



PERSONNEL AND
READINESS

UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-4000

CLEARED
For Open Publication
Feb 13, 2017
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

JAN 18 2023

Chair
Committee on Armed Services
U.S. House of Representatives
Washington, DC 20515

Dear Chair:

The Department's response to section 1077 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117-81), which addresses the results of the Federal Voting Assistance Program's Study on End-to-End Electronic Voting Services, is enclosed.

Thank you for your continued strong support for the voting rights of our Service members, their families, and U.S. citizens residing overseas. I am sending a similar letter to the Committee on Armed Services of the Senate.

Sincerely,

A handwritten signature in black ink, appearing to read "Gilbert R. Cisneros, Jr.", written in a cursive style.

Gilbert R. Cisneros, Jr.

Enclosure:
As stated

cc:
Ranking Member



PERSONNEL AND
READINESS

UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-4000

JAN 18 2023

Chair
Committee on Armed Services
United States Senate
Washington, DC 20510

Dear Mr. Chair:

The Department's response to section 1077 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117-81), which addresses the results of the Federal Voting Assistance Program's Study on End-to-End Electronic Voting Services, is enclosed.

Thank you for your continued strong support for the voting rights of our Service members, their families, and U.S. citizens residing overseas. I am sending a similar letter to the Committee on Armed Services of the House of Representatives.

Sincerely,

A handwritten signature in black ink, appearing to read "Gilbert R. Cisneros Jr.", written in a cursive style.

Gilbert R. Cisneros Jr.

Enclosure:
As stated

cc:
Ranking Member

Report to Congress on End-to-End Electronic Voting Services



January 2023

This report has been prepared by the staff of the
Federal Voting Assistance Program
Washington, DC

The estimated cost of this report or study
for the Department of Defense is
approximately \$33,000 in Fiscal Years
2021 - 2022. This includes \$0 in expenses
and \$33,000 in DoD labor.

Generated on 2022Oct11 RefID: 1-
1A00B9B
labor.

Table of Contents

Executive Summary 2

Research Objective 4

Prior Research Conducted by FVAP on Electronic Voting Services 7

Characteristics of Immature Postal Operations 9

Factors to Consider in Election Administration 14

Existing Defense Department Role and Authorities..... 17

Notional Implementation Resources and Timeline 21

Key Findings..... 23

Executive Summary

Pursuant to Executive Order 12642, “Designation of the Secretary of Defense as the Presidential designee under title I of the Uniformed and Overseas Citizens Absentee Voting Act [UOCAVA],” June 8, 1988, the Secretary of Defense (SecDef) serves as the Presidential designee tasked with administering UOCAVA. The Federal Voting Assistance Program (FVAP) is delegated responsibility for this administration, under the direction of the Under Secretary of Defense for Personnel and Readiness (USD(P&R)). FVAP submits this report on behalf of the SecDef in accordance with the requirements in section 1077 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2022 to study and prepare a report on providing end-to-end electronic voting services in participating States for absent overseas Uniformed Service personnel operating in areas with limited postal services. Army, Navy, Air Force, Marine Corps, Coast Guard, Space Force, Commissioned Corps of the Public Health Service, and Commissioned Corps of the National Oceanic and Atmospheric Administration personnel are authorized for Military Post Office service as long they are activated by their organization or agency when operating in areas with limited postal service. Under the UOCAVA definition of “absent uniformed services voter,” this may include members of the merchant marine while operating in areas with limited postal service. FVAP relied heavily upon previous research in this area, and as directed by section 1077 prepared this report, in consultation with the Department of Defense (DoD) Chief Information Officer (CIO).

End-to-end electronic voting services is not explicitly defined in the NDAA for FY 2022 requirement so in defining the scope of its research FVAP examined the potential for providing an electronic path for each step of the absentee voting process for absent uniformed services voters serving overseas. Steps of the absentee voting process for UOCAVA voters entail:

1. Completing and submitting a Federal Post Card Application (FPCA) to simultaneously register and request an absentee ballot.
2. Receiving an official ballot from an election office;
3. Returning the voted ballot to the election office; and
4. Receiving confirmation from the election office that the ballot was accepted for inclusion in the final tabulated results.

The challenge of supporting electronic voting services is that it is entirely reliant upon each State authorizing submission methods for election materials. FVAP’s program focus remains on providing absentee voting assistance to all covered voters under UOCAVA, not just military members serving from specific States that authorize the electronic submission of election materials. While the requirement in the NDAA for FY 2022 is intended to involve only States participating in any subsequent research, FVAP examined this research requirement from the standpoint of longer-term sustainability for all States and territories of the United States.

Past research efforts conducted by FVAP identified a significant shortcoming that would occur if the Federal Government specified the performance and operating requirements of voting systems used by State and local election officials. Namely, that each State is ultimately responsible for the conduct of its elections and must procure systems best suited for their election infrastructure; any funding provided by the Department (i.e., grants) should be flexible to include

consideration of commercial or internal development of systems to meet the specified requirements under State law as well as State certification requirements.

Dynamic environments impact postal operations and information technology infrastructure currently required for the election process. The NDAA for FY 2022 required this research on end-to-end electronic voting services to consider persons deployed to locations with limited or immature postal services. The lack of military postal services generally corresponds with an overall lack of information technology infrastructure, which in turn limits the implementation of end-to-end electronic voting services. FVAP's ongoing research indicates overseas personnel have broad levels of access to information technology hardware, so the availability of local postal services may not be a key factor for consideration in implementation. However, it should be noted that various operational considerations do impact the level of access to information technology infrastructure.

State reliance on physical signatures for voting purposes remains a key hurdle for reducing logistics and drives the continued requirement for the availability of printers, paper, and ink. In order to support an entirely electronic voting process, the assumption that a voter may complete all steps without the aid of additional hardware besides a workstation and network connectivity is premised on the home State's acceptance of digital signatures, such as those generated by the DoD Common Access Card (CAC). Currently, three States support the acceptance of digital signatures for some or all of the UOCAVA absentee voting process, so voters must rely on printing materials for signature and subsequent scanning and transmission back to election offices.

