Attachment E

February 5, 2009

Dear Chair Todd and Members of the House State...Affairs Committee,

I am writing to ask that you vote "no" on HB09-1160, which would allow online voter registration, as is not as "secure" as some people claim it to be.

The only study on the subject written with input from computer security experts is a report from the California Online Voting Task Force, done in 2000. Appendix A of that report discusses online registration. Please find that Appendix attached. It is worth reading. I will quote only a few sentences here:

"...with a paperless Internet registration system, the possibility of registering fraudulent or ineligible voters can be automated, and electronic registrations, almost by definition, will not receive the same human scrutiny as in a paper system...there is also the danger that the voter registration process might be interfered with by malicious code infecting the computer used for paperless registration. We discuss these issues at length later under the subject of Internet voting; but all of the potential problems that malicious code can present for Internet voting apply to paperless Internet voter registration as well. "

Since 2000, internet voting has been studied in more depth, and the dangers of internet voting have been established with greater certainty since 2000.

I asked David Jefferson, the lead researcher for the 2000 California study, and a reputable computer security expert with extensive knowledge of internet voting, if he would comment on online voter registration. Here was his reply of Feb. 2nd, 2009:

"Internet voter registration is a complex subject with potentially serious security and privacy hazards that no one has comprehensively investigated yet. Internet voting proved to be vastly more dangerous than anyone realized when it was proposed in 1999-2000, and while Internet voter registration may prove less hazardous, no one really knows at this point because it simply has not been seriously studied by technical experts. The much simpler issue of merging county registration records into statewide databases has proved to be a major problem in many states--far more difficult and fraught with problems than officials anticipated. A transition to Internet registration is likely to be equally technically challenging even if the security and privacy issues were resolved. Rather than jump in to Internet voter registration, I would urge any State to commission a comprehensive study of the subject first, with competent independent experts in computer and Internet security, databases, and election administration, with an emphasis on security vulnerabilities that could result in compromise of the contents of the registration database or its privacy."

When non-experts advocate using the internet for registration, they often mention that they bank online with no problem, so online registration should be equally safe. The answer to that, often made by computer security experts, is that banks are not safe from hacking, but that we don't often know about it, and when this is discovered, clients' losses are covered.

I happen to have a personal very recent example of this.
I got a letter just a few days ago from my credit union in Boulder, saying that they had to issue me a new VISA card because my old one "may have been compromised as a result of an unauthorized intrusion into Heartland Payment Systems", the company processing my VISA card charges.

Banks have the money to spend on very sophisticated security systems, and still their systems are vulnerable. Counties or states don't have the same kind of money to put into security, and it is a lot harder to make right the injustices done when registration lists are tampered with.

In conclusion, it is not in the interest of voters that new systems such as online voter registration are approved before comprehensive studies by responsible experts are done. These studies should cover the security risks and do a careful documentation of the actual, as opposed to the supposed, benefits.

Thank you for considering these comments.

Sincerely,
Margit Johansson
Coloradans for Voting Integrity
303-442-1668/ margitjo@gmail.com

Appendix A

# California Internet Voting Task Force

# Technical Committee Recommendations

Table of Contents

## 3 Internet voter registration

Voter registration systems are the basis of election legitimacy in most of the U.S. In most states each county maintains a database of names, addresses, and signatures for all eligible voters in that county who wish to vote. Its purpose is to guarantee that only people eligible by law to vote in a given district can do so, and that no one can vote more than once ("one person, one vote"). Any major compromise of the voter registration system could lead to fraudulent elections.

### 3.1 The current California voter registration system

To be eligible to vote in a particular district in California a person must be a resident of that district, a U.S. citizen, at least 18 years old, and not in prison or on parole for conviction of a felony. When a person registers to vote, his or her name and residence address are added to the database of eligible voters and he or she is also assigned to a voting precinct and to the appropriate election districts (assembly district, state senate district, congressional district, school district, utility district, etc.). A voter's registration remains valid for all subsequent elections until the county receives information that the voter has moved, or died, or otherwise become ineligible to vote. The voter's handwritten signature is kept on file and is checked against signatures submitted on requests for absentee ballots, on absentee ballot return envelopes, on initiative and other petitions, and, if our recommendations are accepted, on requests for authorization of i-voting.

