NISTIR 7711

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

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

[This page intentionally left blank.]

NISTIR 7711

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

Andrew Regenscheid
Geoff Beier

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2011

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

[This page intentionally left blank.]

Abstract

This document outlines the basic process for the distribution of election material including registration material and blank ballots to Uniformed and Overseas Citizen Absentee Voting Act (UOCAVA) voters. It describes the technologies that can be used to support the electronic dissemination of election material along with security techniques – both technical and procedural – that can protect this transfer. The purpose of the document is to inform Election Officials about the current technologies and techniques that can be used to improve the delivery of election material for UOCAVA voters. This document is part of a series of documents that address the UOCAVA voting. The first National Institute of Standards and Technology (NIST) publication on UOCAVA voting, entitled NISTIR 7551 A *Threat Analysis on UOCAVA Voting Systems*, was released in December 2008. In addition to NISTIR 7551, NIST has released NISTIR 7770 *Security Considerations for Remote Electronic UOCAVA Voting*, *Accessibility and Usability Considerations for Remote Electronic UOCAVA Voting,* and NISTIR 7682 *Information Systems Security Best Practices for UOCAVA-Supporting Systems.*

Acknowledgements

The authors of this document, Andrew Regenscheid of NIST and Geoff Beier of CygnaCom, wish to thank the state and local election officials who provided us with UOCAVA election procedures in preparation for this document. In particular, comments from Paul Miller, Matt Masterson and Carol Paquette were instrumental in the development of this document. The authors would also like to thank Russell Kasselman, Helen Purcell, Paul Lux, and the Florida Division of Elections staff. In addition, the authors wish to thank their colleagues who reviewed earlier drafts of this document, particularly Nelson Hastings, Barbara Guttman, Theresa O'Connell, and Quynh Dang.

Table of Contents

1 Introduction

To support State and local election officials in carrying out their responsibilities under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), the Election Assistance Commission (EAC) requested that the National Institute of Standards and Technology (NIST) develop security best practices to assist jurisdictions wishing to use electronic means to send or receive voter registration materials and ballot requests, or to distribute blank ballots to overseas and military voters. Many jurisdictions across the country already use electronic mail and fax for these purposes, and some jurisdictions have begun to use Web sites to distribute or collect this information.

1.1 Background

In December 2008, NIST released NISTIR 7551, *A Threat Analysis on UOCAVA Voting Systems* [1], which documents the threats to UOCAVA voting systems using electronic technologies for all aspects of the overseas voting process. NISTIR 7551 identifies a number of threats to using electronic technologies to obtain voter registration materials, deliver blank ballots, or return cast ballots, emphasizing the need for implementing strong and comprehensive security controls to mitigate the identified threats. That report concluded that existing widely deployed technology can be used to safely expedite the transmission of voter registration and ballot request materials, as well as blank ballots.

1.2 Purpose and Scope

This document first outlines the basic process for the distribution of election material including registration material and blank ballots to UOCAVA voters. It then describes the technologies that can be used to support the electronic dissemination of election material along with security techniques – both technical and procedural – that can protect this transfer. The purpose of the document is to inform Election Officials about the current technologies and techniques that can be used to improve the delivery of election material for UOCAVA voters.

This document provides security best practices for the delivery and receipt of documents such as voter registration applications and absentee ballot request forms, and the distribution of blank ballots to overseas and military voters using electronic mail or Web sites. It does not address remote electronic voting systems or the electronic return of cast ballots.

This document is part of a series of documents that address UOCAVA voting. In addition to NISTIR 7551, NIST has released NISTIR 7682 *Information Systems Security Best Practices for UOCAVA-Supporting Systems* [2]. NISTIR 7682 is a companion document to this document, NISTIR 7711. While this document covers security best practices and considerations for electronic transmission of UOCAVA election materials for election officials, NISTIR 7682 provides general computer security best practices for IT professionals charged with configuring and administering IT systems used to support UOCAVA voting. Jurisdictions should consult NISTIR 7682, and other NIST computer security guidelines, for general computer security best practices prior to deploying and using an IT system to support voter registration, ballot request, and blank ballot delivery activities. The best practices in this document are intended to extend, not override, the best practices in NISTIR 7682.

In addition to these security-focused documents, NIST released a document highlighting important human factors issues in UOCAVA voting systems, *Accessibility and Usability Considerations for Remote Electronic UOCAVA Voting,* in 2011 [23].

Jurisdictions seeking best practices related to election management, including election management for UOCAVA voting, should consult the EAC's *Election Management Best Practices* document [28], as well as their existing best practices for facilitating UOCAVA voting [29].

1.3 Audience

The intended audience for this document is election officials who are considering the use of electronic mail or Web sites to expedite transmission of voter registration materials and blank ballots. Readers are expected to consider this information within the framework of state and local election procedures and regulations. Only a basic understanding of information technology is required.

These best practices may also be useful to IT support staff charged with deploying, configuring, or maintaining the IT systems used to support the UOCAVA voting related activities described in this document, as well as system developers designing systems for these activities. As jurisdictions begin to deploy electronic delivery mechanisms alongside existing postal delivery mechanisms, previous decisions on appropriate policies and procedures for protecting election information may have to be reevaluated. This document identifies some of these issues that may come up when deploying a new system. As this document is primarily intended for election

officials, many technical details are left out of this document. The primary resource for technical computer security best practices is Draft NISTIR 7682 [2], along with NIST's existing collection of cyber security standards and guidelines.

1.4 Organization

Section 2 provides an overview of the types of election materials that jurisdictions may wish to send to voters by electronic means, and describes what information is provided in this document to facilitate the secure and reliable transmission of those materials to overseas and military voters. It also provides high-level descriptions of the two Internet-based transmission methods that are considered in this document, electronic mail and Web sites.

Section 3 discusses security best practices for sending or receiving voter registration and ballot request materials via fax, electronic mail or Web sites. The section emphasizes the importance of protecting sensitive personally identifiable information that may be recorded or stored by the system, and discusses items that jurisdictions should consider on the issue of voter authentication.

Section 4 covers security best practices for using fax, electronic mail and Web sites to deliver blank ballots to overseas and military voters. The section discusses issues that jurisdictions must consider before deploying electronic ballot delivery systems, including ballot control and tracking, and if voter authentication is required prior to serving ballots. This section also considers the use of e-mail to deliver printable ballots, posting blank ballots on Web sites for voters to download, and the use of online ballot markers.

This document includes two appendices that provide an election officials and staff with an introduction to key computer security processes. This information is similar to the material covered in Draft NISTIR 7682, but written for election officials rather than system administrators and IT staff. A basic understanding of these processes will help election officials manage their staff, and ensure that policy decisions are made and key activities are performed by the proper staff members. Appendix A provides a brief overview of general computer security best practices that jurisdictions should follow, mainly from a process perspective. Appendix B provides an overview of technical controls for protecting IT systems used to support UOCAVA voting.

2 Overview

2.1 Types of Election Materials

Electronic transmission methods can be used to deliver election materials at all stages of the election process. This section outlines different types of election materials that jurisdictions may wish to deliver to their uniformed and overseas voters using fax, electronic mail or Web sites, and highlights some issues regarding security controls needed to keep information confidential and unmodified.