Differences in ballot acceptance methods among States adds to the complexity of offering support to the entire population of absent uniformed services voters. States remain the information technology (IT) system owners and are responsible for the underlying security of electronic voting services and specific functionalities. Currently 46 States and territories accept electronic submission of the FPCA for voter registration and absentee ballot request. Twenty-seven States and territories accept the electronic submission of voted ballots. All States and territories are required by UOCAVA to provide blank ballots for Federal office elections electronically upon request. FVAP recognizes that election officials rely on the security of their primary systems, but may also use unencrypted email to support transmission of electronic absentee voting materials. Therefore, an opportunity exists for additional research to identify methods for issuing commercial or governmental credentials to election officials to enable the use of encryption protocols and enhance the security of the existing environment.

Based on these identified challenges to the implementation of end-to-end electronic voting services, the Department is continuing to review a 48-month action plan to support research grants to participating State and local governments. The earliest implementation possibility would be the Federal election cycle that aligns with year four. The exact scale and cost of this type of research would be driven by statutory and regulatory requirements at the State-level; however, certain cost efficiencies could be leveraged through State-level implementations versus local.

Research Objective

Section 1077 of the NDAA for FY 2022 requires the SecDef to conduct the following research in consultation with the DoD CIO:

In consultation with the Chief Information Officer of the Department of Defense, the Presidential designee under the Uniformed and Overseas Citizens Absentee Voting Act shall conduct a study on providing end-to-end electronic voting services (including services for registering to vote, requesting an electronic ballot, completing the ballot, and returning the ballot) in participating States for absent uniformed services voters under such Act who are deployed or mobilized to locations with limited or immature postal services (as determined by the Presidential designee).

In conducting the study under 6 subsection (a), the Presidential designee shall include: (1) methods that would ensure voters have the opportunity to verify that their ballots are received and tabulated correctly by the appropriate State and local election officials; (2) methods that would generate a verifiable and auditable vote trail for the purposes of any recount or audit conducted with respect to an election (3) a plan of action and milestones on steps that would need to be achieved prior to implementing end-to-end electronic voting services for absentee uniformed services voters; (4) an assessment of whether commercially available technologies may be used to carry out any of the elements of the plan; and (5) an assessment of the resources needed to implement the plan of action and milestones referred to in paragraph 3.

The Presidential designee shall conduct the study under subsection (a) in consultation with appropriate State and local election officials. To the extent the Presidential designee determines to be appropriate, the Presidential designee may include in the study conducted under subsection (a) an analysis of the potential use of contractors to provide voting services and how such contractors could be used to carry out the elements of the plan referred to in subsection (b)(3).

Not later than 180 days after the date of the enactment of this Act, the Presidential designee shall provide to the Committees on Armed Services of the Senate and House of Representatives a briefing on the interim results of the study conducted under subsection (a). Not later than one year after the date of the enactment of this Act, the Presidential designee shall submit to the Committees on Armed Services of the Senate and House of Representatives a report on the results of the study conducted under 22 subsection (a).”

In response, FVAP operating under its authority prescribed in Department of Defense Instruction 1000.04, “Federal Voting Assistance Program,” and on behalf of the USD(P&R), operating on behalf of the SecDef as the Presidential designee, set out to establish a research plan to review and answer the following questions:

1. To what extent do immature postal service locations operate and what characteristics do they share? Are there inherent challenges associated with operating conditions that align to immature postal service locations and, if so, how does this inform and educate the consideration of electronic voting services?
2. How does past FVAP research inform the consideration of electronic voting services and the need to establish specific functional elements for electronic voting services themselves? To what extent do commercial technologies support the ability for voters to verify ballots are successfully returned and counted accurately?
3. What resources would be required for the Department to support electronic voting services within these environments? What is the associated lead time for implementing such services?
4. What opportunities exist for the Department to support electronic voting services in response to its initial observations?

FVAP determined the scope of this study and report by examining the potential for providing an electronic path for each step of the absentee voting process for absent uniformed services voters serving overseas. Steps of the absentee voting process for UOCAVA voters entail:

1. Completing and submitting a FPCA to simultaneously register and request an absentee ballot;
2. Receiving an official ballot from an election office;
3. Returning the voted ballot to the election office; and
4. Receiving confirmation from the election office that the ballot was accepted for inclusion in the final tabulated results.

The Presidential designee's role pursuant to UOCAVA includes prescription of the official post card form, the Federal Write-In Absentee Ballot, the standard oath for use on the forms, and suggested design for absentee ballot mailing envelopes. Additionally, the Department works to ensure State and local election officials are aware of their requirements under UOCAVA, and provide descriptive materials to guide voters through their State's absentee voting process. The Presidential designee does not:

1. Register voters;
2. Process absentee ballot requests;
3. Choose ballot types or send blank ballots to voters;
4. Accept, approve, or tabulate voted ballots; or
5. Conduct election audits.

These parts of the election process are carried out by State and local election officials. Thus, States are the entities with the ability to study and implement methods that would ensure absent uniformed voters can verify that their ballots are received and tabulated correctly by their

State and local election officials and the methods that would generate a verifiable and auditable vote trail for the purposes of any recount or audit conducted with respect to their elections.

Given these realities, for the Presidential designee to facilitate methods that would ensure voters can verify that their ballots are received and tabulated correctly by the appropriate State and local election officials, the Department would require links to the State or local official sites developed by them to provide this information. The generation of a verifiable and auditable vote trail for the purposes of any recount or audit of an election falls under a State's jurisdiction. Again, the Department would need to rely upon the State and local systems to receive any research about their methods. Given the State and local province of their election systems, the Presidential designee is not able to assess commercially available technologies that may be used for an end-to-end absentee voting system. A high level assessment of the resources needed to implement the plan of action and milestones for potential research within the Department's role to provide voting assistance under UOCAVA is included in the report's conclusion.

