



10.December, 2009

**The Honorable Julius Genachowski, Chair
Federal Communications Commission**

c/o Commission's Secretary
445 12TH Street, S.W.
Washington, D.C. 20554

OSDV Foundation
Board of Trustees

Peter F. Harter
Intellectual Ventures LLC

Fran Maier
TRUSTe

Stacey Paynter
Strategic Connections LLC

Dr. Edgard Quiroz
QTeam Ventures LLC

Dr. Michael Henry
Frost Foundation

Gregory A. Miller
OSDV Foundation

E. John Sebes
OSDV Foundation

Strategic Adviser
Mitch Kapor

Re: Comments—NBP Public Notice # 20
Moving Toward A Digital Democracy
GN Docket Nos. 09-47, 09-51, 09-137

Greetings Chairman Genachowski:

The Open Source Digital Voting Foundation (OSDV), a non-profit public benefits corporation developing open source voting technology and representing the general public and stakeholders comprised of States' elections directors and other voting systems experts across the nation, is pleased to submit comments on *NBP Public Notice #20, Moving Toward A Digital Democracy*.

We applaud the Federal Communications Commission (FCC) effort and commitment to developing a national broadband plan that particularly includes a plan for the use of broadband infrastructure and services to advance civic participation. The portion of that civic participation plan we provide comment on hereunder addresses the election process *only*, specifically questions 1-3 inclusive, contained in DA 09-2431.

We completely concur that the election process and voting are essential to maintaining a functioning democracy and are also the civic processes in which the most Americans participate. We take that assertion one step further and submit that voting systems are a cornerstone of our increasingly digital democracy and should be treated as "*critical democracy infrastructure*." We hope that the Chair and the Commission find our comments helpful and informative.

Respectfully Submitted,

Gregory A. Miller, JD

Co-Executive Director & Chief Development Officer
Open Source Digital Voting Foundation
503.703.5150 | gam@osdv.org

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington DC 20002**

In the Matter of)
)
Moving Toward a Digital) GN Docket Nos. 09-47, 09-51
)
Democracy) GN Docket No. 09-137

REPLY COMMENTS — NBP PUBLIC NOTICE #20

THE OPEN SOURCE DIGITAL VOTING FOUNDATION AND TRUSTTHEVOTE PROJECT

In these reply comments to the Commission’s NBP Public Notice #20, the Open Source Digital Voting Foundation¹ (“OSDV”) and the TrustTheVote™ Project² encourage the Commission to embrace a citizen-centric approach to utilizing broadband infrastructure for civic participation, particularly in the essential democracy process of elections and voting. The so-called digital democracy phenomenon has been catalyzed by two key developments: **1)** the commercialization of the global Internet making it into the greatest information and communications medium since the advent of the telephone; and **2)** the increasingly mobile nature of American society. The result has been a dramatic increase in civic participation. Broadband technology can have a pivotal role in sustaining and

¹ The OSDV Foundation is a California-based non-profit public benefits corporation committed to making voting technology a publicly owned infrastructure asset that is open source to achieve accuracy, transparency, trustworthiness, and security in public elections. Private philanthropists including the Mitchell Kapor Foundation and other Grantor Organizations back the OSDV Foundation. See: <http://www.osdv.org>

² The TrustTheVote Project is the flagship effort of the OSDV Foundation, actually designing and developing open source voting technology driven by the requirements and specifications of its stakeholder community, a volunteer group comprised of States’ elections directors, experts, and officials across the nation. The Project is led by some of the most experienced technical architects in the California Silicon Valley, Boston’s famous Route 128, and the Pacific Northwest’s Silicon Forest with key contributors formerly or currently with companies such as Netscape Communications, Lotus Development Corporation, Mozilla Foundation, Apple, Network Associates, Oracle, and others. See <http://www.trustthevote.org>

increasing citizen participation in the processes of democracy provided its leverage is employed with care.