2.1.1 Dissemination of Election Information Materials

Jurisdictions often make announcements reminding voters of upcoming elections, or asking them to ensure their voter registration information is up to date. They may also disseminate sample ballots and information explaining questions that will appear on the ballot, such as a bond issue.

The same message may be provided to all voters. In such cases, the information in the announcement is considered public information and therefore is not sensitive. This document will not discuss best practices for the distribution of these election information materials. However, ensuring the availability and reliability of the systems used to disseminate this information is important, and jurisdictions are directed to NISTIR 7682, *Information System Security Best Practices for UOCAVA Supporting Systems* [2], for information on security best practices to guard against accidental or malicious threats to system availability.

In some cases, announcements to voters may be personalized, particularly in the case of personalized e-mail messages to registered voters. For instance, an e-mail requesting that UOCAVA voters update their voter registration information may be personalized with the mailing address on file for each voter. Such communications should be treated as any other transmission of voter registration materials (see Section 2.1.2 for further discussion on voter registration and ballot request). In other cases, jurisdictions should consider the sensitivity of the personalized information on each communication when determining if additional security precautions should be taken.

2.1.2 Distribution and Receipt of Voter Registration/Ballot Request Forms

In most jurisdictions, overseas and military voters must register in the jurisdiction where they are eligible to vote absentee in order to be qualified to vote in future elections, although some jurisdictions waive registration for

military voters. A common method for voters to submit this information is the Federal Post Card Application (FPCA) [4], a standard federal form that all states are required to accept. In addition, each state has its own registration form that reflects its specific registration requirements. Both the state specific forms and the FPCA request the following information from voters: name, date of birth, sex, race, home address and political party preference. They also ask for various forms of contact information, including telephone number, fax number, e-mail address, and mailing address. The FPCA provides a field for a complete Social Security number and a field for a state driver's license number or other state identification number. The FPCA instructions for most states require only the last four digits of the Social Security number. This information is a matter of public record, and state law dictates both which fields may be shared upon request as well as how requestors may use that information. Both the FPCA and state specific forms typically require a wet signature. Signatures, Social Security Numbers and driver's license numbers are typically considered to be protected information that cannot be publicly released.

Blank FPCA and state specific registration and absentee ballot request forms are publicly available for downloading from multiple websites and do not require any special protections for electronic transmission. However, Social Security numbers, other official identification numbers, and original signatures require protection from unauthorized disclosure or modification when completed forms are being returned to jurisdictions either by mail or electronically. Section 3 will identify issues that jurisdictions should consider when evaluating the suitability of e-mail and Web-based return of these materials, and will discuss security controls that jurisdictions can implement to protect this information.

2.1.3 Blank Ballot Delivery

Because electronic transmission does not suffer from the same delays associated with postal mail delivery, e-mail or Web-based delivery of blank ballots can significantly reduce the round-trip transit time. Postal mail delivery to overseas locations can take significantly more time than delivery times within the United States. For example, one-way delivery through the military postal system to Middle East post offices takes at least 7-12 days [5]. Then the mail piece may have to be forwarded to the recipient's actual location, further increasing the transit time to the voter.

Blank ballots typically do not contain any sensitive information that must be protected from disclosure to third parties. However, care should be taken that ballots are reliably delivered to voters without unauthorized modification that could invalidate voters' cast ballots. Section 4 will discuss procedures

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

scale; an individual with the necessary technical skills may be able to intercept a large number of e-mails, while relatively few postal workers may be in a position to intercept a large number of mailed election materials. E-mail appears relatively more vulnerable to interception of messages compared to postal mail, where there are well-established legal penalties for tampering or intercepting mail.

Election officials considering the use of e-mail transmission of election materials should carefully consider the security limitations of e-mail and the availability of alternative delivery methods. Sensitive information sent over e-mail could be intercepted, read, and modified in transit. Sensitive information should not be sent over e-mail when suitable alternatives are available. E-mails can be easily forged to make it look like it was sent from another individual. These threats are not unique to e-mail, but could potentially be done on a larger scale than was possible with election materials mailed through the postal system. Election officials should consider the sensitivity of the information, the level of risk that it could be intercepted or modified, and the availability of suitable alternative delivery methods before using e-mail to transmit election materials.

- ***Registration and Ballot Request Materials:*** A typical application of e-mail in the UOCAVA voting process is to e-mail attachments (see Section 2.2.2.3) containing blank voter registration forms to voters (e.g., FPCAs), or receive completed forms from voters. Section 3.4 describes security best practices for e-mail transmission of voter registration and ballot request materials.

- ***Blank Ballots:*** E-mail is currently being used by many jurisdictions to send blank ballots to voters. Section 4.4 describes security best practices for e-mail transmission of blank ballots.

2.2.2.2 E-mail Error Messages

Incoming and outgoing mail servers may send error messages to the e-mail sender or originator in the event of some type of error. These take the form of e-mails from the sender or recipient's e-mail server. Election officials that send e-mails to voters should be familiar with typical e-mail error messages, but the absence of an error message does not necessarily mean that an e-mail was properly received by the intended recipient.

E-mails can fail to be properly delivered to a recipient for a variety of reasons. These include:

- The intended recipient's e-mail address is not recognized (e.g., the intended e-mail account does not exist, the address was mistyped, etc.).

- The outgoing e-mail server is unable to send e-mails due to a loss of communications or a malfunction.
- The recipient's e-mail server cannot be contacted.
- The intended recipient's e-mail folder is full, and the server will not accept additional e-mails.
- The outgoing e-mail server, or the recipient's e-mail server, detected a virus or classified the e-mail as spam.
- The e-mail is too large (e.g., due to a large attachment) for either the outgoing e-mail server, or the recipient's e-mail server.

Election officials should read error e-mail messages in their entirety to determine what additional steps to take. For instance, if the outgoing or recipient's e-mail server is down temporarily, the issue may be resolved on its own. However, if the error message indicates that a message was not delivered, the official should attempt to identify the source of the problem. The error message may reveal a technical problem that can be remedied, such as a problem with the e-mail server or a simple mistake, allowing the e-mail to be resent. If the problem cannot be remedied, election officials should apply the same procedures used by the jurisdiction when it has evidence that a mailed ballot did not reach its destination.

Election officials should be aware that some e-mail error messages are sent to the intended recipient, not the sender. For example, if an e-mail is filtered by the recipient's e-mail server due to a detected virus, often that server will only send the error message to the recipient.

2.2.2.3 Attachments

E-mail messages are text-based, but can include one or more files as attachments. While text-based e-mails are usually relatively small, e-mails containing attachments can be quite large. Depending on the attachment, an e-mail could become large for the sender's or recipient's e-mail server. In most cases, e-mails under 2MB) will be transmitted and accepted by e-mail servers.

E-mail servers often scan attachments for viruses, and some e-mail servers will reject e-mails containing attachments of certain file types that often contain viruses. In most cases this should not be an issue for jurisdictions, as typical file types (e.g., .DOC, .PDF, .RTF, .JPG) will be accepted.

2.2.2.4 E-mail Encryption and Signing

E-mail can be cryptographically protected using encryption or digital signatures. E-mail encryption protects e-mails from being read by unauthorized parties, while e-mail signing allows recipients to verify the origin and integrity of the message. The most widely-used standard for e-

mail encryption and signing is called Secure/Multipurpose Internet Mail Extensions (S/MIME) [7], which is described further in NISTIR 7682, *Information System Security Best Practices for UOCAVA Supporting Systems* and NIST SP 800-45, *Guidelines on Electronic Mail Security* [9].