FVAP established an internal DoD working group to assess these questions and provide an overall approach in consideration of electronic voting services and the Department's role. Specifically, from December 2021 through September 2022, representatives from FVAP, the DoD CIO, the Defense Information Systems Agency, the Military Postal Service Agency, and the Defense Manpower Data Center convened to assist with the overall research associated with this effort. FVAP conducted this research and findings based on past research, internal technical findings, comprehensive literature reviews and feedback from election officials through FVAP's existing cooperative agreement with the Council of State Governments.

Prior Research Conducted by FVAP on Electronic Voting Services

The requirement for FVAP to research the viability of providing electronic voting services is not new, prior research in this area dates back over twenty years. In the 2000 general election, FVAP sponsored a small pilot project called “Voting Over the Internet (VOI)” in which Service members used their personal computers to register, request, and receive absentee ballots, and mark and return their ballots online. This FVAP research history is captured in a prior Congressional Report from 2010 highlighting how the VOI led to inclusion of language in the NDAA for FY 2002 (Public Law 107–107)¹ instructing the SecDef to implement a larger project.

Thus, the “Secure Electronic Registration and Voting Experiment (SERVE),” was developed to allow Service members to vote online using their Common Access Card (CAC). SERVE was planned for the 2004 election; however it was cancelled before implementation. As a result of the cancelled SERVE project, NDAA FY 2005 (P.L. 108-375) delayed the requirement for the Secretary of Defense to conduct an electronic voting demonstration project. NDAA FY 2005 modified the timing of this requirement “until the first regularly scheduled general election for Federal office, which occurs after the Election Assistance Commission (EAC) notifies the Secretary of Defense that the Commission has established absentee voting guidelines and certifies that it will assist the Secretary in carrying out the project.”²

In September 2004, FVAP created and developed a new online project called the Interim Voting Assistance System (IVAS). This system provided for electronic submission of ballot requests and delivery of blank ballots using a secure DoD server. Voters in participating States and jurisdictions were notified by email when their ballot was available on the server. The voter would then download and print the ballot, mark his or her selections, and return the voted ballot by postal mail or fax (if the voter’s State permitted this option).

For the 2006 election, the capabilities of IVAS were extended to enable all UOCAVA voters in participating States and jurisdictions to use the system for submitting ballot requests. In 2008, IVAS was further modified to enable all UOCAVA voters in participating States and jurisdictions to make ballot requests and receive blank ballots. This enhanced capability was called the Voter Registration/Ballot Delivery System.³

¹ Section 1604(a)(1) of Public Law 107–107:

ESTABLISHMENT OF DEMONSTRATION PROJECT.—

(1) IN GENERAL.—Subject to paragraph (2), the Secretary of Defense shall carry out a demonstration project under which absent uniformed services voters are permitted to cast ballots in the regularly scheduled general election for Federal office for November 2002, through an electronic voting system. The project shall be carried out with participation of sufficient numbers of absent uniformed services voters so that the results are statistically relevant.

² Section 1604(2) of Public Law 107–107.

³ Electronic Voting Support Wizard. (2010). Federal Voting Assistance Program. https://www.fvap.gov/uploads/FVAP/Reports/evsw_report.pdf.

In 2010, FVAP conducted further research on the use of electronic blank ballot delivery systems to encourage and assist States to meet requirements set forth in the UOCAVA as amended by the Military and Overseas Voter Empowerment (MOVE) Act to transmit ballots 45 days prior to each Federal election and offer an electronic means of delivering blank ballots. Due to unresolved security concerns regarding the electronic return of voted ballots, FVAP explicitly excluded this aspect of the voting process from the 2010 effort.

From 2010 until 2014, FVAP conducted research on various aspects of the UOCAVA absentee voting process in support of the Congressional requirement to conduct an electronic voting demonstration project (i.e., internet voting). Dating back to the NDAA for FY 2001, Congress required FVAP to conduct an internet-voting pilot in 2002 with subsequent authorization through the NDAA for FY 2004 implying that a pilot should occur after there are voting guidelines for electronic absentee ballots and after the EAC certifies that it will assist DoD in this effort. From 2005 to 2014, the EAC did not establish applicable guidelines other than those associated with the conduct of a kiosk-based system.

In December 2014, section 593 of the NDAA for FY 2015, enacted in December 2014, repealed the requirement for FVAP to conduct an electronic voting demonstration project. Concurrent to these various authorizations for electronic voting (i.e., internet voting) FVAP continued to support research on the implementation of blank ballot delivery systems while explicitly restricting the funding of systems supporting the electronic return of voted ballots in the absence of applicable security guidelines. FVAP accomplished this through its Electronic Absentee System Evaluation grant program, which officially concluded in 2017.

Through its years of research on electronic transmission of materials aspects of the absentee voting process, FVAP identified these key observations and findings:

1. Do not specify rigid requirements or involve the Department in direct procurement of election systems as each State differs in acceptable technologies;
2. Participating States in any research objective should be given overarching elements and requirements to share data and findings, but the actual procurement of voting systems should remain with State and local election authorities;
3. The logistics associated with fielding electronic voting systems to forward operational theaters need to be considered not only from a feasibility perspective, but the level of appropriateness given the lack of universal acceptance within the States of electronically voted ballots and FVAP's focus on supporting the absentee voting process for all active duty military (ADM) personnel at a national level.⁴

These findings impact the decision to consider the specific functional elements of voting systems as part of a procurement action, and directly inform the consideration of future milestones for any implementation of end to end electronic voting services. These findings also underscore how the Department supports the ability for ADM personnel to participate in the absentee voting process without taking ownership of the process, but instead assist them with instructions from and communications with their election office.

