identified many of the key issues associated with using a CAC in the context of elections. Before delving into Nevada's experience using a CAC for signing election materials, it is important to first review how digital signatures work and how they compare to conventional wet signatures.

AN OVERVIEW OF DIGITAL SIGNATURES

An Overview of Digital Signatures

Digital signatures are used within a public key infrastructure, or PKI—that is, a combination of products, services, facilities, policies, procedures, agreements and people—that provides for and sustains secure interactions on open networks such as the internet. PKI is not a single monolithic entity, but a distributed system in which the components may include multiple agency-specific public key infrastructures which are interoperable and interconnected. The infrastructure provides assurances that information is protected while being entered, during transit and when stored.⁹

Through digital signatures and encryption, PKI provides four basic security services:

1. Identification and authentication services establish the authenticity of a transmission, messages and its originator. The goal is for the receiver of the signed transmission to be able to verify the identity of the sender of the transmission.
2. Data integrity services address the unauthorized or accidental modification of data, such as data insertion, deletion and modification. A system must be able to detect unauthorized data modification to ensure data integrity. The goal is for the receiver of the transmission to be able to detect if data have been altered.
3. Nonrepudiation services prevent an individual from denying that a previous action has been performed. The goal is to ensure that the recipient of a transmission can be assured of the sender's identity.
4. Confidentiality services restrict access to the content of sensitive data to only those individuals who are authorized to view the data. Confidentiality measures prevent the unauthorized disclosure of information to unauthorized individuals.

A certificate authority acts as a notary in a PKI.¹⁰ It issues a public key certificate (digital certificate) for each identity and this confirms that the identity has the appropriate credentials. The digital certificate includes the public key and the time the certificate is valid. Each certificate authority also keeps a certification revocation list, which lists certificates that have been revoked for reasons such as

lost or stolen CAC or people leaving an organization that issued the certificate. In addition to checking the certificate authority trust chain when validating a certificate, it is also very important to check the certification revocation list to ensure the certificate is not on the list. The DOD is the certificate authority for CACs, and it has a very robust process for ensuring that the certificates it issues are up to date and issued by a trusted source.

COMMON ACCESS CARD/DIGITAL SIGNATURE VERIFICATION RECOMMENDATIONS

RECOMMENDATION: States should allow the use of a CAC electronic signature to complete election-related activities (For example, when submitting a FPCA to register to vote.), when requesting an absentee ballot, and when indicating UOCAVA voting status via a state's online election portal.

RECOMMENDATION: State laws should accommodate the use of electronic signatures in the election process for UOCAVA voters as they have in other sectors.

RECOMMENDATION: State election offices should develop procedures and training materials in cooperation with FVAP and their local election offices regarding acceptance and use of a CAC electronic signature.

CASE STUDY: NEVADA EASE GRANT PROJECT AND USE OF CAC

As a recipient of FVAP's Effective Absentee Systems for Elections, or EASE, grant initiative, the state of Nevada created an online ballot delivery system, which seamlessly integrates registration, request and ballot delivery into one electronic process. This system mimics the existing process in Nevada, requiring local jurisdictions to process applications for voter registration and request an absent ballot, as well as receive a marked absentee ballot according to the existing process for each.

One key aspect of the Nevada EASE project is that it's built upon a legal foundation¹¹ that permits UOCAVA voters to use electronic and digital signatures to sign registrations, ballot requests and ballot materials. The Nevada Legislature allows electronic and digital signatures to reduce barriers encountered by UOCAVA voters. These voters are often without access to a printer and/or scanner so are less likely to return their ballot because of the additional steps necessary to sign their documents with a wet signature.

Signing with an electronic signature works the same way as Nevada's online voter registration, which utilizes the image of the user's existing signature, when available, to sign their voter registration application being submitted via the online system. The use of a digital signature varies

slightly from that of an electronic signature by way of being applied. Both electronic and digital signatures can be used to sign election documents, but digital signatures must be directly applied in order to attach their digital certificate to the document. Digital signatures also provide local election officials with an additional, optional, way to authenticate a document through the digital signature certificate attached to the document. The certificate provides additional security, such as document encryption, as well as detail about the document such as authentication of the user and the contents within the document, i.e. whether any edits or modifications were made to the document since signing.

Nevada’s EASE grant project is the first entirely online application. Assembly Bill 175, passed during the 2013 legislative session, authorizes covered voters to use digital or electronic signatures to sign applications to register to vote and apply to receive military-overseas ballots. Previously, military and other Nevadans covered by the UOCAVA were required to submit their ballots by mail or they needed a printer and a scanner to receive, mark and return their documents via email.