Jurisdictions may receive digitally signed e-mails from UOCAVA voters, particularly from military voters using their Department of Defense e-mail accounts. The contents of these e-mails can generally be read without any specific e-mail software, but additional measure must be taken to verify the digital signatures on these messages. Jurisdictions that wish to verify the signatures from military voters need to use an e-mail client that supports S/MIME and will need to install the trust anchor for the US Department of Defense Root Certificate Authority. Configuring e-mail clients to receive and verify S/MIME signed e-mails is covered in Section 5 of NISTIR 7682.

Jurisdictions could also digitally sign messages they send. This also requires an e-mail client that supports S/MIME, which must be configured with a cryptographic key and a certificate that binds that key to the jurisdiction. Certificates can be purchased from commercial Certificate Authorities (CA), although only some of them issue certificates for S/MIME. Some states also run their own Certificate Authority. However, signing e-mails is only beneficial if voters have a properly-configured e-mail client that supports S/MIME, expect to receive signed emails, and know how to use the client to verify the signatures on those e-mails. As signed e-mails are not common outside of the military environment, this may not be true for overseas civilians or military personnel using personal e-mail accounts. Jurisdictions that still wish to sign e-mails should consult Section 5 of NISTIR 7682.

2.2.2.5 DomainKeys Identified Mail

The Internet Engineering Task Force recently completed a suite of standards for DomainKeys Identified Mail (DKIM) [10]. DKIM is a limited form of e-mail authentication that allows a jurisdiction's e-mail server to sign outgoing messages so other DKIM-aware e-mail servers can verify the integrity and origin of the message. This is typically used to protect against unsolicited e-mails, also known as spam. Individuals sending spam sometimes forge e-mails to trick recipients or to try to avoid e-mail spam filters. DKIM provides a mechanism for detecting forged e-mails, but only when the receiving e-mail server and the e-mail server for the (possibly forged) organization support DKIM.

Use of DKIM by jurisdictions' e-mail servers can help to reduce the chances that their outgoing e-mails will be marked as spam by recipients, and could help to improve their own e-mail filtering systems for spam and malware.

Current best practices for jurisdictions include using DKIM to sign outgoing mail and have DKIM-aware servers to process e-mails to protect themselves from spam and malware, but should not rely on DKIM to verify the original senders of e-mails. Accepted best practices will change over time as DKIM is more widely adopted.

2.2.3 Web-Sites

2.2.3.1 Overview and Description

Web sites are a popular method for posting information so that anyone with a Web browser can access it. Web sites can be used to host election information, voter registration forms, or blank ballots. Some jurisidictions have also used web sites to allow voters to submit voter registration information.

While e-mails could be lost or delivered to an invalid address, web sites allow voters to instantly access information at-will. While web sites could become unavailable due to technical difficulties or malicious attacks, they do not suffer from some of the potential delivery problems as postal mail or e-mail.

However, just as with postal mail and e-mail, communication between a voter and a web site could be intercepted, read, or potentially modified in-transit. Wide-deployed cryptographic protections, such as Transport Layer Security (see Section 2.2.2.4) could be used to guard against many of these attacks. However, there are less sophisticated, but often just as effective, attacks that attempt to trick users into accessing the wrong web site. For example, a typical attack on the Internet called Phishing involves tricking a user into clicking on a link to a fraudulent Web site that closely mimicks the legimate site, such as copying the jurisidictions' logos. Such attacks are very difficult to block by technical means, but can be mitigated through awareness training.

2.2.3.2 Online File Repositories

Web sites may be used to host election-related documents, such as voter registration and ballot request forms (e.g., FPCA) or blank ballots. These sites could be available for all visitors to the site, or access to these forms may be controlled so that only users with a password, or some other authenticator, can access the forms. While Web sites may be more expensive to deploy and use than e-mailing election materials, they do have several advantages. Notably, there are greater security protections possible for delivery of materials over Web sites than over e-mail (see Section

2.2.3.4). Security best practices for posting forms and other information on Web sites will be discussed in Sections 3.5.1 and 4.5, respectively.

It is also possible for users to upload files to a Web site, as an alternative to e-mail. Again, an advantage to this approach is that Web-based transmission is easier to protect than e-mail transmission. Receiving voter registration or ballot request forms over Web sites will be discussed in Section 3.5.2.

2.2.3.3 Sites with Active Content

Rather than merely posting static Web pages or documents, Web sites often include active content that run as a sort of application in users' browsers. This could take the form of a Web-based form and javascript where a voter enters information, or a Java or Flash-based application that is downloaded by a voter's browser and executed within the browser window.

For example, a Web site supporting voter registration and ballot request could have a Web-based form that allows voters to enter their registration and contact information, and submit it to the election officials. Often Web-based forms will include some logic that advise users of mistakes, such as omitting required information such as an address or phone number. These sorts of forms are a staple of e-commerce Web sites. These forms could also be used for online ballot marking, allowing voters to record their selections on the form before printing the voted ballot for return through the mail.

Section 3.6 contains security best practices for receiving voter registration or ballot request information using Web sites with active content. Section 4.6 contains security best practices for using these technologies to allow voters to receive and mark a ballot electronically.

2.2.3.4 Transport Layer Security

Transport Layer Security (TLS) [14], and its predecessor, Secure Socket Layer (SSL), are cryptographic protocols that provide confidentiality and integrity protection for communications between a Web server and a client accessing that server. TLS and SSL are widely used on the Internet to provide a safe communications channel for sending sensitive information. For instance, nearly all e-commerce Web sites use TLS to protect any financial or transaction information sent between the server and user.

TLS is typically used with only server-side authentication, meaning that users connecting to a Web site can verify that they are communicating with the intended entity, but the Web server does not cryptographically verify the users. To be effective, TLS-enabled Web servers must have a public key

signed by a commonly-trusted certificate authority. There are a number of commercial vendors for TLS certificates. However, while TLS is capable of verifying the identity of users (typically called client-side authentication), this requires users to have a public key signed by a trusted certificate authority. This typically is not the case.

TLS is an inexpensive, widely deployed and supported technology, which should be employed by any Web server that sends or receives sensitive information.

2.3 Cryptography

Cryptography is the use of mathematical and computer algorithms to protect the confidentiality or integrity of information as it is stored or transmitted. Most cryptographic algorithms fall into one of two classes:

- Encryption algorithms for protecting the confidentiality of information in-transit or in storage.
- Message authentication codes or digital signatures for establishing trust in the authenticity and integrity of information.

Cryptographic algorithms are used in cryptographic protocols to provide the intended security properties. These protocols often combine several different algorithms to provide confidentiality and integrity protections. Proper use of cryptography is critical to the protecting information in computer systems. Previous sections gave some examples of the use of cryptography to protect information as it is transmitted over the Internet: e-mail encryption and signing, and the SSL/TLS protocol for protecting web sites. This section provides additional background information intended to give readers a better understanding of how cryptography can be used to protect information in UOCAVA voting systems.