⁴ Ibid.

Characteristics of Immature Postal Operations

A major element in this research objective per the legislation is the consideration of immature or limited postal operations. Specifically, what are the supporting characteristics and elements surrounding those locations and how do these characteristics align with providing end to end electronic voting service?

The Military Postal Service Agency defines locations with immature postal services as those that do not have access to military or commercial networks. The lack of network connectivity for these locations means that various business operations associated with the purchase of postage that require access to postal finance systems in alignment with United States Postal Service operations cannot be supported so no post office exists. These locations receive mail support from either military post offices utilizing mobile missions or diplomatic post offices. Locations that fall into these categories are typically few and characterized by austere operational environments associated with contingency operating bases. It is important to note that all naval ships are immature because none offer access to commercial or military networks for postal operations. Postal service is provided manually on Aircraft Carriers, Guided-Missile Destroyers and Cruisers, General and Multi-Purpose Amphibious Assault Ships, Resupply Ships for Submarines, Hospital Ships, and while in port. On average, most ships get regular service and receive mail 10 days after acceptance.

Locations with limited postal operations describe a location that may have limitations on the frequency of mail services. Any mail services representing less than 3 days per week is identified as having limited postal services. Factors that influence the frequency of mail include overall volume, costs, availability of commercial or military air and ground transportation, and overall security and operational conditions.

If postal operations do not exist due to the lack of network connectivity, a larger question arises on the overall access for military personnel to access technical resources that would be required for the use of end-to-end electronic voting services. FVAP's 2020 post-election survey of ADM included an assessment of the overall availability of technical resources that ADM members require to participate in the absentee voting environment. The current absentee voting environment still requires broad access to a full suite of technical products such as network and computer access, printers to allow for wet signatures and to prepare postal based election materials for submission, and scanners to prepare election materials for electronic transmission to election officials. Below are key results and observations from FVAP's post-election survey of ADM personnel:

Table 1: Results from the 2020 Post-Election Voting Survey for Active Duty Military (PEVS-ADM) showing the percentage of ADM’s survey responses when it came to their perception of having access to the various electronic voting resources in 2020, by Service.

Service	Fax	Internet	Scanner	Printer
<i>Overall</i>	22%	89%	61%	71%
<i>Army</i>	20%	88%	59%	69%
<i>Navy</i>	25%	87%	60%	71%
<i>Marine Corps</i>	19%	87%	53%	67%
<i>Air Force</i>	22%	92%	65%	76%
<i>Coast Guard</i>	33%	92%	76%	82%

NOTE: The 2020 PEVS-ADM allowed respondents to select more than one option when asked about access to the above resources.

NOTE: These percentages are based on the results FVAP received from the 2020 Post-Election Voting Survey for ADM. They are based off of the boxes that the survey respondents checked off in question 64, FVAP tried to verify the actual access of these resources at every installation, or on every ship; however FVAP was unable to obtain this data, therefore this survey data is the only data available regarding electronic voting resources.

- As can be seen in Table 1, internet access among ADM is very high with 89 percent of survey respondents reporting they have access. This trend holds when breaking the data down by Service and where ADM are stationed except for those who are stationed on a ship (Table 2). For example, in Table 2, 63.0 percent of Navy members who are stationed on a ship have internet access.
- Seventy one percent of ADM report having access to printers (Table 1). The estimates are similar when broken down by Service and where ADM are stationed with the Coast Guard having slightly higher estimates than the other Services (Table 2).
- Sixty one percent of ADM report having access to scanners (Table 1). When looking at the estimates by Service, the Marine Corps members report having lower access (53.4 percent) compared to the other services who have estimates close to the overall estimate. However, for Navy members stationed on a ship, only 42.3 percent report having access to scanners (Table 2).

Table 2: Results from the 2020 Post-Election Voting Survey for Active-Duty Military (PEVS-ADM) showing the percentage of ADM’s survey responses when it came to their perception of having access to the various electronic voting resources in 2020, by Station Location and Service.

Service	Location	Fax	Internet	Scanner	Printer
<i>Army</i>	Domestic	21%	88%	60%	70%
	Overseas	15%	86%	55%	64%
<i>Navy</i>	Domestic	25%	88%	60%	71%
	On Ship	5%	63%	42%	65%
	Overseas	21%	86%	66%	74%
<i>Marine Corps</i>	Domestic	19%	87%	52%	66%
	On Ship*	N/A	N/A	N/A	N/A
	Overseas	21%	88%	61%	67%
<i>Air Force</i>	Domestic	23%	92%	66%	77%
	Overseas	17%	92%	65%	73%
<i>Coast Guard</i>	Domestic	34%	N/A	77%	83%
	On Ship*	N/A	N/A	N/A	N/A
	Overseas	N/A	100%	77%	84%

NOTE: The 2020 PEVS-ADM allowed respondents to select more than one option when asked about access to the above resources.

NOTE: Locations marked with a ‘*’ indicate that total n was too small to include in results.

NOTE: These percentages are based on the results FVAP received from the 2020 Post-Election Voting Survey for ADM. They are based off of the boxes that the survey respondents checked off in question 64. FVAP tried to verify the actual access of these resources at every installation, or on every ship, however FVAP was unable to obtain this data, therefore this survey data is the only data available regarding electronic voting resources.

Table 3: Results from the 2020 Post-Election Voting Survey for Active Duty Military (PEVS ADM) showing the percentage of ADM’s survey responses when it came to their perception of having access to the various electronic voting resources in 2020, by Combat Zone and Service.

