NISTIR 7711

Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

and technical controls that jurisdictions can use to help ensure safe transmission of ballots.

Blank ballots may be accompanied by additional personalized information on the voter affidavit or the ballot return envelope. This information often takes the form of a bar-coded voter identification number, which can help jurisdictions process returned ballots more efficiently by partially automating some of the data entry steps. Some commercially available systems allow jurisdictions to send out ballots with tracking information on return envelopes or ballots. This type of return identification information is usually non-sensitive, and does not require protective mechanisms to ensure confidentiality. However, this information may benefit from integrity protections, depending on how jurisdictions will use this information. Section 4.2 discusses issues that jurisdictions should consider when employing these mechanisms to track and identify ballot materials.

2.2 Electronic Delivery Options

Information can be quickly and easily transmitted electronically between parties by using fax, e-mail or posting information on Web sites. While e-mail and web sites both use the same underlying communications infrastructure, the public Internet, there are important distinctions between the ways these two technologies work, and how they might be used to transmit election materials.

2.2.1 Fax

Many jurisdictions use fax machines to send or receive absentee voting materials. Fax machines scan a document and transmit an encoded representation of it over the telephone network to another fax machine. The receiving fax machine can decode the information and print a copy of the scanned document. Current fax machines create a digital representation of the scanned document. The digital representation is then sent over the telephone network using analog signals.

There is no widely-used standard for fax encryption. Thus, information sent by fax is at risk for possible interception or modification. Jurisdictions should carefully weigh the risks of fax transmission of election materials against the possible alternatives prior to using fax to send or receive sensitive information.

There are some Internet-based fax service providers that allow users to send or receive faxes over the Internet, using web sites or e-mail to send or receive faxes. These services have complex security properties depending on how they are implemented or used. This document assumes jurisdictions using fax to send or receive election information will be using traditional fax machines directly connected to a phone line. However, jurisdictions cannot prevent voters from using these online services if they accept materials by fax.

2.2.2 Electronic Mail

2.2.2.1 Overview and Description

E-mail allows an individual to send text and/or files from one computer to another. E-mail is transmitted from the sender's computer to his or her mail server (often operated by his or her Internet Service Provider (ISP)), and routed through a series of intermediate servers and Internet routers before being delivered to the recipient's mail server (often operated by an ISP, workplace or a commercial e-mail service provider such as Gmail or Yahoo).

An e-mail sent from an election official passes through the jurisdiction's e-mail server, which is typically under the control of the local jurisdiction. The e-mail passes over the Internet, typically unencrypted, to a server controlled by the voter's e-mail service provider. In many cases, e-mail must pass through the public Internet once again to reach the voter, as many users have e-mail hosted by someone other than their Internet Service Provider (ISP). This connection may or may not be encrypted, depending on the voter's e-mail provider.

Just as mailed forms and ballots may be lost or delivered to a no longer valid address, e-mailed materials may not reach the intended voter. In many cases, senders will receive notification if the e-mail server of the recipient does not accept the message. Such an error may happen if the e-mail account is no longer active. However, just as election officials have no way of knowing if voters open election-related mail, they have no way of verifying that e-mails have been read by voters. While some e-mail clients support read-receipts, which are a way to request that the recipient send notification to the sender when an e-mail is read, these receipts are not widely supported in web-based e-mail clients and individuals typically must opt to send a reply. Consequently, the usefulness of read receipts for delivery confirmation may be limited.

As commonly implemented, e-mails are typically sent without cryptographic protections such as encryption or signing. As such, e-mails may be intercepted, read, and potentially modified as they are sent between election officials and voters. This is similar to the threat of mailed registration materials and ballots being delivered through the postal mail, which also has limited protective mechanisms. A key difference between these threats is