2.3.1 Cryptographic Confidentiality Protections

Encryption algorithms are cryptographic algorithms that aim to protect the confidentiality of information. These algorithms scramble (encrypt) information so that it can only be unscrambled (decrypted) and read by someone with the correct key, which must be kept secret. Encryption algorithms might be used on stored data in computer systems to help ensure sensitive information is not read by unauthorized individuals. Or it might be used to protect information that is transmitted over the Internet so eavesdroppers are not able to read the data.

Most encryption algorithms fall into one of two categories: symmetric encryption and asymmetric encryption.

- **Symmetric encryption algorithms** use a single secret key to encrypt and decrypt information. For that reason, it is sometimes called secret key encryption. It is most often used to encrypt information that is stored locally on a machine, or to protect information that is transmitted between two different parts of a single system. Proper key management is particularly important when using symmetric encryption algorithms. The key must be securely stored. If a symmetric encryption algorithm is used to protect information sent between two computers, users must securely load the same key on both systems, usually by manually loading the key. The two government standards for symmetric encryption algorithms are the Advanced Encryption Standard (AES) and the Triple Data Encryption Standard (TDES).
- **Asymmetric encryption algorithms** use two different keys: one key to encrypt data, and one key to decrypt data. The key used to encrypt data is the public key, and can be shared with anyone. The key used to decrypt data is the private key, and must be kept secret. Because the encryption key can be freely shared, asymmetric encryption algorithms are often easier to use when two parties are communicating over the Internet. Asymmetric encryption algorithms are rarely used to encrypt content directly. Asymmetric encryption algorithms are usually used to encrypt a new key. This new key is used in a symmetric encryption algorithm to encrypt the actual content. Asymmetric encryption algorithms include algorithms such as RSA and Diffie-Hellman, and are frequently used in electronic commerce.

2.3.2 Cryptographic Integrity Protections

There are several different types of cryptographic algorithms that can be used to protect the integrity of information. Notably, these include digital signatures and cryptographic message authentication codes. These algorithms primarily provide two security properties. First, they allow users to verify that the information was not changed. Second, they allow users to authenticate the originator of the information.

- **Digital Signature algorithms**, like asymmetric encryption algorithms, use two different keys. One key is used to sign data, while the other key is used to verify signatures created using the first key. The key used to verify signed data is the public key, and can be shared with anyone. The key used to sign data must be kept secret to prevent other people from forging signatures. Digital signatures are used in many applications to provide integrity protection and to authenticate users and information.

- **Message Authentication Codes,** like symmetric encryption algorithms, use a single secret key to compute and verify cryptographic fingerprints. These fingerprints are somewhat similar to signatures, except only someone that knows the secret key can verify the tag. Message authentication codes are frequently used to protect information that is transmitted over the Internet from manipulation.

2.3.3 Cryptographic Protocols

Cryptographic algorithms are used as building blocks in cryptographic protocols. These protocols usually use a combination of cryptographic algorithms to provide a combination of confidentiality and integrity protections. For example, the S/MIME protocol uses digital signature algorithms and both symmetric and asymmetric encryption algorithms to encrypt e-mails, sign e-mails, or encrypt and sign e-mails. The TLS protocol uses all four types of cryptographic algorithms previously described to protect the confidentiality and integrity of data transmitted between users and web servers.

2.3.4 Digital Certificates

Digital signatures and asymmetric encryption are examples of public key cryptography. These types of cryptographic algorithms require that its users have a private key that must be kept secret, and a public key that can be freely shared without a loss of security. However, there needs to be a way to securely bind the identity of a user or system to a specific public key, otherwise users would not know what public key to use when communicating with another user.

This kind of binding is done with a digital certificate. A certificate is a record with several fields. The most important of these fields include:

- *Identifier*: This field (or fields) identifies the person or system that "owns" the certificate. This person or system is known as the "subject." For SSL/TLS, it may be a web site address. For S/MIME it may be an e-mail address. In other cases it might just be a name.
- *Public Key*: This field contains the subject's public key that other users should use when decrypting messages or verifying digital signatures.
- *Algorithm Use*: This field describes what algorithms or protocols may be used with the digital certificate.
- *Expiration Date*: Most certificates expire after a set period of time. The duration of the certificate will depend on a number of factors, including the strength of the cryptographic algorithm and key, how the certificate will be used, and the cost of the certificate.

The information in digital certificates is digitally signed by a certificate authority. This signature is the certificate authority's way of attesting that the individual (or system) in the identifier field is the true owner of the public key found in the certificate.

Which systems require digital certificates depends upon the particular cryptographic protocol. For example, web servers using TLS/SSL need a digital certificate from a trusted certificate authority, but users who access the web site do not need to obtain their own certificates (unless the server is also cryptographically authenticating users, which is sometimes done in high-security systems). A user signing an e-mail using S/MIME must obtain a digital certificate. Signed e-mails from the user contain a copy of this certificate, allowing recipients to verify the signature. However, recipients must trust the certificate authority who issued the certificate.

2.3.5 Certificate Authorities

Certificate authorities are trusted third-parties that vouch for the validity of an individual's certificate, asserting that the individual or system identified in the certificate is the "true" owner of the public key identified in the certificate. The receiver of a signed message, or the sender of an encrypted message, must trust the certificate authority that issued the certificate used in the transaction.

For the applications of cryptography outlined in this document, there are primarily two ways to obtain widely trusted digital certificates. The most common way is to purchase one from a commercial certificate authority. There are several commercial certificate authorities that sell digital certificates. Jurisdictions should be careful to purchase certificates from authorities that are widely trusted by their targeted systems. For example, if a jurisdiction is purchasing a digital certificate to enable the use of TLS on a web server, the jurisdiction should ensure the issuing certificate authority is trusted by all major web browsers that voters may use to access the web site.

Alternatively, some states may run their own certificate authority. State and local jurisdictions may also be able to obtain and use certificates from these authorities, particularly if the state's certificate authority is affiliated with the federal government's certificate authority. Again, jurisdictions will need to ensure the certificate authority is widely trusted by applications that may use the system.

Jurisdictions will also need to ensure that they obtain the right kinds of certificates. A certificate used for S/MIME e-mail signing cannot be used to

digitally sign documents, or implement TLS on a website. Certificate authorities usually do not issue certificates for all types of applications.

While the costs of obtaining certificates can add up if a large number of certificates are needed for a large number of systems or users, the applications of cryptography identified in this document will typically not require such large deployments. In most cases, jurisdictions will only need to purchase a very small number of certificates to make use of TLS on web servers or to sign documents.

3 Transmission of Registration/Ballot Request Materials

3.1 Overview

Voter registration and requests for a blank ballot by the UOCAVA voter can be reliably facilitated and expedited by the use of any of the electronic transmission options discussed in this document, including transmission over e-mail and Web sites. Voter registration applications and absentee ballot request forms, such as the Federal Post Card Application, are frequently available on websites and transmitted to voters by fax or e-mail. As public forms, these materials do not need confidentiality protections, but could benefit from technical controls aimed at ensuring the integrity and availability of these forms. However, completed voter registration or ballot request forms can contain sensitive information, and improper protection of these forms in transit, storage and processing can put this information at risk of theft or manipulation. Failure to securely transmit these forms to election officials could impact the ability of voters to obtain ballots. This section will cover basic procedural and technical security controls aimed at protecting information related to voter registration and blank ballot request materials.