As a preamble to the OSDV Foundation’s comments specifically and exclusively addressing the first three questions posed in NBP Public Notice #20 with regard to the use of broadband infrastructure and services in elections processes, we submit the following general position statement with regard to the use of, or reliance upon the Internet in the conducting of elections. The OSDV Foundation believes election administrators and government must soon decide if and how they will use broadband infrastructure to improve election processes, and engage citizen input as early as possible, as is being done with this NBP Public Notice #20. There is no doubt that influence of the Internet in elections is growing worldwide³. However, that does not circumvent the fact that results of Elections must be verifiably accurate. In other words, they must be contained in a permanent record independent of any hardware or software used to produce said results. The OSDV Foundation believes there are several technical challenges to be addressed if ballot casting, that is, “votes” are ever to be transacted across packet-switched broadband infrastructure in a verifiable manner. There are other policy-oriented questions we set aside here as beyond the scope of our work, domain expertise, or position, but concern 1) to what extent citizens have equal access to the Internet to participate, or whether that is best addressed by a strategy that restricts broadband enablement to official polling places, which is the OSDV Foundation’s preferred approach, and 2) whether and to what extent ballot secrecy—a hallmark of American elections—can be properly preserved.

The OSDV Foundation believes there is potential to adopting broadband infrastructure for all aspects of elections administration but only after the technical challenges have been completely resolved in a transparent manner. A growing community of Computer Scientists has addressed those technical

³ Challenging the Norms and Standards of Election Administration, F. Clifton White, Applied Research Center for Democracy and Elections, 2007
<http://www.ifes.org/electionstandards.html>

challenges in a statement⁴ the OSDV Foundation largely endorses. Given those challenges, there is good cause to be cautious in fashioning a plan for civic engagement that includes using broadband infrastructure for casting and counting ballots. Such a plan, to be actionable and successful, must therefore publicly disclose in complete detail any principles of broadband-based elections administration that includes the ability for citizen's to cast a ballot and for said ballot to be tallied. Furthermore, any plan that intends to accommodate voting by broadband means must be based on principles that ensure integrity including, but not limited to: accuracy, transparency, trustworthiness, and security, in an auditable manner with complete accountability loops. Finally, the OSDV Foundation believes avoidance of these issues by simply ignoring the growing relevance and role of the Internet in American digital democracy will neither stop the revolution the Internet represents, or slow the evolution of our democratic process in a digital age.

The Commission, in effort to properly fashion a Plan as part of its Broadband policy, requests comment on specific issues in the consideration of the role of broadband infrastructure in the processes of democracy and citizen participation. We turn to the three pertinent questions in NBP Public Notice #20.

1. Registering to Vote.

- a. **Are there government jurisdictions that have implemented online voter registration? Can the impact of online voter registration be quantified compared to traditional methods, including registration numbers, voter registration application errors, and rejected applications? Are there qualitative impacts of allowing citizens to register to vote online, including positive or negative effects?**
- b. **Are there privacy concerns that jurisdictions must address if online voter registration is adopted?**
- c. **Are there fraud concerns that government jurisdictions must address if online voter registration is adopted? What steps can jurisdictions undertake to mitigate and elimination potential fraud in facilitating online voter registration?**
- d. **Would allowing citizens to register to vote online make it easier for those who have to travel long distances (such as people in rural and Tribal areas) or people who have difficulty traveling (such as some elderly or disabled Americans) to register to vote and therefore to vote?**

⁴ See Computer Technologists' Statement on Internet Voting at <http://verifiedvoting.org/downloads/InternetVotingStatement.pdf>

e. **How would online voter registration affect overseas military personnel, overseas diplomatic personnel, or other Americans living overseas?**

1a. Jurisdictions are implementing online voter registration.

So far, the states of Washington, Kansas, and Arizona have done so. And the key to their success is not primarily the online automation, but the data interoperability between their Secretary of State and their Department of Motor Vehicle IT systems, that enables on-line voter registration for an applicant who applies with a valid driver's license number for which there is a match between the driver's license data and the voter registration data. The impact of online voter registration be can quantified compared to traditional methods, including registration numbers, voter registration application errors, and rejected applications. In fact, traditional methods have to be supported in addition to new online methods. Since the same voter-record systems must be able to handle registration requests of both types, quantified comparisons are feasible from the voter-record system's log of registration application transactions.