Nevada’s EASE grant solution retrieves the electronic image of the voter’s signature already on file with their county clerk or registrar or from the Nevada Department of Motor Vehicles, so it can be used by the voter to register to vote, request an absent ballot or return an absent ballot, negating the requirement of printing and signing the ballot before returning it. After a military or overseas voter marks his or her own ballot through the EASE solution, the system applies the voter’s electronic signature to the ballot and generates a cover sheet with the necessary declarations,

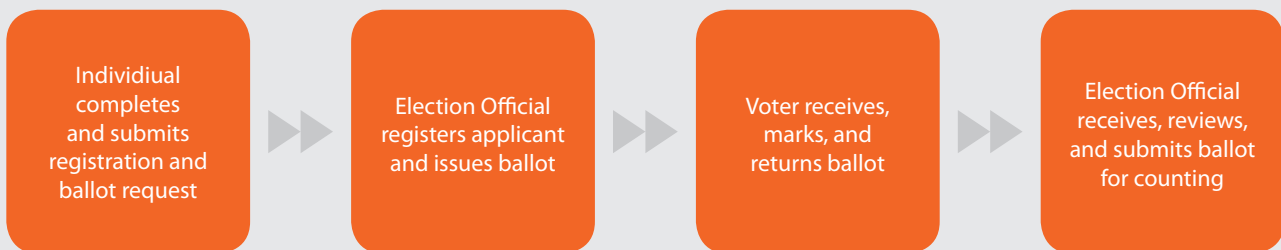
affirmations and information to allow the counties to process and count the military or overseas absent ballot. When finished, an EASE solution user has the option of saving the ballot materials as a PDF file and emailing the document as an attachment to the respective county clerk or registrar’s office, or printing it and returning by mail or fax. Users must return their completed documents and ballot to their Nevada election office independent of the EASE solution. The Nevada EASE solution does not return any documents or information for a user.

In 2014, the EASE solution was made available to all Nevada UOCAVA voters during a soft launch. During the general election, 208 voters generated their ballot using EASE. Over 63 percent of these users were credited with participation.

In 2016, the Nevada EASE solution was used by 2,192 voters to generate their ballots for the general election. Over 73 percent of these users were credited with participation in the election. Not only does the EASE solution facilitate the state’s military and overseas voters with the highest ballot return rate among other ballot types, EASE solution ballots are also the least likely to be rejected due to missed deadlines or issues with a voter’s signature.

According to results from the 2012 EAVS, not receiving on time or missed deadlines are the most common reasons a UOCAVA ballot is rejected. Of the users that generated a ballot via the EASE solution, 384 users were not registered to vote and able to simultaneously submit their voter registration applications with their ballots. Because users are able to submit their documents electronically simultaneously with their requests and balloting documents, EASE solution users are less likely to have their documents or ballots rejected due to a missed deadline or

NEVADA REGULAR VOTER REGISTRATION & UOCAVA BALLOT REQUEST PROCESS



NEVADA EASE VOTER REGISTRATION & UOCAVA BALLOT REQUEST PROCESS

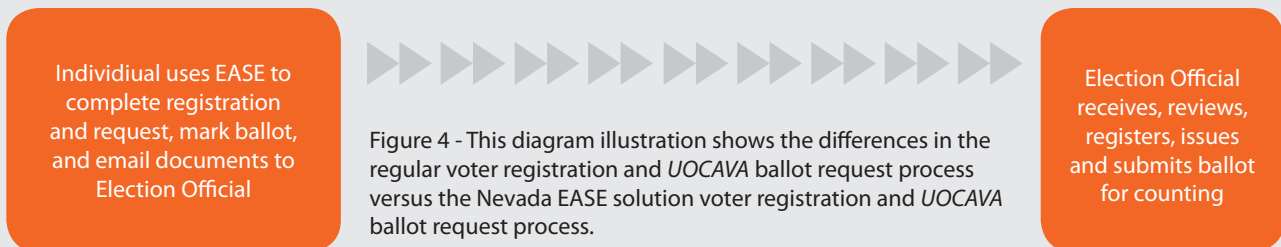


Figure 4 - This diagram illustration shows the differences in the regular voter registration and UOCAVA ballot request process versus the Nevada EASE solution voter registration and UOCAVA ballot request process.

the materials not being received.

Problems with required voter signatures are the second most common reason a *UOCAVA* ballot is rejected. Because the EASE solution provides users with their existing signatures on record for over 90 percent of users, the system is able to significantly reduce *UOCAVA* ballots rejected in Nevada for signature issues. During the 2016 general election, the EASE solution successfully provided 2,064 users with their signatures from an existing record. Of these signatures, 1,727 were provided from the user's existing voter registration record and 337 signatures were provided from an EASE solution user's existing Department of Motor Vehicle record. Additionally, 55 individuals used their CACs to access and provide certain information in the EASE solution.

EASE solution users that use their CACs to access and prefill fields in the EASE solution are significantly less likely to have their identity questioned. This is due to the additional, optional, resources available to the local election official to authenticate the person submitting registration, request and balloting documents, such as the digital certificate attached to a file with the user's digital signature.

