Fw: Please use this one w/ e-mail redactions -For SF Election Commission : Senate Hearing information/ election system security

Commission, Elections (REG)

Sun 1/14/2018 7:46 PM

Sent Items

To: Commission, Elections (REG) <elections.commission@sfgov.org>;

From: Brent Turner [redacted]
Sent: Tuesday, November 21, 2017 3:15 PM
To: Commission, Elections (REG)
Subject: Please use this one w/ e-mail redactions -For SF Election Commission : Senate Hearing information/ election system security

---------- Forwarded message ----------
From: **Brent Turner** [redacted]
Date: Tue, Nov 21, 2017 at 3:12 PM
Subject: For SF Election Commission : Senate Hearing information/ election system security
To: "Commission, Elections (REG)" <elections.commission@sfgov.org>

> Dear SF EC-
>
> Please include this information in the next meeting packet- it highlights some " nuance" regarding the open source system issue-
>
> Best - Brent Turner

_____Letter to Senate Intel Committee _____
_____

> Dear Senators / Congressmen and interested parties:
>
> Please accept this letter of information regarding the Senate Select Intelligence Committee hearing on election system security.
>
> To be clear we should initially note there was no mention of defense technology i.e. open source. As you may be aware,there is a growing movement in the United States to implement /deploy open source voting systems, and New Hampshire has now deployed such systems. San Francisco, Los Angeles and Travis County, Texas have started open source voting projects.

Currently the Department of Defense, NASA and the Air Force utilize open source and it is stipulated within the election technology community this is a necessary component of a proper election system.

Prof Halderman's lack of testimony regarding open source is curious His affiliation with those sympathetic to corporate software interests is hereby recognized. Although obviously paper ballots and robust auditing procedures are necessary elements of a proper system, they must be considered with the actual software. The fact this was omitted from his testimony speaks volumes. Although there was zero mention of open source technology by witness Professor Halderman at the hearing, this is not due to the lack of necessity of open source to the foundation of proper defense moving forward.

To be clear, we are on record as leading California legislative efforts for mandatory paper ballots and for the pioneering of paper ballot printing systems since 2004. However, it must be further stated that a paper ballot with a proprietary software system is still unacceptably vulnerable to hacking. The key to the defense environment is the elimination of the " secret /corporate /proprietary " software.. and an overhaul of the vendor controlled surrounding security environment via publicly owned systems.

Regarding certification, it should be stated that the father of the certification process Roy Saltman has made statement that the current US certification process is broken due to the intellectual property software issue.The"Independent Testing Labs" have been the focus of much investigation and are highly suspect. A proper open source environment with upgraded lab testing procedures will cure this problem

Regarding "Logic and Accuracy Testing", that too currently suffers from the lack of proper procedure and open source software usage. This current proprietary code testing process is not an appropriate defense against further manipulations. Again,solution to this element of the crisis is available but being under-presented due to business interests that are conflicting with the national security.

I have included some correspondence with the DHS as well as a letter from renowned technologist Brian Fox for your perusal. Attached is a letter from New Hampshire Secretary of State Bill Gardner This national security crisis is available for remedy but we must get our facts straight.

Please contact me to schedule technology solution conversations

Best regards,

Brent Turner
National Association of Voting Officials
[redacted]
www.navo-us.org

---------- Forwarded message ----------
From: **Brent Turner** [redacted]
Date: Mon, Jun 19, 2017 at 8:51 AM
Subject: Election system security information
To: associates.hq.dhs.gov
Cc: Brian Fox <>

Hello

As noted in our conversation and within the following correspondence , there has been a major effort to replace the vulnerable - proprietary - voting systems with appropriately secured -open source - voting systems. You are probably aware the Dept. of Defense , NASA, Air Force etc. utilize open source for " mission critical ".

As mentioned, corporate business interests not only have kept solution systems delayed (other than incremental steps in New Hampshire and California) but also are potentially keeping open source solutions from being fully presented at the crisis management and remedy conversations / hearings.