3.2 General Issues

3.2.1 Voter Registration

Once an applicant is determined to be a qualified voter in a jurisdiction, the voter registration process implicitly establishes a trusted relationship between the applicant and the jurisdiction. The voter registration process may establish a trusted authentication token that is used to authenticate future correspondence from the voter. For instance, the voter's signature on a voter registration form may be used to authenticate received absentee ballots, or updates to the voter's registration information. Systems used for UOCAVA voting may require the voter registration process to establish electronic authentication tokens, such as a password or cryptographic key.

State law may prohibit receiving voter registration forms via electronic methods. For instance, some state and local jurisdictions require that the voter registration form have an original hand-written signature, often called a "wet" signature. In these cases, faxed or scanned registration forms sent over e-mail or web sites would not be allowed.

The move to electronic or online voter registration may require changes to the process of establishing this authentication token, as allowed by state law. For example, some states and local jurisdictions now have the ability to

use signatures from Department of Motor Vehicle records to authenticate election correspondence.

Jurisdictions that are unable to accept electronically transmitted voter registration materials may still be able to accept electronically transmitted materials for updating voter registration information, or requests for blank ballots.

3.2.2 Voter Authentication

State law will determine appropriate authentication mechanisms for accepting voter registration materials, blank ballot requests, and returned marked ballots. This includes the initial authentication and identity-proofing information to verify an individual's voter registration materials and eligibility to vote, as well as any subsequent correspondence between the jurisdiction and the voter, such as updates to mailing addresses or returned marked ballots.

Most state and local jurisdictions primarily use voters' signatures to authenticate voter registration forms and returned marked ballots. In these cases, election officials use the signature from the voter's file to authenticate correspondence. The signature on file might be from the voter's initial voter registration form, or it may be a signature from other state records, such as Department of Motor Vehicle (DMV) records.

The move to electronic transmission methods may require the use of alternative authentication mechanisms, particularly in cases where voters are allowed to submit information electronically. For example, some state and local jurisdictions allow voters to register to vote, request blank ballots, or change their voter registration information online. Digitized voter signatures may not be a viable or desirable option for voter authentication for these types of systems. Local election officials should consult state law to determine what forms of electronic authentication are required or allowed in their jurisdictions.

Identification numbers, such as the social security, drivers' license, or passport number, are sometimes used in online voter registration or ballot delivery systems for voter authentication. However, these identifiers, while forms of sensitive information, have limited strengths as authenticators. Social security numbers are known by many parties other than the holder, and in some states driver's license numbers are merely an encoding of the holder's name and date of birth. Jurisdictions should carefully consider the use of these identification numbers as authenticators.

E-mail return addresses and headers cannot be used for voter authentication purposes. As noted in Section 2.2.2, this information is very easy to forge.

3.2.3 Protecting Personal Voter Information

Voter registration applications and absentee ballot requests contain personally identifiable information, such as names, addresses, and identification numbers. The Government Accountability Office defines personally identifiable information (PII) as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[24] Election authorities should consult relevant state and local laws to review relevant rules and regulations governing the use and protection of PII and voter registration information in their jurisdiction.

Voter registration information is a matter of public record, but state law may limit public distribution of some categories of information, such as identification numbers (e.g., Social Security, driver's license, and passport numbers) and, in some cases, home addresses. State law may also limit acceptable uses of information obtained from voter registration records, and force individuals requesting this information to take an oath affirming compliance with relevant laws. Jurisdictions should consider any relevant legal and procedural controls in place for protecting PII in voter registration records when determining appropriate technical and procedural controls for this information in electronic systems.

Not all PII must be protected equally. Public availability of the data is just one item to consider when determining an appropriate level of protection for PII and voter registration information. Section 3 of NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, identifies six factors that organization should consider when determining the appropriate level of protection. Organizations should consider the following:

- How easily the PII can be tied to specific individuals.
- The number of individuals whose PII is stored in the system.
- The sensitivity of the data.
- The context of how the data will be used, stored, collected, or disclosed.
- Legal obligations to protect the data.
- The location of the data, and level of authorized access to the data.

Further guidance on what constitutes PII, factors that influence PII sensitivity, and how PII should be handled from collection to destruction is provided in NIST SP 800-122 [25].

Highly-sensitive forms of PII should not be sent over the Internet without use of encryption technology. After consulting local, state and federal law, jurisdictions must determine what constitutes sensitive PII, or whether the factors provided above indicate that a given set of PII may or may not be sent over the Internet without encryption or integrity protections, erring on the side of caution when possible. However, it is relatively easy and inexpensive for jurisdictions to encrypt information in-transit to and from Web sites using TLS.

3.2.4 Preparing Registration/Ballot Request Forms

Voter registration forms that are intended to be e-mailed or posted on Web sites should be converted into a publicly-available document format. Fort example, many jurisdictions use the Portable Document Format (PDF) [21].

Notably, forms should not be merely electronic scans of paper documents. Electronically scanned documents are typically much larger than documents directly saved in an electronic document format, often contain text that is more difficult to read, and are typically not compatible with screen readers. Additional usability and accessibility issues are discussed in *Accessibility and Usability Considerations for Remote Electronic UOCAVA Voting* [23].

As noted in Section 3.2.3, forms developed by state and local jurisdictions for voter registration and ballot requests should not ask for information that is not required or desired by jurisdictions. State and county-specific forms should be designed to dissuade voters from filling in unnecessary information. When Federal forms, such as the FPCA, are used, the form should be accompanied with clear instructions for the voter identifying what information is and is not required.

Some publicly-available document formats support electronically-fillable forms, allowing voters to fill in the forms on their computers, even if they intend to print the document prior to return. Many formats have extensions that support scripting languages that can be used to help voters avoid mistakes when filling out forms. For instance, Javascript could be used in the PDF format to warn voters if they miss required questions. However, these extensions can cause compatibility problems, and such documents should be tested in widely-used document viewers and introduce a variety of potential security vulnerabilities. In particular, jurisdictions using these extensions should ensure that the forms work even in document viewing

applications that do not support those extensions, or have these features disabled (e.g., Javascript may be disabled in many PDF readers for security reasons).

Some publicly-available document formats, such as PDF, support digital signatures. Jurisdictions may consider digitally signing voter registration or ballot request forms prior to e-mailing or posting them in order to give voters additional assurance that they received the correct, unaltered forms.

In order to sign documents, jurisdictions will need to obtain software packages capable of signing documents as well as a digital certificate from a certificate authority that is trusted in widely used document viewers. Usually a single certificate is all that would be needed. There are several commercial certificate authorities which sell certificates that can be used to sign documents, although these are less common than other types of certificates. State and local jurisdictions may also be able to use a certificate authority operated by the state, particularly if the state's certificate authority is affiliated with the federal government's certificate authority.

The benefits of signing documents should be weighed against the costs of obtaining the software and digital certificates necessary to support document signing, as well as the number of voters expected to be able to verify the digital signatures on signed documents. Most voters will not notice the difference between a signed document and an unsigned document, and in many cases signed documents are only verifiable using a document viewer from a particular software vendor. Users with other document viewers may still be able to open and view the document, but would not be able to verify the authenticity of the document. For those reasons, election officials may want to consult with other agencies in their jurisdiction to determine if another agency already has the requisite software and digital certificate to sign documents. If no other agency has these items, jurisdictions must decide whether or not the security benefit justifies the expense of the software and digital certificate.