The traditional voting process requires a *UOCAVA* voter to submit an FPCA, which is then processed. The election official then issues the voter a ballot, which is transmitted to the voter by mail or electronically (typically by email), and the voter then receives the ballot, marks it and returns it. The returned ballot is then processed. The EASE process is intended to promote electronic ballot delivery and ballot return through an electronic portal. Instead of the ballot being emailed, the voter downloads the ballot from the portal, can potentially mark the ballot electronically, then can return the ballot using the portal. The EASE process overcomes problems associated with email and potentially provides an opportunity to mark the ballot electronically. Some EASE systems also facilitate the registration and ballot request process as well.

III. DUPLICATION OF DAMAGED OR MACHINE-UNREADABLE BALLOTS

In all states, Washington, D.C., and the five U.S. territories, groups of voters who meet certain qualifications determined by that jurisdiction can cast paper ballots using a vote by mail or absentee voting process. Many of these voters are *UOCAVA* voters and do not have the option to vote in person within their voting jurisdiction. According to the U.S. Election Assistance Commission's, or EAC's, Election

Administration and Voting Survey, or EAVS, in the November 2014 general election, more than 14 million absentee ballots were cast nationwide. In the 2012 general election, more than 22.5 million absentee ballots were cast.¹²

Voters covered by the *UOCAVA* typically receive and return their ballots by mail; in many states, the only way a ballot can be returned is via mail. However, with the passage of the MOVE Act, all *UOCAVA* voters can receive their ballots electronically—typically, by email or via an online portal. Some states allow ballots to be returned electronically as well, most commonly by fax or email.

PROBLEM BALLOTS

In almost all local election jurisdictions, paper ballots are tabulated electronically, using some form of ballot scanning technology. There are four common problems that arise, rendering paper ballots difficult or impossible to process

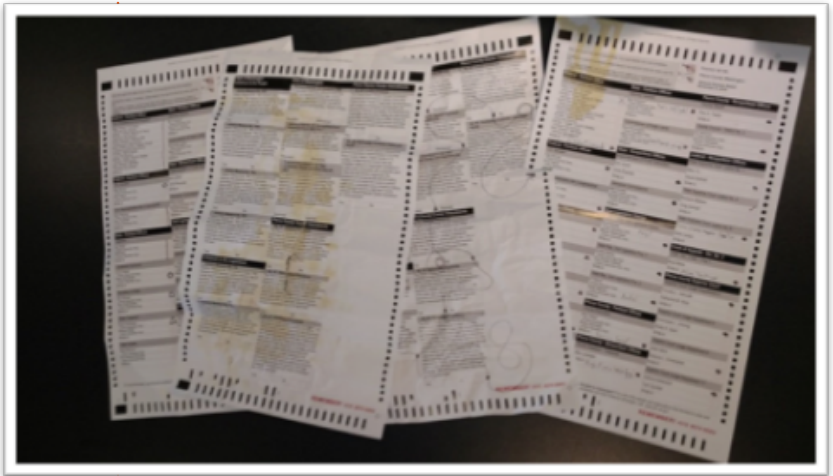


Figure 5 - This photograph shows actual damaged ballots that are not able to be read by ballot tabulators without duplication. Image provided by the Okaloosa County, Florida Supervisor of Elections' office.

with a ballot tabulation system. They are:

1. Ballots can be torn or damaged by the voter or during the mailing process. Coffee spills, wrinkles and tears interfere with ballots being scanned.
2. Ballots can be filled out with inappropriate marking implements—pencils, highlighters, colored pens, chalk, cosmetic pencils, paints, crayons and colored art pencils—that a tabulation system cannot process.
3. The voter may mark the ballot inappropriately (e.g., circling a candidate's name instead of marking it as instructed) so that the voter's intent may be clear under a state's election laws but marked in a way that a tabulation system cannot read. Stray marks can also interfere with the tabulation process.
4. The returned ballot may not be (1) the appropriate paper stock quality and weight, (2) the correct size, (3)

the correct orientation (portrait or landscape), or (4) sized so that the voting marks and ballot positions can be read by the scanner and the ballot tabulated.

The last problem occurs most often when UOCAVA voters have requested a ballot electronically. These ballots are typically not printed on paper that is the same weight as regular paper ballots and are often printed on A-4 sized paper, which is the global paper standard size outside the