Brian Fox is available for duty on this if requested. Brian demonstrated solution systems in 2008 and is notable in the world of technology (Bash shell etc) Also I have attached a letter from the New Hampshire Secretary of State Bill Gardner. Please let me know if you desire further information regarding our efforts in San Francisco or elsewhere toward open source systems. Also,as mentioned, I spoke today with EAC Executive Director / NAVO board member Brian Newby and he is available as well.

We have briefed DHS, DNI and many others regarding this issue but remain concerned the solution is not being appropriately expedited. Obviously we are in national crisis so timing of solution effort is crucial.

Best regards,

Brent Turner
National Association of Voting Officials
www.navo-us.org
[redacted]
---------- Forwarded message ----------
From: **Brian J. Fox** <xxxx>
Date: Fri, Jun 16, 2017 at 2:23 PM
Subject: Statement and Questions
To: Brent Turner [redacted]

Esteemed members of the U.S. Senate -

I am Brian J. Fox, a technologist and software programmer of some note, and one of the founders of the Open Source movement.

I am certain that we are all in complete agreement that the integrity of our democratic process is paramount. I am beseeching you to take into careful consideration the following discussion related to our election systems, and the dangers of having computer systems that are not, at the minimum, running fingerprinted open source software during our elections, national or otherwise.

The use of a paper ballot for the purposes of counting votes is recommended for both machine-related vote tallying, and for audit and recounting purposes. In the case of machine tallying, the machine doing the tallying should be running software that the world can transparently validate the source code to, and processes should be in place to verify that the software running in the machine on election day is in fact the machine readable version of the publicly available source code. Any tallying machines should produce visible output for the public to see at each precinct no less than at the end of the of the polls, and photographic records of those tallies should also be made publicly available, along with the verification of the code in the machine.

These measures, coupled with visibly verifiable ballots, and good chain-of-custody practices, should result in an election that we can trust. Manipulating the software on the machine in secret will become detectable nearly instantly, and bugs in the software can be found by the eyes of 10's of thousands of software engineers, instead of only a few who are being paid to produce software that doesn't have bugs (a good ideal, but the wrong incentive to find bugs).

Proprietary software cannot satisfy such goals. The software for our democratic process should belong to the people that use it, and those people are the people of the United States at large, not an entity such as a single corporation which may have its own interests at a higher priority than the integrity of our vote.

Only open source software, licensed in such a way that it must remain open source, can satisfy the technology needs of a truly transparent and high integrity election system. We believe that every vote should be counted as cast, period.

Sincerely,

Brian J. Fox

==========
Letter for Haldeman
==========

Dear Alex -

I'm Brian J. Fox, a technologist and software programmer of some note (I wrote the Bash shell for one thing), and one of the founders of the FOSS movement.

I'm excited both for you and for your opportunity to help the people of the United States have a transparent and high integrity election. I would implore you to ensure that the following information is delivered to the senate via your testimony. I'm certain that you want to deliver the best possible chance of an unhacked election, and I know that you, like myself, would be devastated to have had the chance to explain to the senate how to avoid getting our election hacked, but to have allowed proprietary software to do just the opposite.

So, please explain the necessity for open source within our election systems. The need for fingerprinted binaries so that we can be sure that the software that is running is built from the publicly available sources. The requirement to have public records of the tally at each precinct so that anomalies can be spotted rapidly. The benefits of having large numbers of bi-partisan programmers and scientists evaluating the intent and execution of the algorithms. And the need for this infrastructure to belong to the people of the United States, and not to a corporate entity with its own interest.

It can only serve to make your arguments, testimony, and discussions more meaningful and memorable to the committee. And to deliver the sanctity of our vote that we were promised in the land of the free.

Thanks so much for your time and attention,

Brian
--
Brian J. Fox

On Wed, Jun 21, 2017 at 10:19 AM, Brent Turner <> wrote:

> Dear Senators / Congressman and interested parties:
>
> Please accept this letter of information regarding the Senate Select Intelligence Committee hearing on election system security.