Resource Type	Service	In Combat Zone	Not in Combat Zone
<i>Fax</i>	<i>Army</i>	22%	20%
	<i>Navy</i>	17%	25%
	<i>Marine Corps</i>	30%	19%
	<i>Air Force</i>	15%	23%
	<i>Coast Guard</i>	23%	33%
<i>Internet</i>	<i>Army</i>	87%	87%
	<i>Navy</i>	74%	88%
	<i>Marine Corps</i>	99%	86%
	<i>Air Force</i>	85%	92%
	<i>Coast Guard</i>	100%	92%
<i>Scanner</i>	<i>Army</i>	57%	59%
	<i>Navy</i>	42%	61%
	<i>Marine Corps</i>	72%	53%
	<i>Air Force</i>	50%	67%
	<i>Coast Guard</i>	100%	77%
<i>Printer</i>	<i>Army</i>	65%	69%
	<i>Navy</i>	56%	72%
	<i>Marine Corps</i>	73%	66%
	<i>Air Force</i>	61%	77%
	<i>Coast Guard</i>	100%	83%

NOTE: The 2020 PEVS-ADM allowed respondents to select more than one option when asked about access to the above resources.

NOTE: These percentages are based on the results FVAP received from the 2020 Post-Election Voting Survey for ADM. They are based off of the boxes that the survey respondents checked off in question 64. FVAP tried to verify the actual access of these resources at every installation, or on every ship; however FVAP was unable to obtain this data, therefore this survey data is the only data available regarding electronic voting resources.

- For the technology availability analyses, the PEVS-ADM survey asks ADM whether they deployed to a combat zone within the past 2 years, and for many PEVS analyses that focus on deployment the time frame is recoded so deployment coincides with an election year. However, we do not know when they returned from deployment, which makes comparing combat zone deployment to where ADM are stationed difficult because there is considerable overlap between the stationed and deployment questions. The majority of ADM who report deployment to a combat zone are also stationed domestically. This feature of the data produces similar estimates when comparing the stationed location to combat zone deployment. For example, 87.9

percent of Army members who are stationed domestically report having internet access, and 87.7 percent of Army members who are deployed to a combat zone report having internet access.

Table 4: Percentage of Active Duty Military Who Voted Electronically and by Mail in 2016 and 2020.

Ballot Return Type	2016	2020
<i>Electronic</i>	14.0%	12.5%
<i>Mail</i>	85.9%	87.5%

- As shown in Table 4, the overwhelming majority of ADM vote by mail. Of those who voted, 87.5 percent of ADM voted by mail during the 2020 election, which as an increase of about 2 percentage points from the 2016 election.
- ADM voted by mail at higher rates in 2020 than they did during 2016. This trend holds even among States that allow electronic ballot returns.

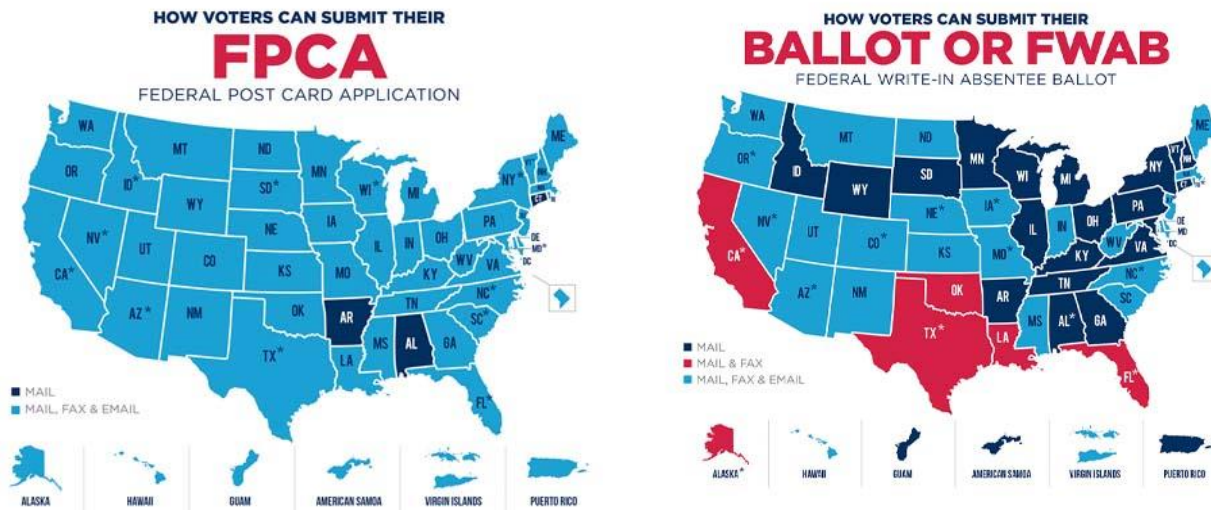
This section identified the overall availability of the technical resources necessary to participate in the absentee voting process. This broad availability is not connected to the availability of postal services. In fact, it should be noted that even with the 46 States/territories currently accepting the electronic submission of the FPCA and 27 States/territories currently accepting electronic submission of voted ballots, military personnel rely more on mail than electronic means of casting ballots. This could be a function of confidence in the military postal system, but also the technical complexities of navigating an electronic absentee voting process, which lacks usability features such as the acceptance of digital signatures and requires the printing, signing, and scanning of materials for submission.

Factors to Consider in Election Administration

As captured in FVAP’s prior cumulative report on internet voting, “Federal elections are administered by State and local officials through a combined framework of Federal and State laws. Federal laws provide a framework for Federal elections by regulating when elections are held, establishing what the minimum requirements are for who can vote in Federal elections (e.g., enfranchisement of women, language access for voters), limiting requirements States can put on voters that would prevent them from voting (e.g., poll taxes), and establishing requirements of when ballots have to be ready to be sent to UOCAVA voters.”⁵

There is no existing authority for FVAP to prescribe requirements or compel participation from States in offering electronic voting services to overseas military personnel. “State laws cover issues such as the design and layout of ballots, the voting technology used, the rules regarding the timing of registering to vote, and the timing of when ballots must be returned and, ultimately, the actual conduct and certification of election results.”⁶

A key feature of election administration in the United States is that the U.S. Constitution delegated the authority to regulate elections to the States, while reserving the authority for Congress to regulate Federal elections. This imposes significant limitations for any centralized electronic voting effort, such as those studied by FVAP in its research under the now-repealed electronic voting demonstration project requirement.