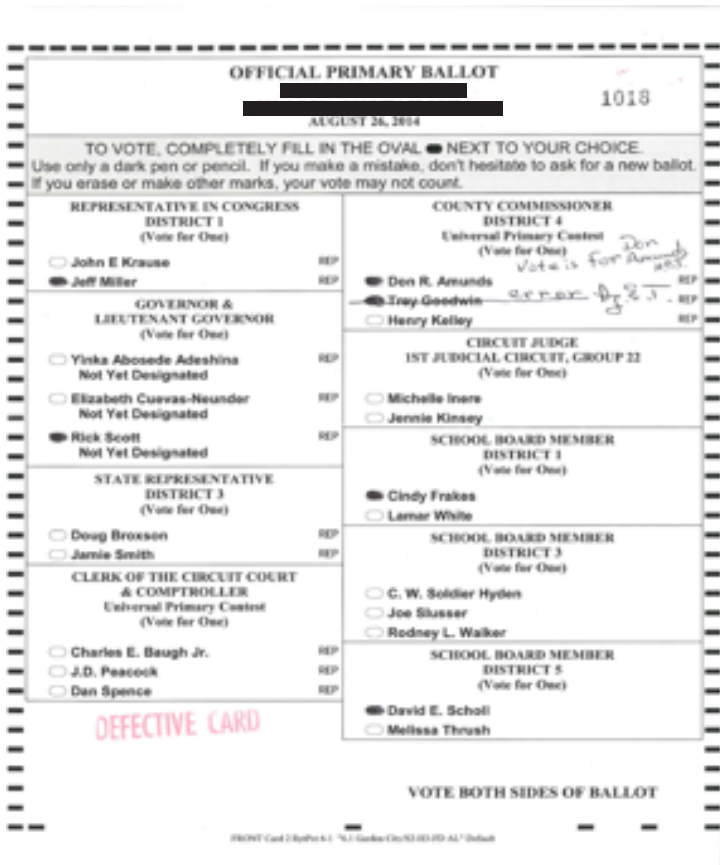


Figure 6 - This is a scan of an actual damaged ballot that was not able to be read by ballot tabulators without duplication due to a voter writing on the ballot outside the ovals. This is an actual ballot provided to the OVI for the purposes of studying ballot duplication with the jurisdictional information removed.

United States. Additionally, some voters either reduce or enlarge the ballot; both actions reduce image quality.

HANDLING PROBLEM BALLOTS: HAND COUNTING OR BALLOT DUPLICATION

Problem ballots cannot be automatically processed by a vote tabulation system and require some sort of special handling. To that end, the OVI conducted a survey of state election offices to determine the ways in which states processed problem ballots. The survey found that, in general, there are two ways in which problem ballots are processed: hand-counting and ballot duplication.

In this survey of states regarding their ballot duplication policies, 26 states provided information about how they handle ballot duplication. There are five states that require ballots to be hand counted—no ballot duplication is allowed in these states—and two states allow duplication in some cases. There are 19 states that require problem ballots to be duplicated, of which eight have an administrative rule requiring duplication, 10 require duplication under state statute, and one has a state policy requiring duplication. Four states allow for the use of technology in the ballot duplication process. Duplication in all states requires that the activity be conducted by teams of individuals—a minimum of two people—or be conducted in front of witnesses.

HAND COUNT

With hand counting, the problem ballots are segregated from the ballots that can be automatically tabulated. Each problem ballot is then typically examined by two or more individuals, who examine the ballot markings and then tally the vote choice based on their common agreement of the voter's selection.

MAINE'S STATUTE FOR HAND COUNTING BALLOTS

21-A M.R.S §695 (2013). Counting of ballots

1. Counted in public. The ballots must be counted publicly so that those present may observe the proceedings.
2. Separated into lots. In counting the ballots, the election clerks shall form into counting teams of 2 election clerks, each of whom has a different party affiliation. The counting teams shall separate the ballots into distinct lots. Each of these lots must consist of 50 ballots, except for one lot, which may have less than 50 ballots. Each counting team shall use one of the approved counting methods prescribed by the Secretary of State to produce 2 tally sheets for each lot that are in complete agreement as to the count for each candidate and question choice. They shall place with each lot one of the tally sheets for that lot that is signed by the election clerks who made the count. They shall wrap the tally sheet around the outside of the applicable lot of ballots. The 2nd tally sheet for each lot must be provided to the warden for use in completing a total tally of each office and question and for completing the election return.

Figure 7- This is an excerpt from Maine's 2013 state statute for the hand counting of ballots describing the process followed in the state as prescribed by law. See additional information on this statute at <http://legislature.maine.gov/statutes/21-A/title21-Asec695.pdf>.



Figure 8 - This is an actual ballot with its outer return envelope that was damaged on its way through the postal system from a voter to the local election office. Photo of the ballot envelope was provided by the Okaloosa County, Florida Supervisor of Elections' office.

BALLOT DUPLICATION METHODS

The other way in which problem ballots can be handled is through some form of ballot remaking or duplication.¹³ Some states require or encourage ballots to be duplicated so the votes can be counted by the tabulator. In general, ballot duplication involves transferring the voter's choices to a new paper ballot and creating an audit record (e.g., numbering the original ballot and the duplicated ballot) so that the original and duplicated ballots can be linked throughout the tabulation and election certification process.

The CSG OVI Technology Working Group recognized that the laws, policies and procedures for ballot duplication vary by state. Taking that into account, the working group members noted that jurisdictions should ensure that their process for ballot duplication meet basic auditing standards. This would include having at least two individuals overseeing the duplication of any ballot and having a process to confirm that the duplicated ballot is

accurate. An audit log should exist so that the original ballot can be linked to the duplicated one. For example, the duplicated ballots might be marked with a number, so they can be re-connected should a question arise, but not in such a manner that the voter can be identified. The Wyoming statute regarding ballot duplication is an example of a law that has most of these components.