There are qualitative impacts of allowing citizens to register to vote online, including positive and negative effects. Positive effects can include computer-aided assistance in filling out an on-line application, to prevent cases where a person is not registered because of uncaught errors in providing information required for registration. Similar positive effects include real-time error checking, such as detecting when a person has provided an incorrect drivers license number because of data entry error. Just as all these and other forms of computer assistance can be a positive factor, each can be a negative qualitative factor if the online system is poor in user interface, contains accessibility issues including literacy level, multi-language support, or contains technical defects that lead to an unreliable or confusing user experience. Much of the qualitative impact depends on the quality of the technical implementation and usability.

1b. There are privacy concerns to be addressed.

Jurisdictions must address some privacy concerns if online voter registration is adopted. A state must have clarity on what aspects of voter records are public, and what aspects are subject to the privacy constraints, and the corresponding privacy constraints must be implemented consistently, including resilience to malicious intent. One example of abuse is so-called “phishing expeditions” conducted by malfeasants in attempt to modify existing voter records, to discover name/address or name/drivers-license-number pairs. In addition to matters of public record, there may be exceptional cases as well, where a voter record is exempt from public record rules, such as where there is a restraining order in case of domestic violence, and a person's voter registration address should be maintained as private.

1c. There are fraud concerns to be addressed.

Government jurisdictions must address fraud concerns if online voter registration is adopted. Disenfranchisement can occur via intentionally erroneous preemptive registration of citizens, or fraudulent change-of-address of existing registered voters. These threats exist outside of a digital realm, but online automation can enable greater ease of carrying out these attacks in large numbers. Deterrence of large-scale automate abuse can be performed with technology referred to as "CAPTCHA" techniques⁵. However, additional work may be required to implement an online voter registration update system in which the risk of disenfranchising fraudulent re-registration is at least on a par with the risk in a paper-based system.

1d. Online voter registration supports and increasingly mobile and remote society.

In many cases, allowing citizens to register to vote online makes it easier for those who have to travel long distances, such as citizens in rural and

⁵ See generally: <http://en.wikipedia.org/wiki/CAPTCHA>

Tribal areas, or individuals who have difficulty traveling, such as certain elderly or disabled citizens to register to vote and therefore to participate in elections. However, these people would have to have immediate access to computing and networking facilities, and the on-line systems would need appropriate quality of accessibility and language support.

1e. Online voter registration would potentially have a very positive affect on overseas military, diplomatic personnel, and NGO Americans living overseas.

It might become possible for the ease of overseas persons registration and update to be on a par with domestic citizens who can use online voter registration. Reliance on paper systems, especially when coupled with distinct paper forms currently puts overseas citizens at a distinct disadvantage in terms of timeliness and feasibility of registration. To this extent, the OSDV Foundation believes the signing of Military and Overseas Voter Empowerment (MOVE) Act legislation into law is an imperative development in supporting overseas citizens' participation in our democratic processes of elections.

2. **Processes leading up to Election Day. There are many steps that come before the election polls open and close where broadband and online services may positively impact civic participation.**
 - a. **Do local, state, federal, Tribal or international government entities offer online mechanisms for providing information on elections? For example, as a supplement to web sites, do governments email out sample ballots or send email reminders regarding deadlines for registration? If not, are there existing barriers that prevent the use of online mechanisms for providing information on elections?**
 - b. **Do local, state, federal, Tribal or international government entities offer online mechanisms for voting on days other than Election Day? For example, are there online mechanisms that allow citizens to request absentee ballots, cast absentee ballots, or to schedule in-person voting on days other than Election Day? If not, are there barriers that prevent the use of online mechanisms to facilitate voting on days other than Election Day?**
 - c. **Are there positive or negative effects on the democratic process that can be directly attributed to enabling online versions of the processes leading up to Election Day?**
 - d. **How would enabling online versions of the processes leading up to election**

day impact overseas military personnel, overseas diplomatic personnel or other Americans living overseas?

2a. Many local, state, federal, Tribal or international government entities offer online mechanisms for providing information on elections.

Several states and local election jurisdictions both electronically and physically publish election information. Existing barriers are principally in the limitations of currently deployed proprietary election management system products, which do not in every case have easy mechanisms for exporting data such as ballot data or address/precinct/polling-place-location in a public format, and converting it to format useful for electronic publication.

2b. It is unclear whether state, federal, Tribal or international government entities offer online mechanisms for voting on days other than Election Day.