Figures 1 and 2 above illustrate the patchwork of authorizations associated with submitting election materials. Consideration of providing end-to-end electronic voting services remains limited to States accepting election materials by mail, fax, and email for both the FPCA and the Federal Write-In Absentee Ballot.

⁵ Electronic Voting Demonstration Project Research. (2015). Federal Voting Assistance Program.

⁶ Ibid.

The decentralized structure of election administration in the United States leads to a patchwork of election rules, regulations, and procedures. Each State has unique laws and regulations regarding the conduct of elections. The ultimate responsibility for certifying the results of an election rests with each State and its State election official.⁷ The EAC groups States into four categories related to voting system certification:

1. **Baseline Help America Vote Act (HAVA) Requirements:** State statutes and/or regulations do not explicitly State that voting systems must be tested to Federal standards or be certified by a Federal agency or federally accredited laboratory. However, voting systems must, at a minimum, meet standards for voting equipment set forth by the 2002 HAVA.
2. **Requires Testing to Federal Standards:** State statutes and/or regulations require that voting systems are tested to Federal voting system standards. They may include references to Federal standards drafted by administrative bodies such as the Federal Election Commission, which formerly set Federal voting standards, but HAVA transferred this authority to the EAC, the only government agency which formally adopts Federal standards for voting systems.
3. **Requires Testing by a Federally Accredited Laboratory:** State statutes and/or regulations require that voting systems are tested by a Federally or nationally accredited laboratory to Federal standards. Older statutes may refer to Independent Testing Authorities, but such test labs are now known as Voting System Test Laboratories under the EAC's testing and certification program.
4. **Requires Federal Certification:** State statutes and/or regulations require that voting systems are certified by the appropriate Federal agency responsible for testing and certification of compliance with Federal voting system guidelines. Post-HAVA, the EAC is the only Federal agency with the authority to test and certify voting systems, but older, unrevised statutes may not specify this.⁸

Additionally, varying State laws and regulations would impact development and implementation of a centralized system. The issues would likely include, but not be limited to:

- Variations across States related to ballot design. States typically have specific laws related to the size of font, order of candidates, having straight party voting options, candidate ordering, ballot designations of candidates, and related matters. This means that the ballot interface for any remote electronic voting system must be unique to meet State rules and regulations; and

⁷ Ibid.

⁸ United States Election Assistance Commission. 2020. "State Requirements and the U.S. Election Assistance Commission Voting System Testing and Certification Program." Retrieved from [eac.gov](https://www.eac.gov/sites/default/files/TestingCertification/State_Requirements_for_Certification09042020.pdf) on May 27, 2022.

- Security requirements related to using the Internet in voting. Some States have very strict laws and regulations related to having any voting technology connected to the Internet or related networks. Such regulations limit the ability of States to participate in a remote electronic voting initiative for multiple aspects of the process.⁹

Consideration for providing end to end to electronic voting services needs to be reconciled with existing State certification requirements as part of any requirement moving forward. This is especially true in consideration of enabling State and local jurisdictions and the associated lead times necessary to procure and develop appropriate systems. These systems would need to have the associated requirements established and the resulting system subjected to State or Federal certification requirements, which may run as long as 2 years. The certification and security of these systems are a critical component for implementation.

Our understanding regarding the potential and realized security threats to any computer network-based system have only become more apparent since the Federal designation of election systems as part of the nation's critical infrastructure in 2017. This creates an opportunity for State and local election authorities to meet Federal information assurance requirements through a State administered process with support from appropriate Federal agencies.

⁹ Electronic Voting Demonstration Project. (2015). Federal Voting Assistance Program.

Existing Department of Defense Roles and Authorities

Under UOCAVA, and through its delegated authority, FVAP is required to engage in a set of specified activities, including:

1. Consulting State and local election officials in carrying out this subchapter, and ensure that such officials are aware of the requirements of this Act;
2. Prescribing an official post card form [the FPCA, containing both an absentee voter registration application and an absentee ballot application];
3. Developing a Federal Write-In Absentee Ballot (including a secrecy envelope and mailing envelope for such ballot) for use in general, special, primary, and runoff elections for Federal office by UOCAVA voters who do not receive their absentee ballot, and implementing an online system whereby UOCAVA voters can enter their address (or other relevant information) and receive a list of all Federal candidates for which they are eligible to vote;
4. Describing a suggested design for absentee ballot mailing envelopes;
5. Compiling and distributing descriptive material on State absentee registration and voting procedures, and to the extent practicable, facts relating to specific elections, including dates, offices involved, and the text of ballot questions;
6. Reporting to the President and the Congress, not later than the end of each year after a Presidential election year, on the effectiveness of assistance under this subchapter, including a statistical analysis of Uniformed Services voter participation, a separate statistical analysis of overseas nonmilitary participation, and a description of State-Federal cooperation;
7. Prescribing a standard oath for use with any document under this subchapter affirming that a material misstatement of fact in the completion of such a document may constitute grounds for a conviction for perjury;
8. Establishing procedures for collecting marked absentee ballots of absent overseas Uniformed Services voters in regularly scheduled general elections for Federal office, including absentee ballots prepared by States and the Federal Write-In Absentee Ballot, and for delivering such marked absentee ballots to the appropriate election officials;
9. Taking actions as may be necessary (a) to ensure that absent Uniformed Services voters who cast absentee ballots at locations or facilities under the jurisdiction of the Presidential designee are able to do so in a private and independent manner; and (b) to protect the privacy of the contents of absentee ballots cast by absentee Uniformed Services voters and overseas voters while such ballots are in the possession or control of the Presidential designee;