WYOMING SECRETARY OF STATE

RULES FOR ESTABLISHING STANDARDS FOR COUNTING DAMAGED BALLOTS – CHAPTER 6

SECTION 1. AUTHORITY

These rules are authorized by W.S. 22-14-114.

SECTION 2. PURPOSE

These rules are promulgated to establish standards and procedures for counting damaged absentee ballots that have been rejected by the appropriate counting system.

SECTION 3. APPLICABILITY

(a) These rules apply to the handling of absentee ballots that are returned to the county clerk in such condition that the appropriate counting device rejects them, e.g. they may be wrinkled, the bar code may be soiled, they may be torn and so forth.

(b) Despite the damage, the ballots must clearly express the intent of the voters casting them in order to be counted by the tabulating device. When the intent is clear on the damaged ballots, they may be duplicated and counted.

SECTION 4. DUPLICATING BOARD

(a) At each polling place, the "duplicating board" shall be a subdivision of the counting board or of the election judges appointed to count the absentee ballots in that precinct or counting center. The duplicating board shall consist of at least three individuals of different political affiliation, where possible, responsible for duplicating the damaged ballots that the voting machine has rejected.

(b) Each duplicate ballot shall be a true copy of the original with the effect of the damage removed. Each duplicate ballot shall be marked "duplicate" and have a control number recorded on it that is also recorded on the original ballot.

SECTION 5. BALLOTS THAT CANNOT BE TABULATED

(a) Damaged ballots that cannot be counted by a tabulating machine shall be duplicated by the counting board, duplicating board or the election judges.

(i) Three election judges shall duplicate the ballot.

(ii) One election judge shall read the vote off the official ballot and the second election judge shall mark a blank ballot with that vote. The third election judge shall witness the duplication process.

(b) The original ballot shall be marked as original ballot and then given a number.

(c) The duplicate ballot shall have “duplicate ballot” written on the ballot, along with the number given to the original ballot.

SECTION 6. COUNTING OF DUPLICATE BALLOTS

(a) The duplicate ballots shall be counted by the tabulating machine along with the other absentee ballots and the vote tallies added to the precinct or counting center totals and reported together.

(b) The original ballot shall be retained in a “duplicated ballot” container.

(c) All rejected, spoiled or duplicated ballots shall be kept for a minimum of 22 months or until any election contest affected by the ballots has been terminated.

THE USE OF TECHNOLOGY IN BALLOT DUPLICATION

Small jurisdictions may only have a few ballots that need to be duplicated but mid-sized and large jurisdictions may duplicate a large number of ballots every election. Ballot duplication can be a time-consuming process when done entirely by hand. In a large jurisdiction, like Orange County, California, for example, more than 13,000 ballots may need to be duplicated for an election. Fortunately, there are technologies that can simplify this process and facilitate accurate and efficient ballot duplication. One key issue with any use of technology in duplication is the tradeoff between factors such as speed, reliability, transparency and accuracy in the duplication process.

BAR CODES

As a part of the OVI survey of state ballot duplication procedures and experiences, three states—Maryland, Oklahoma and Washington—reported using barcode technology as a part of their ballot duplication efforts. In these states, the state, or counties within the state, utilized an online ballot marking tool as a part of their online ballot delivery solution. Once a ballot is marked using the tool, it can be printed. During the printing process, a barcode is included on the ballot. When the ballot is returned to the local election office, the barcode can be scanned and it will reproduce the vote choices on the voter’s ballot. (The barcode does not include any information about the voter.) Once the duplicate ballot is printed on a standard ballot paper, the original and duplicated ballot can be reviewed by a verification team, logged, and the duplicated ballot counted using a scanner.

AUTOMATED BALLOT DUPLICATION USING SCANNING/SCRAPING

There are several technologies that providers have developed that will automate the ballot duplication process. In general, these technologies take the original ballot, scan it, and identify the markings made by the voter. These marks are then “scraped” from the PDF of the scanned original ballot using image processing. These scraped markings

can then be exported and placed onto a blank ballot. The benefits associated with these technologies are that they can more quickly and accurately populate a ballot that needs to be duplicated, with election workers checking to ensure that the new ballots were populated correctly. These technologies typically allow the scanned ballot to be viewed on a screen with the proposed new ballot so that the original and duplicate ballot can be compared. The CSG OVI Unreadable/Damaged Ballot Duplication Methods Subgroup examined many of the different technologies that can be used to duplicate ballots.

The New Jersey Electronic Ballot Duplication System Project report,¹⁴ which was prepared by Scytl, an election technology solutions provider, for the state of New Jersey under an EASE Grant from FVAP, provides an overview of one such technology and discusses some of the issues related to the use of technology in ballot duplication. The report includes a set of criteria that should be evaluated in comparing whether to use automated ballot duplication instead of manually duplicating a ballot. These criteria include cost, auditability, transparency, accuracy, ease of use, speed, reliability and scalability.