To be clear we should initially note there was no mention of defense technology i.e. open source. As you may be aware,there is a growing movement in the United States to implement /deploy open source voting systems, and New Hampshire has now deployed such systems. San Francisco, Los Angeles and Traverse County, Texas have started open source voting projects.

Currently the Department of Defense, NASA and the Air Force utilize open source and it is stipulated within the election technology community this is a necessary component of a proper election system.

Prof Halderman's lack of testimony regarding open source is curious His affiliation with those sympathetic to corporate software interests is hereby recognized. Although obviously paper ballots and robust auditing procedures are necessary elements of a proper system, they must be considered with the actual software. the fact this was omitted from his testimony speaks volumes. Although there was zero mention of open source technology by witness Professor Halderman at the hearing, this is not due to the lack of necessity of open source to the foundation of proper defense moving forward.

To be clear, we are on record as leading California legislative efforts for mandatory paper ballots and for the pioneering of paper ballot printing systems since 2004. However, it must be further stated that a paper ballot with a proprietary software system is still unacceptably vulnerable to hacking. the key to the defense environment is the elimination of the " secret /corporate /proprietary " software.. and an overhaul of the vendor controlled surrounding security environment via publicly owned systems.

Regarding certification, it should be stated that the father of the certification process Roy Saltman has made statement that the current US certification process is broken due to the intellectual property software issue.The"Independent Testing Labs" have been the focus of much investigation and are highly suspect. A proper open source environment with upgraded lab testing procedures will cure this problem

Regarding "Logic and Accuracy Testing", that too currently suffers from the lack of proper procedure and open source software usage. This current proprietary code testing process is not an appropriate defense against further manipulations. Again,solution to this element of the crisis is available but being under-presented due to business interests that are conflicting with the national security.

I have included some correspondence with the DHS as well as a letter from renowned technologist Brian Fox for your perusal. Attached is a letter from New Hampshire Secretary of State Bill Gardner This national security crisis is available for remedy but we must get our facts straight.

Please contact me to schedule technology solution conversations

Best regards,

Brent Turner
National Association of Voting Officials

www.navo-us.org

---------- Forwarded message ----------
From: **Brent Turner** [redacted]>
Date: Mon, Jun 19, 2017 at 8:51 AM
Subject: Election system security information
To: [redacted]@associates.hq.dhs.gov

Cc: Brian Fox <xxxx>

Thank you for the conversation. Please confirm receipt. We are hopeful to provide information to Jeannette Manfra and did leave her a message.

As noted in our conversation and within the following correspondence , there has been a major effort to replace the vulnerable - proprietary - voting systems with appropriately secured -open source - voting systems. You are probably aware the Dept. of Defense , NASA, Air Force etc. utilize open source for " mission critical ".

As mentioned, corporate business interests not only have kept solution systems delayed (other than incremental steps in New Hampshire and California) but also are potentially keeping open source solutions from being fully presented at the crisis management and remedy conversations / hearings.

Brian Fox is available for duty on this if requested. Brian demonstrated solution systems in 2008 and is notable in the world of technology (Bash shell etc) Also I have attached a letter from the New Hampshire Secretary of State Bill Gardner. Please let me know if you desire further information regarding our efforts in San Francisco or elsewhere toward open source systems. Also,as mentioned, I spoke today with EAC Executive Director / NAVO board member Brian Newby and he is available as well.

We have briefed DHS, DNI and many others regarding this issue but remain concerned the solution is not being appropriately expedited. Obviously we are in national crisis so timing of solution effort is crucial.

Best regards,

Brent Turner
National Association of Voting Officials
www.navo-us.org

---------- Forwarded message ----------
From: **Brian J. Fox**
Date: Fri, Jun 16, 2017 at 2:23 PM
Subject: Statement and Questions
To: Brent Turner

Esteemed members of the U.S. Senate -

I am Brian J. Fox, a technologist and software programmer of some note, and one of the founders of the Open Source movement.