The OSDV Foundation is not aware of online mechanisms for casting absentee ballots; issues with these would be on a par with online voting, discussed in comments to question 3. For other cases such as absentee ballot request, or early voting request, the informational barriers are similar to those for **2a supra**. In addition, if some of these mechanisms are transactional in nature, and the transactions are not implemented in current election management system products, then custom government system development would be required.

2c. There are positive and potentially negative effects on the democratic process that can be directly attributed to enabling online versions of the processes leading up to Election Day.

As with online voter registration and record management, increased access and reduction in errors and error-detection-time are possible, but issues of technology access, usability and accessibility, etc could potentially offset these

positive outcomes.

2d. Enabling online versions of the processes leading up to election day would significantly impact overseas military personnel, overseas diplomatic personnel or other Americans living overseas.

Our comments are rendered largely moot by the signing of the MOVE legislation into law last month by President Obama. However, we go on record that in addition to recent improvements in overseas voter registration, the greatest feasible near term impact will be online distribution of printable un-marked paper vote-by-mail ballots, together with printable materials for return mail from the overseas voter to the correct mailing address of the election jurisdiction for that voter. Such online distribution will eliminate the outbound transit of ballot to voter, and enable most overseas voters to vote in time for their ballot to be transported to and arrive at the appropriate election jurisdiction. Another advantage will be providing the voter with the correct full ballot with all the contests and questions that they are entitled to decide. Currently, many overseas voters are limited to federal emergency write-in ballots for timely delivery, effectively barring them from participation in local elections.

- 3. Voting. Voting is the most fundamental of civic acts. As technology transforms all aspects of society, could voting be transformed as well?**
- a. **With existing technology, is it possible to enable and ensure safe and secure voting online today?**
 - b. **What can we learn from other nations that have considered or implemented online voting?**
 - c. **What can we learn from pilot projects that have tested online voting?**
 - d. **Have localities or states enabled online voting either domestically or for citizens abroad (such as military personnel stationed overseas)?**
 - e. **Do government jurisdictions at any level, domestic or foreign, allow online voting for any citizen? Have there been quantifiable impacts tied to online voting, including impacts on the number of citizens that voted? Have there been qualitative impacts tied to online voting, either positive or negative?**
 - f. **What are the security and privacy risks that government jurisdictions must consider when considering the implementation of online voting?**
 - g. **What are the history and current state of play of online voting technologies?**

- h. **What are best practice processes concerning online voting?**
- i. **How would enabling online voting impact overseas military personnel, overseas diplomatic personnel or other Americans living overseas?**

3a. With existing technology, is it difficult to enable and ensure safe and secure voting online today.

It is very difficult at present, because the fundamental goal is "parity;" that is, the risks and benefits of online voting should be in parity with the risks and benefits of vote-by-mail voters or remote paper voters compared to in-person voters. Comparison of risks and benefits is detailed, and burdened by the wide variety of election practices in thousands of separate jurisdictions nationwide. One solution would not offer parity for all the election jurisdictions in the county. Fortunately, the Federal Elections Assistance Commission ("EAC") has begun risk assessment and comparison work of various voting systems, including various forms of remote voting—an assessment that a member of the technical team of the OSDV Foundation is participating in to produce a study and ideally, a set of recommendations. Though far from complete, this work may have substantial impact on the ability for local jurisdictions to assess the feasibility, security, privacy, integrity, and authenticity of remote digital voting.

Aside from the lack of clear goals or requirements—well-specified parity of risks and benefits—there are substantial technical challenges to safe and secure online voting today, and significant variation in these challenges depending on the specific of various possible online voting approaches. For example, the most risky is the use of overseas-resident citizens' existing personal computers as the device for the voter to use in voting. A large portion of such computers are compromised by locally resident malicious software and their remote control, such as so-called "bots" in "botnets"⁶, that could enable re-purposing of malicious software to intentionally tamper with, falsify, or misappropriate a citizen's voting capability. By contrast, fixed-purpose, purpose-built voting kiosks could be more effectively protected and controlled; and deployment in physically controlled

⁶ See generally: <http://en.wikipedia.org/wiki/Botnet>

facilities, such as consular offices or military bases, could enable further control over the voting process. Even then significant problems remain, but these comparisons indicate the broad range of approaches and risks of several approaches to "on-line voting."

3b. There is minimal learning to be had from other nations' experiences with broadband voting systems.