The CSG OVI Technology Working Group recommended that technologies for ballot duplication be easy to use and promote transparency. There are a variety of technologies that can assist election officials in duplicating ballots by automating the process. Ballot duplication technologies should enlist simple and intuitive on-screen navigations that prevents errors in the process. These technologies may include features such as providing a side-by-side on-screen comparison between the original and the duplicated ballots in order to facilitate accuracy in the process, or producing a printed ballot that provides auditability and additional transparency.

RECOMMENDATIONS OF THE UNREADABLE/DAMAGED BALLOT DUPLICATION SUBGROUP

RECOMMENDATION: State and local jurisdictions should select a ballot duplication process that is appropriate for the number of paper ballots they process.

RECOMMENDATION: Regardless of whether a jurisdiction uses a manual or an electronic ballot duplication process, there should be clear procedures that ensure auditability.

RECOMMENDATION: Technologies for ballot duplication should be easy-to-use and promote transparency.

RECOMMENDATIONS¹⁵

Following are the recommendations of the Common Access Card/Digital Signature Verification Subgroup of the CSG OVI Technology Working Group:

1. Recommendation: States should allow the use of a CAC electronic signature to complete election-related activities such as submitting a Federal Post Card Application to register to vote, requesting an absentee ballot and indicating *UOCAVA* voting status via a state's online election portal. The OVI Technology Working Group notes that the current process of signature verification uses a wet, or handwritten, signature given by an individual in an official capacity to a government representative—at the Department of Motor Vehicles, at a polling location, etc.—which is used as a reference signature for subsequent interactions between the voter and the election office. Just like the process for accepting a wet signature described above, a DOD CAC also is issued by a governmental official at a government facility. In 2015, FVAP issued a report on the use of CACs in the context of elections administration that discussed how an active CAC can be used to provide an electronic signature in the voting process without additional DOD involvement.¹⁶ There are several federal laws that support the use of electronic signatures. Perhaps the most important is the Electronic Signatures in Global and National Commerce Act. The key concern with accepting any signature—an electronic signature or digitized signature—relates to the potential challenges to the enforceability of the signature. This issue can be evaluated using a risk analysis, which should consider the likelihood of a successful challenge to the validity of the signature, and the adverse impact that would result from such a successful challenge to the enforceability of the signature. These risks are substantially reduced, if not eliminated entirely, by leveraging the DOD as the trusted credentialing authority.
2. Recommendation: State laws should accommodate the use of electronic signatures in the election process for *UOCAVA* voters as they have in other sectors. The OVI Technology Working Group recommends that state laws address several key principles to best serve the *UOCAVA* population. First, laws should avoid being overly specific. A law based on specific principles, instead of based on a current technology, will remain relevant over time as cryptographic methods and technologies change. Second, laws should treat signatures equally whenever possible. States that accept electronic signatures for other transactions should apply these authorities to the use of electronic signatures on election documents.
3. Recommendation: State election offices should develop procedures and training materials in cooperation with FVAP and their local election offices regarding acceptance and use of a CAC electronic signature. State election offices should also develop, in conjunction with FVAP and their local election offices, educational resources for *UOCAVA* voters about using a CAC electronic signature and coordinate educational efforts with local military installations. The OVI Technology Working Group recognizes that state and local election offices play a central role in coordinating and providing services to their *UOCAVA* voters. Given that there is variation in states' acceptance of an FPCA signed with an electronic signature, and how states



process the FPCA, states will be in the best position to work in conjunction with local election offices to reconcile state requirements and help educate their *UOCAVA* population about their electronic signature options. FVAP, as a component of DOD, is well positioned to assist with the education process and work directly with the states and local election offices as they consider the use of electronic signatures in the voter registration and absentee ballot request process.

Following are the recommendations of the Unreadable/Damaged Ballot Duplication Methods Subgroup of the CSG OVI Technology Working Group:

1. Recommendation: The OVI Technology Working Group supports state and local jurisdictions selecting a ballot duplication process for unreadable and damaged ballots that is appropriate for the number of paper ballots they process. Jurisdictions will vary in the number of paper ballots they process and, likewise, the number of ballots that need to be duplicated. Some jurisdictions duplicate a small number of unreadable or damaged ballots, but larger jurisdictions may duplicate thousands in each election. Jurisdictions that duplicate a large number of ballots may want to consider using an electronic ballot duplication technology that can automate the manual process.
2. Recommendation: Regardless of whether a jurisdiction uses a manual or an electronic ballot duplication process for its unreadable and damaged ballots, there should be clear procedures that ensure auditability. The OVI Technology Working Group recognizes that the laws, policies and procedures for ballot duplication vary by state. Taking that into account, jurisdictions should ensure that their processes for ballot duplication meet basic auditing standards. This would include having at least two individuals duplicate any unreadable or damaged ballot and having a process to confirm that the duplicated ballot is accurate. An audit log should exist so that the original ballot can be linked to the duplicated one. For example, the remade or duplicated ballots might be marked with a number that is linked to the original ballot so that the two ballots can be reconnected should a question arise, but not in such a manner that the voter can be identified.
3. Recommendation: Technologies for ballot duplication of unreadable and damaged ballots should be easy to use and promote transparency not only for election officials, but also for external observers. There are a variety of technologies that can assist election offices in duplicating ballots by automating the process. Ballot duplication technologies should enlist simple and intuitive on-screen navigations that prevent errors in the process. These technologies may include features such as a side-by-side, on-screen comparison between the original and the duplicated ballot to ensure accuracy in the duplication process or produce a printed ballot that provides auditability and additional transparency.

CONCLUSION

The technology solutions offered here and studied by the CSG OVI Technology Working Group—a group of state and local election officials—address critical problems facing *UOCAVA* voters. As more ballots are transmitted electronically, there is a need to be able to duplicate these ballots so they can be counted by vote tabulators. As more activities related to voter registration and ballot requests occur online, leveraging the DOD CAC identity system will ensure that election officials can verify an individual's identity using the best technology possible.

The members of the CSG OVI Technology Working Group—and specifically related to this report—the Common Access Card/Digital Signature Verification and Unreadable/Damaged Ballot Duplication Methods subgroups used a variety of resources and worked with many subject matter experts within the elections community and beyond. Through this resulting work product, they have provided state and local election officials, their stakeholders, military and overseas voters and FVAP with collaborative and critical research, anecdotal evidence, and real-world examples from their jurisdictions and the election community at large.

The resulting recommendations and case studies aim to enhance the voting experience through technology for our nation's military and overseas citizen voters as well as election officials dedicated to serving them.

ACKNOWLEDGEMENTS

The success of The Council of State Governments Overseas Voting Initiative and specifically its Technology Working Group was made possible due to the talents, dedication and insight of many, but most specifically the members of the CSG OVI Technology Working Group. These members are:

- Marci Andino, Executive Director, South Carolina State Election Commission
- Lori Augino, Director of Elections, Washington Office of the Secretary of State
- Thomas Connolly, Director of Election Operations, New York State Board of Elections
- Robert Giles, Director of Elections, New Jersey Department of State
- Neal Kelley, Registrar of Voters, Orange County, California
- Paul Lux, Supervisor of Elections, Okaloosa County, Florida
- Amber McReynolds, Director of Elections, City and County of Denver, Colorado
- Donald Palmer (Auxiliary Member), Democracy Project Fellow, Bipartisan Policy Center
- Stan Stanart, County Clerk, Harris County, Texas
- Justus Wendland, HAVA Administrator, Nevada Office of the Secretary of State

Additionally, CSG would like to acknowledge Lori Augino and Bob Giles who served as leads for the CAC Subgroup and the Ballot Duplication Subgroup, respectively. We could not have completed our work in these areas without their leadership, involvement and enthusiasm. The other members of these two subgroups are were also critical to our success and we thank Marci Andino and Paul Lux from the Unreadable/Damaged Ballot Duplication Methods Subgroup; and Amber McReynolds, Don Palmer and Justus Wendland from the CAC/Digital Signature Verification Subgroup.

CSG acknowledges the many organizations that sent representatives to present at our CSG OVI Technology Working Group meetings on a variety of topics to help further our knowledge and advance our efforts in assisting military and overseas voters. These groups include the following with thanks to all of their team members: Adobe Corporation, Clear Ballot, Democracy Live, The U.S. DoD Defense Manpower Data Center, the Election Administrator's Office of Bexar County, Texas, Election Systems & Software, Everyone Counts, the Nevada Secretary of State's Office, Pew Charitable Trusts' Election Initiatives, Program for Excellence in Election Administration at the Humphrey School at the University of Minnesota with special thanks to Doug Chapin from this program, Runbeck Elections, and the South Dakota Secretary of State's Office.

CSG thanks the U.S. Election Assistance Commission for their participation and insight on this effort, specifically EAC Chair Matt Masterson, commissioners Tom Hicks and Christy McCormick, and EAC staff members Brian Newby and Sean Greene. Additionally, CSG acknowledges the National Institute of Standards and Technology, and specifically Mary Brady and John Wack, for their work with us across many topic areas specific to the CSG OVI Technology Working Group.

CSG thanks the Fors Marsh Group, or FMG, for their expertise and partnership on the CSG OVI effort as a whole, and specifically with regard to the CSG OVI Technology Working Group. We acknowledge FMG Sr. Vice President Brian Griepentrog and the FMG team of Thad E. Hall, Krysha Gregorowicz, Kinsey Gimbel, Kelly Wurtz, Colin Macfarlane, Carrie von Bose and R. Michael Alvarez.