I am certain that we are all in complete agreement that the integrity of our democratic process is paramount. I am beseeching you to take into careful consideration the following discussion related to our election systems, and the dangers of having computer systems that are not, at the minimum, running fingerprinted open source software during our elections, national or otherwise.

The use of a paper ballot for the purposes of counting votes is recommended for both machine-related vote tallying, and for audit and recounting purposes. In the case of machine tallying, the machine doing the tallying should be running software that the world can transparently validate the source code to, and processes should be in place to verify that the software running in the machine on election

day is in fact the machine readable version of the publicly available source code. Any tallying machines should produce visible output for the public to see at each precinct no less than at the end of the of the polls, and photographic records of those tallies should also be made publicly available, along with the verification of the code in the machine.

These measures, coupled with visibly verifiable ballots, and good chain-of-custody practices, should result in an election that we can trust. Manipulating the software on the machine in secret will become detectable nearly instantly, and bugs in the software can be found by the eyes of 10's of thousands of software engineers, instead of only a few who are being paid to produce software that doesn't have bugs (a good ideal, but the wrong incentive to find bugs).

Proprietary software cannot satisfy such goals. The software for our democratic process should belong to the people that use it, and those people are the people of the United States at large, not an entity such as a single corporation which may have its own interests at a higher priority than the integrity of our vote.

Only open source software, licensed in such a way that it must remain open source, can satisfy the technology needs of a truly transparent and high integrity election system. We believe that every vote should be counted as cast, period.

Sincerely,

Brian J. Fox

==========
Letter for Haldeman
==========

Dear Alex -

I'm Brian J. Fox, a technologist and software programmer of some note (I wrote the Bash shell for one thing), and one of the founders of the FOSS movement.

I'm excited both for you and for your opportunity to help the people of the United States have a transparent and high integrity election. I would implore you to ensure that the following information is delivered to the senate via your testimony. I'm certain that you want to deliver the best possible chance of an unhacked election, and I know that you, like myself, would be devastated to have had the chance to explain to the senate how to avoid getting our election hacked, but to have allowed proprietary software to do just the opposite.

So, please explain the necessity for open source within our election systems. The need for fingerprinted binaries so that we can be sure that the software that is running is built from the publicly available sources. The requirement to have public records of the tally at each precinct so that anomalies can be spotted rapidly. The benefits of having large numbers of bi-partisan programmers and scientists evaluating the intent and execution of the algorithms. And the need for this infrastructure to belong to the people of the United States, and not to a corporate entity with its own interest.

It can only serve to make your arguments, testimony, and discussions more meaningful and memorable to the committee. And to deliver the sanctity of our vote that we were promised in the land of the free.

Thanks so much for your time and attention,

Brian
--
Brian J. Fox

Fw: CAVO response to Oct 18th TAC comments at EC - Please include in next packet

Commission, Elections (REG)

Sun 1/14/2018 7:43 PM

Sent Items

To: Commission, Elections (REG) <elections.commission@sfgov.org>;

From: Brent Turner <xxxx>
Sent: Wednesday, November 29, 2017 11:10 AM
To: Commission, Elections (REG)
Subject: CAVO response to Oct 18th TAC comments at EC - Please include in next packet

Dear Commissioners:

With all due respect to the fine people involved with Citizens Technical Advisory Committee (TAC) upon hearing their comments Oct 18th with regard to recommendations, and upon hearing the informed remarks of Commissioner Donaldson, it is the opinion of CAVO that TAC comments should be READ by others within the process but not necessarily stipulated toward as these citizen recommendations are merely opinions set forth by participants with no experience in creating open source election systems.

Though the TAC representative points toward 18 (f) and Los Angeles County for guidance, we want to again point the SF project toward the experts with experience that instituted the project,namely Alan Dechert, Brian Fox , and Dr. Juan Gilbert.