Today, voter registration in California is based essentially on the honor system. A potential voter simply fills out and mails a voter registration form with his or her name, address, and signature. By signing the form, the voter attests under penalty of perjury to the truth of the name and address provided, *and* to his or her eligibility to vote (citizenship, age, etc.). A potential voter need not appear in person (as one must in order to get an initial driver's license or passport), nor is he or she currently required to present any documentary evidence either of identity or of eligibility to vote. Other than checking that the address listed on the registration form is a real address, and that the post office will deliver to the voter at that address, there is little that a county can do in California to check the legitimacy of a voter registration.

Unfortunately, the current paper-based voter registration system in California carries a potential for at least small-scale vote fraud. Anyone who is willing to fill out, sign, and mail a number of registration forms with distinct false names and real addresses, and who is willing to sign false affidavits, can attempt to register any number of fake voters and subsequently vote multiple times by absentee ballot using those false identities. But the current registration system involves actual paper forms with live signatures, and human inspection of the forms, and so any attempt to commit *massive* fraud successfully by registering a *large* number of ineligible or non-existent voters would be a complex, risky task. Patterns in the false names or addresses, or the postmarks, or the timing, or the purported signatures, would almost certainly be noticed by local officials, and the fraud would be detected.

A more secure voter registration system would increase the complexity of the registration process, for example by requiring the voter to appear personally before an official, or present documents, or both. This would reduce the voters' convenience, and possibly intimidate some, which together might reduce the number of people who register and vote. The registration process could less intrusively require voters to include additional information such as their driver's license or a portion of the social security number to help improve accuracy. The California Legislature, in enacting the Election Code, has in effect weighed the risk of fraud versus the risk of reduced voter participation and decided that a certain risk of small-scale fraud is worth taking in order to make voter registration a more convenient and less intimidating process for the law-abiding. This committee is not charged with judging the Legislature's decision on these issues and takes no position on the frailties of current paper-based registration system.

### 3.2 What is Internet voter registration?

There are various systems that might be referred to as "Internet voter registration". Some "print your own registration form" systems use the Internet simply to get a blank registration form to the voter – a service currently provided by the California Secretary of State. Other possible systems might involve registration kiosks of various kinds, and use the Internet to transmit a scanned image of the paper registration form to the county to avoid postal delays and to speed the county's processing of the paper forms. Finally, one can imagine a completely paperless system that would allow voters to register (or re-register) entirely online from a county controlled kiosk or from a home or workplace PC connected to the Internet, without any paper form at all. This is the most ambitious idea, and the most risky. We will discuss these three types of systems in turn.

#### 3.2.1 "Print your own registration form" systems

There are already online services that allow voters to register by bringing an image of the registration form from a server to their PC screens, printing it on their own printers, and then filling it out, signing it, and mailing it, exactly as they would a pre-printed form obtained from the county or state. California already has such a system in place for the federal version of the voter registration form.

One potential problem with such a system is that it is possible that third-party sites might give out registration forms that are not legally correct, for example by not requesting all legally required information, or by failing to inform the voter that a live signature is required. The best solution to this problem is for the state to recommend that third-party sites link to the state site rather than provide their own versions of the form. That way, when and if the form changes, there will not be a confusion of sites offering out-of-date versions.

"Print your own form" systems amount to allowing a facsimile of the official pre-printed registration form to be used instead of the real thing. As long as the paper registration system remains on the honor system in California, and does not require personal appearance or documentation of eligibility, "print your own form" systems present no difficult security problems. This task force recommends that they be encouraged.

### 3.2.2 Paper-based registration kiosks

Another type of Internet voter registration system would be an online registration kiosk provided by the county in convenient public places. A voter would fill out the same paper registration form as usual. But immediately, at the kiosk, some of the information would be keyboarded onto an electronic form, and the signature from the paper form would be scanned. The electronic form, along with the scanned image of the signature, would be transmitted to the county by Internet and immediately added to the county's voter database. The original paper form would be transported to the county later so that the paper form with live signature can be on file along with all other registrations.

A kiosk system might be valuable in states where voters are permitted to register up to a time very close to the election, or even on the same day as the election, because it allows the county voter rolls to be updated instantly, without staff labor, and from a kiosk site convenient to the voters.

There are a few potential problems that must be handled. First, the paper forms must still be used and must be reliably transmitted to the county, or the county could be faced with a registration that has no live signature to back it up. Since a scanned image of a signature alone is not a strong enough basis for future identity checks, the registration should not be considered complete until the county has the original signed form in hand. Until such time, the voter should only be permitted to vote provisionally in any intervening election, and the provisional vote should not count in the final tally unless a signed registration form arrives.