CSG especially thanks FVAP for its leadership, vision and collaboration on this critically important work, without its support the OVI would not be possible. Thank you to FVAP Director David Beirne for his expertise, support and dedication to the success of this project. We'd also like to acknowledge former FVAP Director Matt Boehmer, Katherine Roddy, Scott Wiedmann and the rest of the FVAP staff for their invaluable support.

The work of CSG OVI was supported by Kamanzi G. Kalisa, director of the OVI; Michelle M. Shafer, OVI election technology senior research adviser; Jared Marcotte, OVI senior technology adviser; Ann McGeehan, OVI special adviser; and Jessica Kirby, OVI research associate.

ENDNOTES

- 1 *Uniformed and Overseas Citizens Absentee Voting Act of UOCAVA* information can be found here: <https://www.fvap.gov/info/laws/uocava>
- 2 Information about The Military and Overseas Voter Empowerment, or MOVE, Act can be found here: <https://www.justice.gov/opa/pr/fact-sheet-move-act>
- 3 https://www.fvap.gov/uploads/FVAP/CACVotingFeasibility_20151228.pdf, pages 31-32.
- 4 It may be necessary to configure the software so that it will automatically validate any digital signature certificates.
- 5 This quote was presented in its entirety during Ms. Renteria-Silva's presentation in Monterey, California to the CAC Subgroup of The CSG OVI (November 2015).
- 6 See <https://www.fvap.gov/info/reports-surveys/evdp-report-for-the-DISN/CAC-report-and-the-Final-Report-on-the-Electronic-Voting-Demonstration-Project>.
- 7 Many federal agencies use a Personal Identity Verification (PIV) card, which also has a digital signature component. Civilian federal personnel and contractor personnel who have a PIV might also be able to use the solution discussed here. See: <https://piv.idmanagement.gov/>
- 8 FVAP has studied CACs before. See: https://www.fvap.gov/uploads/FVAP/CACVotingFeasibility_20151228.pdf
- 9 <http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf>
- 10 As the National Notary Association states, "A Notary Public is an official of integrity appointed by... government...to serve the public as an impartial witness in performing a variety of official fraud-deterrent acts related to the signing of important documents." <https://www.nationalnotary.org/knowledge-center/about-notaries>
- 11 Nevada Law 293D <https://www.leg.state.nv.us/NRS/NRS-293D.html>
- 12 http://www.eac.gov/assets/1/Page/2014_EAC_EAVS_Comprehensive_Report_508_Compliant.pdf
- 13 Different States and localities use different terms for this process. This report uses the term "duplication" for the process of taking a ballot that is unreadable by a scanner and creating a new ballot that can be read by the scanner.
- 14 <http://www.nj.gov/state/elections/publications/2017-0310-nj-electronic-ballot-duplication-system-project-report.pdf>
- 15 <http://www.csg.org/OVI/documents/KKOVITechRecs.pdf>

THE COUNCIL OF STATE GOVERNMENTS

ABOUT CSG

Founded in 1933, The Council of State Governments is our nation's only organization serving all three branches of state government. CSG is a region-based forum that fosters the exchange of insights and ideas to help state officials shape public policy. This offers unparalleled regional, national and international opportunities to network, develop leaders, collaborate and create problem-solving partnerships.

ABOUT OVI

Many active duty military personnel are located in remote areas abroad and have limited access to state voting information and, in some cases, their ballot. U.S. citizens living overseas also have unique challenges in exercising their right to vote. These challenges are complicated by extreme variation in how states conduct elections and how absentee ballots are processed.

In September 2013, CSG launched a four-year, \$3.2 million initiative with the U.S. Department of Defense Federal Voting Assistance Program or FVAP, to improve the return rate of overseas absentee ballots from service members and U.S. citizens abroad.

As part of this effort, CSG's Overseas Voting Initiative maintains two separate advisory working groups. The CSG Policy Working Group is examining military and overseas voting recommendations from the Presidential Commission on Election Administration, as well as other successful programs and practices across the country. The CSG Technology Working Group is exploring issues such as performance metrics and data standardization for incorporation into state and local elections administration policies and practices for overseas ballots. Through the initiative, CSG will provide state policymakers and state and local election officials with best practice guides to ensure the men and women of the U.S. military and Americans living overseas are able to enjoy the same right to vote as citizens living in the United States.

OVI STAFF

Kamanzi G. Kalisa, director, CSG Overseas Voting Initiative

Michelle M. Shafer, senior research associate for elections technology, CSG Overseas Voting Initiative

Ann McGeehan, special adviser, CSG Overseas Voting Initiative; member, Presidential Commission on Election Administration

Jared Marcotte, senior technology advisor, CSG Overseas Voting Initiative

Jessica Kirby, CSG Overseas Voting Initiative Research Associate

CONTACT

Overseas Voting Initiative | (202) 624-3539 | csg.org/ovi | [@CSGOverseasVote](https://twitter.com/CSGOverseasVote)