Other nations—all of them parliamentary democracies—have addressed the significant challenges of remote voter authentication by using a national ID system, and in some cases, have strengthened authentication with a national smart-card system⁷. These approaches have historically been problematic in the U.S. although workable in other nations. Other nations have chosen to dismiss the risks of compromise of voter identity or ballot data, determining that the benefits ; that is, accessibility, more participation, outweigh risks deemed to be small in the sense of adversaries having little motive to target elections in that country, and at the level of complexity of a large number of specific localities' national parliamentary offices. The U.S. might well be a much higher profile target, having among other things, a governmental structure that enables a few key elections to have significant attraction for adversaries. Other nations have had less concern with dilution of voting anonymity, risks of electoral fraud, privacy issues, etc⁸. One reason for this may be that in most foreign online voting systems, there are centralized systems that **1**) authenticate voters, thereby ensuring that each voter casts only one ballot and **2**) that record those votes. Another reason appears

⁷ The State of Estonia has deployed such a system. See: http://en.wikipedia.org/wiki/Electronic_voting_in_Estonia and see also: http://en.wikipedia.org/wiki/Estonian_ID_card

⁸ Switzerland has utilized Internet voting and the OSDV Foundation's research and interviews with Swiss officials revealed a very different attitude and philosophy toward the fraud risk question, and greater sense of overall trust in government to function with utmost integrity. In fact, this year, Geneva citizens approved with a 70% majority the inscription of Internet voting into their constitution. See: <http://www.ge.ch/evoting/english/welcome.asp> See also generally: http://en.wikipedia.org/wiki/Voting_in_Switzerland

to be attitude and philosophy about the likelihood of government staff or contractor tampering. In these foreign online voting systems, Government IT staff, staff of outsourced IT services, as well as technical support staff of vendors of online voting systems, all have access to the voting systems and the data. These individuals are bound by operational policies and procedures intended to prevent modification of vote data, and to prevent disclosing the identity of the voter tied to a particular ballot. While there appears to be a far greater amount of trust exhibited by citizens of these foreign nations, this arrangement remains ripe with opportunity to compromise anonymity or vote data integrity. In the U.S. by contrast, many electoral jurisdictions have a far higher sensitivity to the issues voter anonymity, risk of electoral fraud, and data privacy. And their policies vary widely. For example, the Commonwealth of Virginia allows routine absentee voting only for UOCAVA voters, while other absentee voting is allowed only in attested hardship cases, whereas the state of Oregon utilizes vote-by-mail on a near exclusive basis. Therefore, the rubric of "*one size does not fit all*" indicates the difficulty of uniform application of any learning from other countries⁹.

3c. The learning from online voting pilot projects

U.S. pilot projects have essentially disregarded the IT risks to voter anonymity and enablement of electoral fraud, coercion, vote-selling, etc., as not relevant at the small scale of pilots. Most pilots have addressed technical threats using physically controlled kiosk systems. The typical Internet-security threats to the voting data center have been essentially treated as typical commercial-grade threats and counter measures, rather than being of any heightened risk, or any election specific risk, such as a “denial of service attacks” making data centers unavailable for use on election day.

One potential point of exploration, at least to the extent it may

⁹ For more on comparison with other countries, see "*Malfunction or Misfit: Comparing Requirements, Inputs, and Public Confidence Outcomes of E-Voting in the U.S. and Europe*" OSDV Foundation, Miller, Gregory A, and Sebes, Edward J, 3rd International Conference on Electronic Voting, 2008. <http://bit.ly/6bXZG3>

support the needs of UOCAVA voters, is whether Department of Defense (“DoD”) IP Networks could be availed to manage overseas voting and elections services data traffic. For example, the Joint Worldwide Intelligence Communications System (“JWICS”) is a component of the DoD network services used to transmit classified information by packet switching over TCP/IP in a secure environment. It is cleared up to Top Secret and SCI¹⁰. It also provides services such as hypertext documents and electronic mail. Another option is the less secure NIPRNet used to exchange sensitive but unclassified information between "internal" DoD users.

3d. Localities and States are enabling online voting exclusively for citizens abroad in limited cases.