Best regards,

Brent Turner
CAVO Secretary

Fw: Please add to next SF Election Commission hearing packet

Commission, Elections (REG)

Sun 1/14/2018 7:41 PM

Sent Items

To Commission, Elections (REG) <elections.commission@sfgov.org>;

From: Brent Turner <xxxx>
Sent: Sunday, December 31, 2017 9:40 PM
To: Commission, Elections (REG)
Subject: Please add to next SF Election Commission hearing packet

http://www.sfgate.com/politics/article/SF-voting-security-group-urges-recount-of-ballots-10641050.php

SF voting security group urges recount of ballots in swing ...

www.sfgate.com

SF voting security group urges recount of ballots in swing states A voting security group, active in San Francisco for more than a decade, called Monday for a full ...

A voting security group, active in San Francisco for more than a decade, called Monday for a full recount, audit and investigation into the election results of four swing states that helped carry GOP businessman **Donald Trump** to victory in the Nov. 8 presidential election.

“An overwhelming majority of computer scientists have concluded the current voting systems are insecure,” **Brent Turner**, a board member of the **National Association** of Voting Officials, told a small crowd in front of San Francisco City Hall. “We believe there is enough evidence of manipulation to preclude certification of the election results until a thorough recount ... has occurred.”

In a letter last week, the group said that it found a “large and unprecedented discrepancy” between exit polls and final results in Wisconsin, North Carolina, Michigan and Pennsylvania.

While Turner admitted there is no hard evidence of major voting fraud in those states or anywhere else in the country, he argued that reports of efforts by foreign countries, most notably Russia, to influence the results of the election, combined with what he said was the vulnerability of voting machines run with corporate “proprietary” software, are reason enough to delay certifying the election results until a recount, combined with a forensic audit of the results, can be completed.

Jill Stein, the **Green Party** presidential candidate, already has paid for a recount in Wisconsin and Pennsylvania and plans to file Wednesday in Michigan. Democrat **Hillary Clinton**’s campaign will cooperate with the recount effort, although campaign officials have said they have seen no evidence of fraud.

Turner’s group, which is based in San Francisco, is using the uproar over Trump’s surprise victory to push for its long-sought goal of replacing California’s voting machines, now purchased from private companies, with publicly owned open-source voting systems.

Since private companies don’t make their software available for public inspection, it’s impossible to know whether bugs or back doors have been inserted into the voting software, open-source advocates say.

It would be different with a public open-source system, where the code would be available for public review.

“If you can see the bugs, you can fight the bugs,” Turner said. “You can use transparency as an asset.”

But it’s easier to talk about open-source software than it is to put it into use. In the entire United States, only Los Angeles and Travis County, Texas, have moved toward developing open-source systems for their elections, said **John Arntz**, San Francisco’s elections director.

The Travis County effort so far hasn’t made it past the proposal stage, he said, and the Los Angeles effort, which began in 2009, isn’t scheduled for use until 2020 at the earliest.

While San Francisco has put aside money to begin planning for an open-source software system, **“it will be years before one could be up and running,” Arntz said.**

In the meantime, Arntz is asking to extend the current agreement with Dominion Voting of Denver to provide the city’s voting system for two more years.

Dominion is the only company in the nation with a voting system that can handle San Francisco’s ranked-choice voting, Arntz said. Any open-source system would have to be custom-built to deal with the city’s needs.

John Wildemuth

Fw: Election Transparency and Security Act of 2018

Commission, Elections (REG)

Sun 1/14/2018 7:31 PM

To: Commission, Elections (REG) <elections.commission@sfgov.org>;

1 attachments (105 KB)

Initiative_1802881.pdf;

From: Brent Turner <xxxx>
Sent: Friday, January 12, 2018 8:47 AM
To: Commission, Elections (REG); Rowe, Jill (REG); Chris Jerdonek
Subject: Fwd: Election Transparency and Security Act of 2018

Please print out attached and add to next SF EC package-

Best-

Brent
---------- Forwarded message ----------
From: **Alan Jay Dechert** <xxxx>
Date: Thu, Jan 11, 2018 at 3:21 PM
Subject: Fwd: Election Transparency and Security Act of 2018
To: "Brian J. Fox" <xxxx>, Brent Turner <xxxx>, "David RR Webber (XML)" <xxxx>, "Juan E. Gilbert" <xxxx>

this has a few small but important revisions.... I'd consider this final

---------- Forwarded message ----------
From: **Kaplan, Alyssa** <Alyssa.Kaplan@legislativecounsel.ca.gov>
Date: Thu, Jan 11, 2018 at 3:06 PM
Subject: Election Transparency and Security Act of 2018
To: "xxxx" <xxxx>

Please find the revised initiative language attached; the hard copies will follow by mail. You can disregard the copies that were mailed out yesterday.