Unattended registration kiosks are conceivable. The voter could fill out and sign a paper registration form as usual, and then feed it into a roll-type scanner (as opposed to a flatbed) attached to an Internet-connected computer in such a way that the form is retained after scanning in a sealed box for later retrieval by county personnel. However, paper-handling machines must be treated gingerly, and have a tendency to jam, or feed diagonally; so we believe an attended kiosk will be much more reliable, and certainly much less subject to tampering, vandalism, prank registrations, and user errors such as scanning the back of the form instead of the front.

In theory, potential voters with scanners attached to their own home PCs could simulate a kiosk and do all of the steps of kiosk registration themselves, including transmitting the scanned image of the signed and completed form to the county registration servers, and mailing the original. However, there would have to be standards for the scanning parameters (image format, resolution, color depth) which many users would get wrong; and there would have to be defenses against attacks on the registration servers, whose IP addresses would have to be public. The benefit in convenience to tech-savvy voters with scanners does not seem to outweigh the costs, so we recommend against home simulation of a registration kiosk at this time.

Kiosk-based voter registration systems as described here retain the live signature feature of the current paper system in California, and are essentially automation aids to it. There are no insurmountable security problems with them, so this task force sees no reason why the state should not permit certification and deployment of human-attended Internet registration kiosks.

### 3.2.3 Security problems in paperless Internet voter registration system

An all-electronic Internet registration system, i.e. one in which a prospective voter can register himself or herself remotely from any Internet-connected PC, without the use of paper forms, seems like an attractive prospect—one that might simplify voter registration and lower its cost. But it is the judgement of this task force that, at the present time, such a system would also be an invitation to automated, large-scale vote fraud, and hence *we recommend that no system for all-electronic voter registration be certified.* This conclusion could be revisited if some kind of national identification infrastructure were created; but an infrastructure that could at least verify the identity of potential voters and some of the criteria for eligibility to vote is not likely to exist in the U.S. in the foreseeable future.

The following discussion explains the reasoning behind this recommendation. A fully satisfactory Internet voter registration system should verify the following:

*a.* *identification:* make sure that all registrations are associated with a real, living person, not a fake identity or the identity of a dead person;
*b.* *eligibility:* make sure that everyone who registers to vote is legally eligible to do so;
c. *non-duplication:* make sure that no one is registered more than once, either under multiple names or in multiple districts;

If even the first of these could be accomplished satisfactorily in an all-electronic system, one might judge the idea worthy of more study. Unfortunately, current technology has no way to accomplish any of these goals well. We discuss them in turn.

*Identification:* First we should note that current paper-based voter registration systems do a poor job of verifying that the registrant is a real person. This is especially true in California, where one has only to be willing to sign a false affidavit and mail it in order to register a fraudulent voter. One might argue that an Internet registration system with the same limitations as the paper system would at least be consistent with current practice, which is time-tested and reflects tradeoffs between security and convenience that the legislature has deemed appropriate. However, there is a crucial difference: with a paperless Internet registration system, *the possibility of registering fraudulent or ineligible voters can be automated*, and electronic registrations, almost by definition, *will not receive the same human scrutiny* as in a paper system. Anyone with a database of real California addresses, which can be purchased at many software stores, could invent fake names for any number of those addresses, register them to vote from a home PC, and later vote any number of times using those fake identities. Furthermore, he or she could do so remotely, for example from a foreign country, and make it appear that the requests came from many different places, all the while leaving no physical evidence, and perhaps being subject to little or no human scrutiny of the registrations, which would be recorded automatically.

The danger of automated, large-scale vote fraud through fraudulent Internet registrations, possibly committed by persons outside the U.S., is so severe that we believe no system should be certified that does not have strong means of identifying the registrant. Risks that may be quite reasonable with a paper system can become completely unreasonable in an automated system.

But there is today no widely-available, standard way to verify a person's identity over the Internet. There are several general techniques that might be considered, but all have serious limitations:

- *Reference to national identification systems:* One might require someone registering via Internet to include a reference to some other trusted database of certified identity numbers, e.g. birth or naturalization certificate number, or passport number. In business situations it is common to ask for social security number or driver's license numbers as a surrogate for identification. But each of these numbers has its limits as a means of identification, with varying standards for their issuance, and none of them is universal, nor available online to counties for this purpose.

There simply is no national ID system that can be used as a basis for assuring that false identities are not registered to vote via an Internet registration system. Birth certificates are issued by counties, and generally are not online; in any case they may be difficult or impossible to reliably connect to a prospective registrant as they often contain no biometric information at all, or only baby handprints or footprints.

Passport and naturalization certificates are issued by the federal government, and are also not online—at least they are not available to counties for voter registration purposes.