There have been neighborhood council elections in the state of Hawaii conducted electronically, and water-control district elections in King County Washington, using remote electronic voting methods. These were not conducted by the local electoral jurisdictions that conduct statewide and Federal elections, and hence were not bound by regulations requiring the use of state or Federally certified voting systems. There are currently no certified systems that provide online voting.

3e. There are limited pilot projects allowing for citizen voting with varying quantitative and qualitative results.

While there are no certified systems that provide for online remote voting via broadband infrastructure, there are some limited pilot projects. The only project the OSDV Foundation is aware of at this writing is the Okaloosa Distance Balloting Pilot¹¹ in the state of Florida, which has used online voting technology, in kiosk settings, integrated with existing local voting systems, in a pilot effort, with paper ballots as the ballot of record. So far, there have been no quantifiable impacts

¹⁰ Sensitive Compartmental Information—this refers to methods of handling certain types of classified information that relate to specific national-security topics or programs whose existence may not be publicly acknowledged, or the sensitive nature of which requires special handling.

¹¹ See generally: www.operationbravo.org/our_solutions.html

in the U.S. to citizen participation tied to online voting. Other countries have reported increased participation, demographically weighted heavily to younger age citizens. In the U.S. there have been mixed results from remote voting leading to enhanced participation. So far, there have been no qualitative impacts in the U.S. to citizen participation tied to online voting. In other countries, election officials have reported anecdotal evidence of voter pleasure with online voting. Collection of negative impacts has not been performed to the knowledge of the OSDV Foundation.

3f. Security and privacy risks to be considered when implementing online voting are challenging, but potentially addressable in the long term.

This issue has been addressed in part in question **3a**, *supra*. In short, with existing technology, is it difficult to enable and ensure safe and secure voting online today. There are five points of consideration:

1. Integrity of the voting terminal, especially if a potentially malware-compromised personal computer is utilized;
2. Integrity of vote data as stored in the voting system's central data center, including both threats from staff, and electronic intrusion by outsiders;
3. Anonymity threats from trusted IT staff;
4. Authentication of voters, in other words, the ability to uniquely identify voters in a way that is not easy for adversaries to misappropriate, and to this extent, the phishing and key-logging challenges of online banking provide some metrics; and
5. Integrity and privacy of vote data in transit, and to this extent, the standard Internet Secure Socket Layer (“SSL”) mechanism for authentication and integrity can be used, but there remains the challenge of keeping voter data and vote data separate.

3g. The history and current state of online voting technologies is limited to small-scale pilots, although online voting systems vendors do exist.

In the United States, there are some small-scale pilot projects exploring feasibility and examining risk factors and points. There are several vendors of online voting systems, although the majority of their applications are for private elections. Abroad, a range of scale of applications that in all cases rely on key characteristics lacking in the United States including, but not limited to: national ID systems, greater trust in government election IT staff to maintain privacy and anonymity, and a lower assessment of the attractiveness of an online election as a target for adversaries.

3h. Best practices for implementing online voting are still emerging.

This has been addressed in question **3a** *supra*, however, understanding and implementing the “parity” discussed earlier is critical, but currently not well understood. From a technical standpoint, the OSDV Foundation believes two best practice points are already clear: **1)** do not utilize citizen’s personal computing devices as part of an online voting system for public elections, and **2)** if broadband infrastructure is determined to provide a level of service that achieves greater accessibility for an increasingly mobile society in a digital age, then the online voting systems should be utilized in a kiosk application and preferably in an authorized governmental polling place. Of course, the issues of voter identification remain for the purposes of serving a proper ballot for their jurisdiction of residence.

3i. There is varying degrees of impact at this juncture in enabling online voting for overseas citizens and military or diplomatic personnel.