Thanks and all best,

Alyssa Kaplan
Deputy Legislative Counsel
Office of Legislative Counsel
925 L Street
Sacramento, CA 95814
916-341-8307

LEGISLATIVE COUNSEL
Diane F. Boyer-Vine

CHIEF DEPUTY
Aaron D. Silva

PRINCIPAL DEPUTIES
Joe Ayala
Sergio E. Carpio
Amy Jean Haydt
Thomas J. Kerbs
Kirk S. Louie
Fred A. Messerer
Lara Bierman Nelson
Robert A. Pratt

Stephen G. Dehrer
Lisa C. Goldkuhl
L. Erik Lange
William E. Moddelmog
Sheila R. Mohan
Gerardo Partida
Robert D. Roth
Michelle L. Samore
Stephanie Lynn Shirkey

DEPUTIES
JudyAnne Alanis
Paul Arata
Jennifer Klein Baldwin
Jeanette Barnard
Jennifer M. Barry
Vanessa S. Bedford
Robert C. Binning
Brian Bitzer
Rebecca Bitzer
Brian Bobb
Ann M. Burastero
William Chan
Elaine Chu
Paul Coatsum
Byron D. Damiani, Jr.
Thomas Dombrowski
Roman A. Edwards
Sharon L. Everett
Krista M. Ferns
Jessica S. Gosney
Nathaniel W. Grader
Ryan Greenlaw
Mari C. Guzman
Ronny Hamed-Troyansky
Jacob D. Heninger
Alex Hirsch
Stephanie Elaine Hoehn
Russell H. Holder
Cara L. Jenkins
Valerie R. Jones
Lori Ann Joseph
Dave Judson
Alyssa Kaplan
Amanda C. Kelly
Christina M. Kenzie
Michael J. Kerins
Deborah Kilcy
Mariko Kotani
Felicia A. Lee
Kathryn W. Londenberg
Richard Mafrica
Anthony P. Marquez
Aimee Martin
Francisco Martin
Christine P. Maruccia
Amanda Mattson
Abigail Maurer
Natalie R. Moore
Lindsey S. Nakano
Yooli Choi O'Brien
Sue-Ann Peterson
Lisa M. Plummer
Stacy Saechao
Kevin Schmitt
Amy E. Schweitzer
Melissa M. Scolari
Jessica L. Steele
Mark Franklin Terry
Josh Tesney
Daniel Vandehoolwyk
Joanna E. Varner
Bradley N. Webb
Rachelle M. Weed
Genevieve Wong
Armin G. Yazdi
Jack Zorman

LEGISLATIVE COUNSEL BUREAU

A TRADITION OF TRUSTED LEGAL SERVICE TO THE CALIFORNIA LEGISLATURE

LEGISLATIVE COUNSEL BUREAU
925 L STREET
SACRAMENTO, CALIFORNIA 95814
TELEPHONE (916) 341-8000
FACSIMILE (916) 341-8020
INTERNET WWW.LEGISLATIVECOUNSEL.CA.GOV

January 11, 2018

Mr. Alan Dechert
[redacted]

ELECTION TRANSPARENCY AND SECURITY ACT OF 2018 - # 1802881

Dear Mr. Dechert:

Pursuant to your request, we have prepared in appropriate form, the enclosed initiative measure to be submitted to the electors, relating to open source voting. We remind you that a title and summary prepared by the Attorney General are also necessary. (See Cal. Const. Art. II, § 10 (d); Elec. C. § 9002.)