3.3 Fax

Jurisdictions should follow their standard procedures for ensuring voter registration and ballot request forms are correct before faxing them to voters. Election workers should take steps to ensure that disruptions or errors in the fax process are prevented or detected and resolved. If a jurisdiction accepts voter registration materials by fax, the fax machine should be kept in secure physical location to prevent the theft of sensitive personal information that may be on received voter registration forms.

Most fax machines keep a log of faxes that are sent and received. This includes successful and unsuccessful transmission. These logs may be useful auditing records to keep, but also could also allow voters' telephone or fax numbers to be disclosed to unauthorized parties if fax machines are not kept in secure locations, since these logs are usually available to anyone with physical access to the machines.

Some fax machines keep digital copies of sent or received faxes, often unbeknownst to users. These copies could put personal information on received voter registration forms at risk of disclosure to unauthorized individuals. Election workers should consult the documentation for the fax machines to determine if their fax machines store copies of received faxes. The documentation may also provide users with the steps needed to periodically erase this information.

3.4 Electronic Mail

3.4.1 Delivery

Voter registration and ballot request forms should be prepared as described in Section 3.2.4 to ensure the electronic files have the best possible chance of being successfully delivered to voters. Jurisdictions should follow their standard procedures for ensuring these forms are correct before e-mailing them to voters.

Jurisdictions should beware of spam filters which may inadvertently mark their messages as spam and not display it to users. It is difficult to ensure that e-mails sent by jurisdictions will not be marked as spam. As previously noted, use of DomainKeys Identified Mail [10] on the jurisdiction's e-mail server may reduce the changes of outgoing e-mail being marked as spam. Jurisdictions may also consult the Message Anti-Abuse Working Group's *Sender Best Communications Practices* for additional technical measures [13].

E-mails should be addressed to voters individually, rather than sending a single e-mail to a group of voters. There are utilities and e-mail clients that can send the same message individually to a list of e-mail addresses. The "Reply-to" and "From" fields of the outgoing e-mail should be set to an e-mail account monitored by election officials. Election officials should closely monitor this e-mail account for any error messages that indicate a message was not properly received by the voter. Some types of e-mail error messages were described in Section 2.2.2.2. Election officials should read the error message to determine the nature of the problem and remedy it if possible, as it may be a sign of a technical malfunction. If the problem

cannot be remedied, election officials should apply the same procedures used by the jurisdiction when it has evidence that a mailed form did not reach its destination.

3.4.2 Reception of Forms

Completed voter registration forms collected over e-mail are expected to be received and processed by election officials manually. As with e-mail delivery, workstations used to collect voter registration forms over e-mail should be configured according to accepted computer security best practices, such as using an encrypted connection to the e-mail server for both incoming and outgoing messages. NISTIR 7682 provides an overview of the security best practices for procuring, configuring and administering these systems.

As election officials will be opening e-mails from voters, and potentially attackers, it is important to properly secure the workstation against possible attacks. While these protections are appropriate for any election workstation, it is critical to ensure that the workstation is running up-to-date antimalware software at all times, and ensure that it is configured to scan incoming e-mail messages. Applications used to open e-mails, or to open e-mail attachments, should also be hardened. For example,

- Microsoft Office, and other document viewers, can be configured so that macros are disabled.
- PDF viewers may have configurable security protection mechanisms, and active content (e.g., javascript) can be disabled.

As discussed in Section 2.2.2.4, some voters may send e-mail messages signed using S/MIME. E-mail clients should be configured by IT staff to correctly process these messages. Most commercially-available e-mail clients include S/MIME functionality by default.

Election officials should develop appropriate procedures for handling and processing e-mails containing voter registration information. E-mail servers and clients are generally not suitable locations for storing sensitive information for extended periods of time. Election officials should process these e-mails as soon as possible, using their standard procedures for processing received voter registration forms. As part of this process, election officials may wish to save an electronic or physical copy of the received e-mail, including full e-mail headers and attachments, to the voter registration database or other voter management system. After processing, the e-mail should be removed from both the e-mail server and the e-mail client to prevent unauthorized access to any sensitive information on these forms.

Simply deleting e-mails from servers and clients does not typically remove all traces of those e-mails on those systems. Due to the way that e-mails are typically stored on servers and clients, file-level sanitization software cannot be relied upon to securely erase this data. These computer systems should be treated as any other containing potentially sensitive data, and sanitizing storage media prior to decommissioning or repurposing. Section 4.2.4 of NISTIR 7682 provides best practices for decommissioning systems.

3.5 Web-based Distribution and Reception of Forms

3.5.1 Delivery

Voter registration and ballot request forms should be prepared as described in Section 3.2.4. Election officials should follow their standard procedures for ensuring these forms are correct prior to loading them on the server. Access control mechanisms should be used on the server to protect the forms from unauthorized access or modification. The server operating system and Web server application should be configured and deployed according to widely accepted computer security best practices.

Blank voter registration and ballot request forms, such as the FPCA, are public forms that do not require confidentiality protections. However, use of TLS or SSL can also protect the integrity of these forms as they are transmitted to voters.

3.5.2 Reception

Jurisdictions may receive completed voter registration forms over Web sites that allow users to upload the completed form to the jurisdiction's Web server. This approach offers greater security than e-mail transmission of voter registration and ballot request forms, notably encryption and integrity protection in-transit using SSL/TLS. However, these protections can also be used for Web-based forms, as described below in Section 3.6. In most cases, use of online forms will be preferable to uploading completed forms to a Web site, except in cases where a jurisdiction must obtain digitized voter signatures to authenticate received forms.

The Web server's operating system and election application should be configured and deployed according to widely accepted computer security best practices. For example files should be uploaded using the HTTPS protocol using SSL 3.0 or TLS 1.0 or higher and NIST-approved cipher suites. Uploaded files should not be stored directly on the Web server; rather, they should be received by the Web server, and stored on a system that is not directly accessible from the Internet. NISTIR 7682 provides an overview of the security best practices for procuring, configuring and administering these systems.

Jurisdictions should take steps to protect the availability of the online system. This includes ensuring the system has adequate capacity for the expected load, and contingency plans in the event of a service disruption. Jurisdictions may wish to implement technical controls in the repository to protect against attackers overwhelming the system. This could include the use of CAPTCHAs[1] to guard against automated attacks, or limiting the size of uploaded files.

Individuals could attempt to upload carefully crafted files as part of an attack. These files could contain malicious code or hidden instructions that could allow an attacker to take control of the system. Jurisdictions should implement security controls to reduce the likelihood that such files could successfully attack the system. For instance,

- The system could restrict file types users may upload to those commonly used for scanned documents. For example, a server could be configured to only accept commonly-used document or image file formats. This limits the ability of potential attackers to upload malicious code or other unwanted files, and makes it less likely that voters will upload the wrong file.
- The file type verification mechanism could read the contents of the file and verify the file format against the approved list of file formats, rather than only checking the file extension.
- The system could use access control mechanisms to ensure uploaded files are not readable, or executable, by the Web server. This will make it more difficult for malicious individuals to improperly access files uploaded to the server.
- Uploaded files could be sanitized and scanned for malicious code prior to making them readable by any other processes or users. All forms of user-input should be checked, including the file contents and the full file name. This important step attempts to protect workstations accessing these files from attacks involving malicious code.