In terms of the most pressing challenges, the impact might be modest. See the response to question **2d**, *supra*. The OSDV Foundation believes the greatest current challenge may be addressed without online voting. However, wide spread electronic ballot distribution has not yet been attempted, but recently mandated by

the MOVE Act, so it is hard to determine at present whether online voting will have a large incremental benefit in terms of enabling UOCAVA voters to vote effectively as they cannot do today. Experience with MOVE Act implementation will be a valuable guide in that regard. However, as implementation of the MOVE Act progresses, the OSDV Foundation offers four points of consideration:

1. An incremental approach should be taken to using the Internet to help UOCAVA voters, as there are several technical, procedural, and policy challenges in making the large transition from regular vote-by-mail services to a complete vote-by-broadband-connected-device service.
2. This transition, or leap as some might consider such, notwithstanding the public policy issues, involves addressing and resolving three primary challenges: **a)** the integrity of so-called “iVote” processes in light of the risks of UOCAVA voters potentially relying on personal or home broadband connected devices which could become infected with malicious software, combined with the risks of phishing and related Internet security concerns; **b)** the authenticity of the “iVote” process with secure distribution of digital credentials to each UOCAVA voter that enable them to utilize an “iVote” system without undue risk of their right-to-vote being misappropriated by others; and **c)** ensuring anonymity of votes cast by an “iVote” system given that authorized staff who have access to the system may also have the ability to observe both the authentication process and the ballot casting process for a given voter.
3. The next step in building UOCAVA support should be the use of broadband infrastructure for the distribution of blank vote-by-mail ballots, that are today sent by U.S. and international surface mails, resulting in the near impossibility for a UOCAVA voter to receive the ballot, mark their choices, and return it in time to be counted. Internet-based ballot distribution, secured by standard encryption means utilized today, if desired, will eliminate half the round-trip time required for vote-by-mail, making it possible for the voter to cast a

ballot in time to be counted. Moreover, given the strides in Internet-based UOCAVA voter registration, this next step could be piloted with those UOCAVA voters who are already using the Internet for communication with U.S. election officials.

4. Proceeding in an incremental fashion by starting with blank ballot transmittal or availability in digital form across the global Internet will enable elections officials to begin addressing the voter authentication issue, and learn more about secure communications processes. Pilot efforts in this regard should provide a public benefit by increasing UOCAVA participation, and to a level where empirical data about actual problems and limits on participation.

CONCLUSION

The OSDV Foundation and TrustTheVote Project are pleased to have an opportunity to provide comment on an increasingly vital aspect of broadband in the United States: its use in civic participation and the processes of democracy. We encourage the Commission to develop a comprehensive national broadband plan that particularly includes a plan for the use of broadband infrastructure and services to advance civic participation. To the extent this Plan includes consideration of broadband infrastructure for election processes and services, we advise careful consideration of what the architecture for a broadband-based voting system should look like and call upon experts and stakeholders to facilitate that understanding. Clearly, the digital age and increasingly mobile society can benefit from digital means for such civic participation services. However, the extent to which the challenges discussed herein can be adequately addressed remains unclear. Nevertheless, any such Plan should consider the possibility that broadband infrastructure may be called upon in the future to support and sustain elections services in some capacity, whether strictly for back-office functions or all the way out to ballot casting and counting services. We do not recommend reliance on home or personal broadband connected digital devices for citizen-facing voting services for the foreseeable future or until such time as the challenges discussed herein are

resolved to the satisfaction of the public. That advised, we do encourage the Commission to take a citizen-centric approach to fashioning its broadband policy with regard to civic participation in terms of voting and elections services. By “citizen-centric” we are referring to an approach that considers the wants and needs of an increasingly mobile society in a digital age. As one simple example, consider the typical citizen voting situation wherein the voter is employed sufficiently far away from their home precinct such that it is logistically impossible for them to reach their polling place in time before or after their work day to cast their ballot, while fulfilling their responsibilities to their employer. If there are any best-practices we can identify at this juncture with regard to broadband deployment of election services, two are particularly clear: **1)** personal or home connected devices should not be permitted to be utilized for ballot casting; and **2)** broadband connected ballot marking devices should be restricted to government authorized polling places. Finally, the overseas and UOCAVA voting challenges combined with the MOVE Act signed into law offer an opportunity to incrementally approach the reliance and leveraging of broadband infrastructure to improve participation of overseas citizens, military, and diplomatic personnel in U.S. elections. This should begin with the delivery of blank ballots.

At the pleasure of the Chairman and the Commission, OSDV Foundation technology experts and technology policy specialists in the domain of elections and voting technology reform are available to provide further information, insight, and testimony.

Respectfully submitted,

Gregory A. Miller
President & Chief Development Officer
The Open Source Digital Voting Foundation
665 Lytton Avenue
Palo Alto, CA 94301
503.703.5150 | gam@osdv.org