10. Developing online information portals to inform absent Uniformed Services voters regarding voter registration procedures and absentee ballot procedures available for Federal elections and establishing a program, using the military global network, to notify absent Uniformed Services voters 90 days, 60 days, and 30 days prior to Federal elections, of voter registration information and resources, the availability of the FPCA, and the availability of the Federal Write-In Absentee Ballot; and
11. Working with the EAC and the chief State election official of each State, develop standards for States to report data on the combined number of absentee ballots transmitted to absent Uniformed Services voters and overseas voters for the election and the combined number of such ballots, which were returned by such voters and cast in the election, and making these data available to the public. With this context, we can now consider the specific impact of recent congressional actions related to UOCAVA voting in general and electronic voting trials specifically.¹⁰

While FVAP maintains broad authority to conduct research in the areas of innovative voting technology, the longer-term viability of electronic voting services and impact to the Department must be considered. Therefore, FVAP considers the implementation of providing end-to-end electronic voting services from both a research and operational perspective to include longer-term implications associated with fielding such a service.

FVAP prescribes the FPCA to standardize and streamline the absentee voting process for voters eligible to vote under the UOCAVA. The FPCA can be downloaded electronically, but must be completed, printed, and signed using an ink signature and mailed to the address of the jurisdiction where the citizen is eligible to vote. Making this process fully electronic would require the following elements to initiate the absentee voting process through submission of a FPCA or complete the absentee voting process through submission of a voted State issued ballot or Federal Write-In Absentee Ballot:

1. Execution: The ability to complete an electronic form, either by downloading it or by completing the form on a hosted site.
2. Attribution: The ability to sign the form using a legal electronic signature. The e-SIGN act identifies key considerations of an electronic signature, a key criteria is ensuring intent to sign. Affixing a digital signature using a Public Key Infrastructure (PKI) based certificate would provide stronger attribution.
3. Jurisdiction and Confidentiality: The ability to send the completed form to an appropriate official at the appropriate jurisdiction. Electronic delivery and receipt of electronic forms would require augmenting this information with an email address unique to the jurisdiction and a recognized government domain.

¹⁰ Electronic Voting Demonstration Project Research Report. 2015. Federal Voting Assistance Program

4. Attribution and Integrity: The ability for election officials to verify the signature. Digitized signatures cannot be verified, although it is possible to protect the contents of the form so that they cannot be altered. Verification of digital signatures requires that the system the election official is using has trust in the PKI that issued the certificate and can access revocation information.

The Council of State Governments' Overseas Voting Initiative examined the issue of digital signatures such as the one available on the DoD CAC for its potential for enhancing the overall usability for overseas military:

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. 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 has 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.¹¹

The use of the DoD CAC by Uniformed Services voters and overseas DoD civilian voters provides a clear opportunity to enable end to end electronic voting services, but this would also require State level authorization for the acceptance of election materials not only via electronic

¹¹ Council of State Governments. 2017. "Using Technology to Enhance Military and Overseas Voting Vol. 1". Retrieved from csg.org on May 27, 2022.

means, but also the acceptance of digital signatures in lieu of wet signatures. Additionally, the submission of election materials electronically must be reconciled with ongoing concerns over cybersecurity and the State's authority as the official system owner and responsible entity for certifying election results.

With full recognition of the State's responsibility to dictate specific functional elements of each voting system operating within its State and its underlying security, there is an ongoing opportunity for the Federal Government to aid in facilitating underlying security for email transmissions between active-duty military personnel and election officials. While the Department's CAC enables digital signatures, it also allows for the encryption of email between a sender and a recipient. Encryption consists of a certificate and a key pair that permits the encryption of emails through the Federal Public Key Infrastructure (FPKI).¹² The administration of the Department's CAC falls under DoD agency policy, which does not support issuance of these types of credentials to State and local election officials. However, alternatives such as the use of External Certificate Authorities through the Department or the use of the Personal Identity Verification Interoperability (PIV-I) could be leveraged in conjunction with Federal partners such as the Department of Homeland Security. For example, PIV-I is purposely defined to support Federal agencies, Federal contractors, commercial organizations doing business with the Federal government, State and local agencies, critical infrastructure providers and first responder organizations.¹³ The use of digital signatures and corresponding authorization for acceptance by the States in the election transaction is critical to support electronic voting services. The use of PKI to support encryption is not as critical, but does represent a substantial improvement and existing capacity for the Department and other stakeholders to enhance the underlying security of election materials rather than relying on unencrypted email traffic containing personally identifiable information. PKI e-mail encryption can be part of a potential solution to protect the exchange of information between voters with CACs or PIV-I credentials and State election officials with a DoD External Certificate Authority or PIV-I credentials. However, further research is needed to improve user education on setting up encrypted e-mail transactions and explore other solutions.

¹² GSA. 2022. "Basics of a PIV." Retrieved from <https://playbooks.idmanagement.gov/piv/basics> on May 27, 2022.

¹³ Smart Card Alliance. 2022. "A Comparison of PIV, PIV-I and CIV Credentials". Retrieved from www.securetechalliance.org/resources/pdf/FPPIV_PIV-I_CIV_brief_022212.pdf&type=original on May 27, 2022.

Notional Implementation Resources and Timeline

From the standpoint of commercial product availability, several solutions exist in the marketplace for election jurisdictions to leverage when implementing end-to-end electronic voting services. The Presidential designee, however, determined that it is not positioned to include the potential use of commercially available technologies in this study as States are the proper authority to explore the incorporation of procurement for State systems.