Very truly yours,

Diane F. Boyer-Vine
Legislative Counsel

By
Alyssa R Kaplan
Deputy Legislative Counsel

ARK:pjb

INITIATIVE MEASURE TO BE SUBMITTED DIRECTLY TO THE VOTERS

12-point Boldface Type

The Attorney General of California has prepared the following circulating title and summary of the chief purpose and points of the proposed measure:

(Here set forth the unique numeric identifier provided by the Attorney General and circulating title and summary prepared by the Attorney General. Both the Attorney General's unique numeric identifier and the circulating title and summary must also be printed across the top of each page of the petition whereon signatures are to appear.)

TO THE HONORABLE SECRETARY OF STATE OF CALIFORNIA

Type: Roman Boldface not smaller than 12-point

We, the undersigned, registered, qualified voters of California, residents of ____ County, hereby propose amendments to the Constitution of California and to the Elections Code, and petition the Secretary of State to submit the same to the voters of California for their adoption or rejection at the next succeeding general election or at any special statewide election held prior to that general election or as otherwise provided by law. The proposed constitutional and statutory amendments read as follows:

SECTION 1. This act shall be known and may be cited as the Election Transparency and Security Act of 2018.

SEC. 2. Section 7.5 is added to Article II of the California Constitution, to read:

SEC. 7.5. The Legislature shall enact those laws necessary to implement statutes providing for voting technology updates, including the introduction of open source voting systems and smartphone-enabled voting.

SEC. 3. Section 14291 of the Elections Code is amended to read:

14291. (a) After the ballot is marked, a voter shall not show it to any person in a manner that reveals its contents, except as provided in subdivision (b).

(b) ~~A voter may voluntarily disclose how he or she voted if that voluntary act does not violate any other law.~~ A voter may take a photograph or digital image of his or her marked ballot and distribute or share the photograph or digital image using social media or by any other means.

SEC. 4. Section 18540 of the Elections Code is amended to read:

18540. (a) ~~Every~~ A person who makes use of or threatens to make use of any force, violence, or tactic of ~~coercion or intimidation, to induce or compel any other person to vote or refrain from voting at any election or to vote or refrain from voting for any particular person or measure at any election, or because any person voted or refrained from voting at any election or voted or refrained from voting for any particular person or measure at any election~~ coercion, intimidation is guilty of a felony punishable

by imprisonment pursuant to subdivision (h) of Section 1170 of the Penal Code for 16 months or two or three ~~years.~~ years if that action:

(1) Induces or compels any other person to do either of the following:

(A) Vote or refrain from voting at any election.

(B) Vote or refrain from voting for any particular person or measure at any election.

(2) Is undertaken because any person voted or refrained from voting at any election or voted or refrained from voting for any particular person or measure at any election.

(3) Induces, compels, or prevents any other person from distributing or sharing a photograph or digital image of his or her marked ballot.

(b) ~~Every~~ A person who hires or arranges for any other person to ~~make use of or threaten to make use of any force, violence, or tactic of coercion or intimidation, to induce or compel any other person to vote or refrain from voting at any election or to vote or refrain from voting for any particular person or measure at any election, or because any person voted or refrained from voting at any election or voted or refrained from voting for any particular person or measure at any election~~ violate the prohibitions set forth in subdivision (a) is guilty of a felony punishable by imprisonment pursuant to subdivision (h) of Section 1170 of the Penal Code for 16 months or two or three years.

SEC. 5. Chapter 5 (commencing with Section 19400) is added to Division 19 of the Elections Code, to read:

Chapter 5. Open Source Voting Systems

Article 1. General Provisions

19400. The Secretary of State shall promulgate regulations to further implement the provisions of this chapter.

19401. For purposes of this article, the following terms have the following meanings:

(a) "Ballot definition file" means a file that contains data about the contests and candidates specific to a particular election.

(b) "Messaging service provider" means an entity with the capacity to send and receive election materials in conjunction with a smartphone-enabled voting application.