Even if there were a universal ID number that one could reference, and even if it could be somehow "checked" online during the Internet registration process, merely asking for such a number is not enough since that would still allow the person registering to report someone else's ID number, or that of a person who has died. A stronger mechanism, one that is actually linked to the person who is at the computer registering, would be required.

- *Digital signatures:* Another approach to identifying people through the Internet is via digital signatures. Citizens would create public-private key pairs and register the public keys with a certification authority. They could then participate in various cryptographic protocols, and could, for example, digitally sign their requests for registration via the Internet.

However, while a digital signature on a registration request proves that the request came from a holder of the private key, it does not prove that the key has been kept properly private, i.e. that it has not been "shared" with others, or stolen. More importantly, it does not prove that that person has only one such key, possibly issued by different certification authorities. A person with multiple keys might freely register multiple times. And while a certification authority might have a policy of trying to issue at most one key per person, in enforcing that policy it would face the same overall problem we are discussing: how does one verify a person's identity in the U.S., and hence ensure that a person does not create multiple "certified" digital identities.

A recent legislative proposal by Secretary of State Jones would allow Californians to register a public key with the Department of Motor Vehicles after providing proof of identity. The corresponding digital certificate issued by the DMV could then be used as proof of identification for numerous government transactions, possibly including voter registration.

- *County-maintained biometric database:* The strongest approach would be for the county to create (or subscribe to) a database of identification information, requiring potential Internet registrants to submit some biometric that is repeatable, unalterable, and distinctive enough to prevent multiple registrations, e.g. both thumb prints, or a DNA sample. A handwritten signature is not good enough for this purpose because it can be willfully altered: anyone can produce, and then reproduce, numerous different signatures.

Unfortunately, such a biometric-based system would not prevent both Internet and paper registration by the same voter, because biometric identification within the traditional registration process might be judged contrary to the National Voter Registration Act of 1993 ("Motor Voter"). And, although some personal computers today are being sold with fingerprint readers, and those devices are likely to become more common, there are still no open standards for fingerprint identification. In any case, many Americans are opposed to allowing government agencies to create additional biometric databases beyond those already maintained. They are concerned that information in other databases could be combined with that in biometric databases to facilitate tracking their behavior or invasion of privacy. Hence, use of biometric methods for identifying voters must be considered currently infeasible on political/privacy grounds.

*Eligibility:* Even assuming that we could verify the identity of potential voters, an Internet voter registration system should also verify their eligibility, i.e. determine citizenship, age, legal residence, and that the person is still alive. But just as there is no infrastructure for verification of identity, there also isn't any for verification of eligibility, nor is there likely to be any time soon.

Once again, we should note that the current registration system in California does not require any proof of eligibility to vote other than the voter's affidavit under penalty of perjury (and in fact makes it illegal to require such proof); hence one might argue that the standard of proof of eligibility would at least not be lowered if an Internet registration system also required only an affidavit. However, the possibility that, from a single PC anywhere on the Internet, fraudulent registration could be *automated,* is a new danger not present in current registration systems. Such illegal registrations might very well not be caught. In particular, any real people who are ineligible but who are fraudulently registered by someone else might never know it because, knowing themselves to be ineligible, they might never even try to register.

*Non-duplication:* It is easy to detect when a person registers more than once using the same identity in the same county, and to either ignore it, or treat it as a re-registration. But to detect if a person is registered to vote in more than one county or state requires cooperation among the 58 California counties, or the 3000 counties in the U.S. As before, the current paper based system is open to this kind of fraud at a small scale; but committing it on a large scale would be a tedious process, probably involving the efforts of many people to fill out enough registration forms needed to succeed. With Internet registration, however, the fraudulent registration process could be automated by a single person, from anywhere in the world, leaving no physical evidence.

California encourages, but does not require, registrants to write their driver's license number on the registration form. That feature helps a great deal to control benign duplication; but it is limited by the fact that it is not required, and that the driver's license system itself does not cover all voters and has its own security holes. In general, strong prevention of fraudulent multiple registrations is only feasible if there is a strong voter identification system.

As if these arguments were not strong enough, there is also the danger that the voter registration process might be interfered with by malicious code infecting the computer used for paperless registration. We discuss these issues at length later under the subject of Internet voting; but all of the potential problems that malicious code can present for Internet voting apply to paperless Internet voter registration as well.

Because under current conditions a paperless Internet voter registration system is so fraught with potential for automated fraud, and because there is no expectation that there will be any movement toward online infrastructure for strong identity verification in the foreseeable future, this task force recommends against adoption of any such system at the present time.