Election officials should process uploaded forms as soon as possible, using their standard procedures for processing received voter registration forms. As part of this process, election officials may wish to save an electronic or physical copy of the received form. After processing, the uploaded form should be removed from the online system to protect against authorized access.

[1] CAPTCHA is an acronym for Completely Automated Public Turing test to tell Computers and Humans Apart.

3.6 Online Voter Registration Systems

Jurisdictions may deploy Web sites that allow voters to view or submit voter registration and ballot request materials directly within the Web page. These systems typically work by allowing voters to submit information electronically to local election officials. Election officials process the submitted voter registration materials similarly to how they process voter registration forms received through the mail. The voter's record in the voter registration database is updated through this process conducted by the election official. In general, online voter registration systems should not automatically update voter registration information without direct involvement from an authorized election official.

Voters using the web site to register to vote or update their voter registration information will need to be authenticated. State law will determine appropriate authentication mechanisms. Depending on state law and the implementation of the system, voters may be authenticated prior to allowing them to submit information, or the system may allow anyone to submit information, with authentication performed by election officials during processing.

In most cases, it will be desirable to authenticate voters prior to allowing them to submit information. In these cases, the systems may authenticate voters using information stored in the voter registration database, as permitted under state law. For example, the system could ask the voter to provide some difficult-to-guess information that can be verified against existing voter registration information. Because this is a relatively weak form of authentication, measures should be taken to protect against malicious users submitting fraudulent information by correctly guessing the information used for authentication purposes.

For instance, multiple consecutive invalid authentication attempts should result in the voter's account being temporarily locked, preventing further access attempts, for a predefined period of time (e.g., 24 hours) or until the case can be reviewed by an election official. The number of allowable invalid authentication attempts should be dependent on the difficulty of guessing the required authentication information. If information is relatively easy to guess, such as the voter's registered zip code or date of birth, is used for authentication purposes, then a lower number of invalid authentication attempts could be used. Information that is more difficult to guess, such as an identification number that was generated randomly by the issuing authority, may allow a higher number of invalid authentication attempts to be used.

If voters are not authenticated prior to allowing them to submit information to the online voter registration system, the system should use other mechanisms to attempt to prevent automated attacks whereby an attacker submits a large number of invalid registration changes or ballot requests. An example from e-commerce sites is the use of a CAPTCHA to block automated attacks. CAPTCHAs are little puzzles that users are asked to solve, often involving reading distorted text, to prove that a human is accessing a Web application. CAPTCHAs are often used to try to block attacks where automated computer programs access a Web site and attempt to submit or collect information.

Voters should be authenticated prior to showing them any sensitive voter information. In general, highly sensitive data, such as driver license numbers, passport numbers, social security numbers, and other identification numbers, should not be presented to voters. Non-sensitive information, such as publicly-disclosable information from voter rolls, might be viewable with limited or no authentication performed. In these cases, jurisdictions should consider implementing controls to prevent an individual from collecting large amounts of information in an automated fashion, such as using CAPTCHAs.

The Web server's operating system and the election application hosting the vote registration and ballot request form should be configured and deployed according to widely accepted computer security best practices. For example, the Web site should be hosted using the HTTPS protocol using SSL 3.0 or TLS 1.0 or higher and NIST-approved cipher suites. Information submitted using the form should not be stored directly on the Web server; rather, it should be received by the Web server, and stored on a system that is not directly accessible from the Internet. NISTIR 7682 provides an overview of the security best practices for procuring, configuring and administering these systems.

Making voter registration materials available online may create some privacy concerns. Jurisdictions should carefully consider the advantages and disadvantages of deploying such systems. A report issued by the National Research Council, *Improving State Voter Registration Databases* [27], discusses some of the policy and security issues in Appendix D that can be considered prior to deploying online voter registration systems.

4 Delivery of Blank Ballots

4.1 Overview

As noted in NISTIR 7551, blank ballot distribution to overseas and military voters can be reliably and securely expedited by using electronic transmission methods, including electronic mail and Web sites [1]. Several states and jurisdictions deliver ballots electronically to overseas and military voters, usually by sending these ballots as e-mail attachments. Security best practices for e-mail transmission of blank ballots are provided in Section 4.4. However, e-mail offers limited confidentiality and integrity protection in-transit, as the required infrastructure to support e-mail encryption and digital signing technologies are not widely deployed or used by the general population. Web-based methods can provide greater confidentially and integrity protections by using SSL or TLS. Web sites could be used to allow voters to download ballot documents that can be printed and marked by hand, or they provide voters with a Web-based application that can allow voters to make their ballot selections on a computer, and print a marked ballot containing their selections. Best practices for these methods are discussed in Sections 4.5 and 4.6, respectively.

4.2 General Issues

4.2.1 Voter Identification and Authentication

State law will determine if jurisdictions must authenticate voters prior to sending them blank ballots, or if jurisdictions need to only authenticate returned marked ballots. It is important to distinguish voter authentication from voter identification. Web-based ballot distribution systems need to request sufficient information from a voter to identify the appropriate ballot style. If the information requested is not secret, and is primarily intended to identify the correct ballot style, rather than to restrict access to electronic ballots, it should not be considered an authentication mechanism.

However, for Web-based ballot distribution systems, state and local jurisdictions may still decide to employ systems to authenticate voters before serving them ballots, as allowed by state law. For example, a UOCAVA voting system might distribute blank ballots with return identification information on the voter affidavit that is used to assist election officials when processing return ballots. If this information is used to establish trust that a given ballot was completed and returned by the claimed voter, the system will need to authenticate voters electronically prior to giving them ballots and voter affidavits.

In most cases, any mechanism used to remotely authenticate voters will serve as a secondary method to authenticate returned ballots, with voter signatures generally providing the primary mechanism to authenticate returned ballots. As such, the strength of the remote authentication method can be relatively weak as long as jurisdictions are confident in their ability to verify voter signatures.

4.2.2 Ballot Accounting

As part of the ballot accounting process, many jurisdictions keep track of the total number of ballots printed to detect fraud and to audit the election process. Once ballots leave the control of a polling place environment, however, ballots can be copied, limiting the effectiveness of these checks. Printing ballots on special ballot stock provides some level of protection against copying mailed ballots, but electronically transmitted ballots are easy to copy and transmit to third parties.

Jurisdictions that are particularly concerned about unauthorized copying of electronic ballots may put cryptographically integrity-protected identifiers on each transmitted ballot that would uniquely identify a given ballot. For example, a ballot serial number could be digitally-signed or protected using a cryptographic message authentication code. While these ballots could be copied, a third party could not create a new ballot with a different identifier, as the third party could not create a valid digital signature on that identifier. However, placing unique identifiers on ballots introduces potential problems related to ballot secrecy. Jurisdictions should consult relevant state law to determine if such protections are appropriate or allowable.

A possible alternative to placing unique identifiers on each ballot is to cryptographically integrity-protect return identification information that must accompany ballots when they are returned, but are separated from the ballots before tallying. This method provides a similar level of protection against unauthorized individuals returning copied electronic ballots.