(c) "Open source software" means software actually distributed to the public under software licenses that provide that every licensee is free to make copies of the software or derivative works thereof, to distribute them without payment of royalties or other consideration, and to access and use the complete source code of the software.

(d) "Open source voting system" means a voting system that uses open source software for all voting-specific components.

(e) "Shortcode" means a 4, 5, or 6 digit alphanumeric code used to send and receive election materials, including completed ballots, and to otherwise communicate with voters using smartphone-enabled voting applications.

(f) "Smartphone" has the same meaning as defined in paragraph (1) of subdivision (a) of Section 22761 of the Business and Professions Code.

(g) "Smartphone-enabled voting application" means an application that presents data from a ballot definition file to a voter and enables the voter to cast a ballot on his or her smartphone.

Article 2. Open Source Development Grant Program

19410. (a) The Open Source Development Grant Program is hereby established. The purpose of this program is to facilitate the development of open source software to be used in California voting systems.

(b) The sum of thirty million dollars ($30,000,000) is hereby appropriated from the General Fund to the Secretary of State to be issued as grants pursuant to this article.

19411. (a) The Secretary of State shall administer the Open Source Development Grant Program and shall make available three ten-million-dollar ($10,000,000) grants through a competitive process.

(b) By March 1, 2019, the Secretary of State shall allocate each of the three grants to a different consortium that satisfies the requirements of subdivision (c). In considering applicants for the grant, the Secretary of State shall take into account each consortium's demonstrated commitment to the development of open source software intended for use in public elections.

(c) To be eligible for a grant pursuant to this article, a consortium shall be organized as a nonprofit organization that is exempt from federal income taxation under Section 501(c)(6) of the Internal Revenue Code and shall have the stated purpose of making and maintaining open source software for elections systems.

19412. A consortium receiving a grant pursuant to Section 19411 shall use the funds to develop open source software and a smartphone-enabled voting application for use in California elections. A consortium may also use the funds for ancillary costs that are necessary to ensure the viability of the voting system, including documentation, testing, certification, training materials, and membership.

Article 3. Open Source Voting Systems

19420. Notwithstanding any other law, after December 31, 2019, the Secretary of State shall not certify any voting system other than an open source voting system. The state's use of an open source voting system does not preclude the use of the underlying open source software by other entities for other purposes.

19421. The sum of ninety million dollars ($90,000,000) is hereby appropriated from the General Fund to the Secretary of State to award grants to counties and cities to procure hardware necessary or helpful to run open source voting systems.

SEC. 6. Chapter 6 (commencing with Section 19500) is added to Division 19 of the Elections Code, to read:

Chapter 6. Smartphone-Enabled Voting

19500. The Secretary of State shall promulgate regulations to further implement the provisions of this chapter.

19501. (a) On or before January 1, 2020, the Secretary of State shall do both of the following:

(1) Contract with a messaging service provider to make a smartphone-enabled voting application available to voters.

(2) Lease a shortcode to be used across the state in smartphone-enabled voting.

(b) Each county shall make smartphone-enabled voting available to voters in every election conducted after execution of the contract described in subdivision (a). In order to effectuate this provision, the county shall provide the messaging service provider with the ballot definition file and the relevant personal information of each voter who has elected to vote by smartphone, including the voter's need to receive materials in a language other than English, as required by the federal Voting Rights Act of 1965 (52 U.S.C. Sec. 10101 et seq.) or by any other law.

(c) (1) If a voter wishes to vote by the smartphone-enabled voting application but is unable to do so, the elections official shall permit that voter to cast a vote by other means.

(2) If a voter casts a vote by the smartphone-enabled voting application and also by other means, the elections official shall not count the ballot cast by the smartphone-enabled voting application.

(d) A city may conduct a municipal election in accordance with the procedures set forth in this article.

SEC. 7. The statutory provisions of this act may be amended or repealed only by the procedures set forth in this section.

(a) This act may be amended to further its purposes by statute, passed in each house by rollcall vote entered in the journal, two-thirds of the membership concurring.

(b) This act may be amended or repealed by a statute that becomes effective only when approved by the electors.