Election jurisdictions leveraged past FVAP grants to procure commercial products to support electronic blank ballot delivery only as the grants did not enable the electronic return of voted ballots due to a strict prohibition within the grant's program requirements. Should Congress authorize the exploration of implementing end-to-end electronic voting services, existing commercial platforms could be leveraged to satisfy this feature subject to State certification and existing information assurance requirements. This would also apply should a jurisdiction choose to modify an existing system such as a centralized State database that can more readily support the absentee voting process for overseas military personnel and other UOCAVA voters. As grant applications from individual States are reviewed in a proposed grant issuance, contract support may be considered.

The Department requires these steps and associated lead times to support end-to-end electronic voting services for State and local election officials offering the direct systems for their eligible voters and accepting digital signatures:

1. Establish grants to fund the research, procurement, and development of election systems to support key steps of the absentee voting process and adherence to all Federal information assurance requirements. The specific functionalities required for these systems remain within the purview of State and local election authorities. Additionally, each State is required to offer a free access system for voters eligible to vote under UOCAVA to verify whether their ballot was received. An additional classification for acceptance or rejection of these ballots will readily identify whether the ballot was included within the final tabulation.

The ability for these systems to adhere to Federal information assurance requirements represents a significant investment of time and resources prior to implementation. The specific software and hosting architecture will impact the timing overall.

Total elapsed time represents 24 months to support a grant award process lasting 6-9 months with network hosting and software security reviews lasting 12-16 months. Year 3 represents final testing and leading into Federal election years represented by year 4. In this timeline, the approach envisions calendar window initiated in 2023-2024 for a potential fielding of these systems in time for the 2026-2028 election cycle.

2. Require participating States to authorize digital signatures within the election process. As a precondition for participation, election jurisdictions, through their associated State legislature or by administrative authority, must enable authorization digital

signature acceptance from the DoD CAC to support full end-to-end electronic voting services. Within this notional framework of providing end-to-end electronic voting services, the underlying architecture remains solely hosted by the State or locality.

The DoD is solely limiting its role to assisting State and local election officials with technical support to accept digital signatures from its existing identification cards for active-duty military personnel. The specific network connectivity and technical resources available for overseas military personnel would fall within the existing operational frameworks.

The ultimate size and scope of this effort may drive the need for the Department to secure additional technical support to assist election jurisdictions with implementation.

Total elapsed time represents 24-48 months running concurrent to State procurement and development efforts of these systems and subject to appropriation.

3. Conduct further research and issue credentials to State and local election officials to support the encryption of email transmissions to and from overseas military and possibly other UOCAVA voters. The continued use of unencrypted email containing personally identifiable information across DoD networks is an ongoing risk. Upon authorization, the DoD would work with the Department of Homeland Security to identify appropriate credentialing through a Federal External Certificate Authority or use of the PIV-I to State and local election officials in recognition of the critical infrastructure voting systems represent and enhance the overall security of election related transmissions.

It should be noted that the end user experience for overseas military personnel in this scenario would then integrate into the existing operational conditions for the Department. Military Service personnel would access the election materials directly from their workstations and be able to request, receive, mark, and return ballots without having to physically print, sign, scan, and return the completed ballot package. State and local election officials would remain ultimately responsible for the conduct of their systems, and the Department would maintain its current role. Additional opportunities exist for State and local election officials to enhance the security posture of these systems to meet existing Federal information assurance standards.

Key Findings

FVAP should continue the use of grants to assist States as a method of further encouraging solutions for military and overseas citizen voters. The advantages of a grant program would include the ability for the States/jurisdictions to maintain control of the source selection (continuing established vendor relationships if they prefer); develop new systems from the ground up or build on systems that already exist; and possess greater control of the system in the areas of requirements development, procurement, implementation, and testing. Management of the procurement process by State and local jurisdictions would ensure sufficient subject matter experts to provide expertise regarding State-specific election laws and procedures. It would maintain States' ownership of the results and would ensure their level of responsiveness to, and cooperation with, developers was maximized.

DoD remains best suited to support and assist absent uniformed services voters, their families, and U.S. citizens overseas with the absentee voting process, but not directly providing such services. The distribution of such personnel, their families, and overseas citizens across election jurisdictions vary significantly. Resources available for fielding voting systems specifically tied to this population remains driven by the individual jurisdiction. The DoD can assist in facilitating broad access to network and information technology resources, but should be limited external pathways and integration of DoD policy with the absentee voting process.

States provided electronic voting services should incorporate digital signatures to facilitate greater usability and reduce dependence on availability of physical equipment. States such as Nevada, Montana, and Maryland have authorized the acceptance of digital signatures from the DoD CAC for use in the UOCAVA absentee voting process. The use of electronic signatures remains commonplace within the DoD environment for military personnel. This practice should be strictly limited to digital signatures that result from the issuance of a rigorous credentialing process, such as those within the DoD, to ensure the utmost integrity.

Federal agencies should be leveraged to explore avenues for offering election officials the ability to encrypt email to and from active-duty personnel. The DoD leverages existing External Certificate Authorities to facilitate the credentialing process for Federal contractors and other customers doing business within the Federal environment. The use of the DoD CAC remains limited only to DoD personnel, inclusive of active-duty personnel, so its current utilization does not extend to election officials. However, the use of the PIV-I is a potential avenue as it is currently used for Federal contractors, stakeholders, and State election officials involved in critical infrastructure. The Department Homeland Security may have used cases for issuance of the PIV-I that fall within existing policy and could be leveraged to enable the encryption of email to and from military personnel.

As outlined, the proposed research timeline would span a minimum of 48 months culminating in fielding of such systems by State and local election jurisdictions supporting end-to-end electronic voting services that are subject to State certification requirements and applicable Federal information assurance requirements. Additionally, the DoD recommends requiring States to authorize the acceptance of digital signatures as a precondition for any participation and continue to work with the other Federal stakeholders to offer the ability to encrypt and decrypt corresponding election transactions with voters.