However, jurisdictions may still find it desirable to place identifiers on ballots in order to track ballots from distribution to tallying. Such identifiers could assist election officials during the ballot reconciliation process. The advantages and disadvantages to using these types of identifiers are discussed in Section 4.2.4, *Ballot Tracking.*

4.2.3 Return Identification

In order to correctly process completed ballots upon return to a voter's local election office, completed ballots are accompanied with return identification information that identifies (e.g., voter name, voter identification number) and authenticates (e.g., voter signature) the voter. The information identifying the voter may be written by the voters themselves, or it can be pre-generated on the materials provided to voters. In the case of postal mail voting, this information is usually printed on the ballot return envelopes that are delivered to voters with blank ballots. In the case of electronic distribution of ballots this information would likely be printed on sheets of paper that would accompany a completed ballot.

Computer-generated return identification information, whether created by election officials prior to transmission of blank ballots, or by software on voters' machines (e.g., java or javascript running in a browser), can be machine-readable, in the form of barcodes or text printed in a font compatible with optical character recognition. Any machine-readable return identification information should also be available in human-readable form as well, except for information intended to protect the integrity of the machine-readable encoding (e.g., digital signatures, checksums, message authentication codes, or error correcting codes).

As noted in Section 4.2.1, return identification information is usually used as a secondary voter authentication mechanism, with voter signatures serving as the primary authentication mechanism. In these cases, voters should have to authenticate to a system before receiving the return identification information, such as by authenticating to their private e-mail accounts, or authenticating to the election jurisdiction's online ballot delivery system. Return identification information should be presented in a machine-readable format, and cryptographically integrity-protected using a secret key controlled by the election jurisdiction (e.g., a digital signature or cryptographic message authentication code).

4.2.4 Ballot Tracking

When state law or procedure mandates the use of ballot identifiers, these identifiers should be implemented in a manner that prevents linking the voter with his or her ballot choices. Systems storing ballot identifiers should protect this information from unauthorized disclosure through cryptographic and other technical means. For instance, ballot identifiers could be automatically generated by the system and stored in an encrypted format. Depending on legal or procedural requirements, the system should either not provide the capability to link a voter to a ballot, or the system should implement technical protections designed to protect this information from

unauthorized disclosure. There are a variety of cryptographic mechanisms that could be used to implement such features. If tracking information is printed on ballots, jurisdictions should consider printing this information in a form that is difficult to transcribe by hand, such as a barcode, as opposed to numbers or text.

As an alternative, tracking information can be written on ballot return envelopes or voter affidavits. Tracking information on these items do not pose ballot secrecy concerns, as they are detached from returned marked ballots before tallying.

In addition, marked ballots may be given tracking information during processing. For example, ballot privacy envelopes could be numbered after separation from the return identification information that identifies the voter. In this instance, care should be taken procedurally and technically so that the numbering of the privacy sleeves cannot be used in combination with other available information to link voters to ballots.

In most cases, jurisdictions receiving paper ballots that were printed by the voter will have to copy the voter's selections on the received ballot on to official ballot stock. In these cases, tracking information should be written to both the original ballot received from the voter, and the transcribed ballot on official ballot stock that links the two ballots. This linkage does not impact ballot secrecy, as the identity of the voter has already been separated from the completed ballot.

4.2.5 Ballot Preparation

The EAC's Election Management Guidelines [28] and the Ballot Preparation/Print and Pre-Election testing Quick Start Guide [30] provide some best practices that may help jurisdictions identify procedures for preparing ballots prior to an election.

Blank ballots that are intended to be e-mailed or posted on Web sites should be converted directly into a publically-available document format. For example, many jurisdictions use the Portable Document Format (PDF) [21]. Notably, due to file size considerations, ballots should not be merely scans of printed paper ballots.

Some publically-available document formats support electrically-fillable forms, which cold be used to allow voters to make their choices on their computers, even though they are expected to print the ballot and sign accompanying forms. As noted in Section 3.2.4, many formats have extensions that support scripting languages that can be used to help voters avoid mistakes when filling out forms. For instance, Javascript can be used

in the PDF format to warn voters if they overvote. However, these extensions can cause compatibility problems and introduce a variety of potential security vulnerabilities. In particular, jurisdictions that decide to use these extensions should ensure the forms work even in document viewing applications that do not support those extensions, or have them disabled (e.g., Javascript may be disabled in many PDF readers for security reasons).

Some publically-available document formats, such as PDF, support digital signatures. Jurisdictions may consider digitally signing blank ballots prior to e-mailing or posting them in order to give voters additional assurance that they received the correct, unaltered forms. For these signatures to be effective, jurisdictions must obtain a digital certificate from a certificate authority that is trusted in widely-used document viewers. There are several commercial certificate authorities which sell certificates that can be used to sign documents, although these are less common than other types of certificates. State and local jurisdictions may also be able to use a certificate authority operated by the state, particularly if the state's certificate authority is affiliated with the federal government's certificate authority.

The benefits of signing documents should be weighed against the costs of obtaining the software and digital certificates necessary to support document signing. Most voters will not notice the difference between a signed document and an unsigned document, limiting the security benefit. For that reason, election officials may want to consult with other agencies in their jurisdiction to determine if another agency already has the requisite software and digital certificate to sign documents.

If an online ballot marking tool is being provided to voters (discussed further in Section 4.6), constructed ballot definition files should be produced and tested using the same procedures that jurisdictions use to produce and test ballot definition files for polling place systems. For instance, jurisdictions should implement technical and procedural controls to ensure the accuracy and integrity of the information on in the files. After loading the ballot definition files in the ballot marking tool system, election officials should test the system to ensure the proper candidate and ballot question information will be displayed to voters.

4.3 Fax Transmission

Jurisdictions should follow their standard procedures for ensuring ballots are correct before faxing them to voters. Election workers faxing documents should remain near the fax machine as the ballot is sent to ensure no one disrupts the sending process or to deal with any errors that might arise.

Most fax machines keep a log of faxes that are sent and received. This includes successful and unsuccessful transmission. These logs may be useful auditing records to keep, but also could also allow voters' telephone numbers to be disclosed to unauthorized parties if fax machines are not kept in secure locations, since these logs are usually available to anyone with physical access to the machines.

As previously noted, some fax machines keep digital copies of sent or received faxes. While blank ballots and associated election materials (e.g., voter affidavits) typically will not include any sensitive information, some jurisdictions may wish to clear this information periodically.

4.4 Electronic Mail

Blank electronic ballots should be prepared as described in Section 4.2.5 to ensure the files have the best possible chance of being successfully delivered to voters, and contain the accurate candidate and ballot question information. Jurisdictions should follow their standard procedures for ensuring these blank ballots are correct before e-mailing them to voters.

Jurisdictions should beware of spam filters which may inadvertently mark their messages as spam and not display it to users. It is difficult to ensure that e-mails sent by jurisdictions will not be marked as spam. As previously noted, use of DomainKeys Identified Mail [10] on the jurisdiction's e-mail server may reduce the changes of outgoing e-mail being marked as spam. Jurisdictions may also consult the Message Anti-Abuse Working Group's *Sender Best Communications Practices* for additional technical measures [13].

E-mails should be addressed to voters individually, rather than sending a single e-mail to a group of voters. The "Reply-to" and "From" fields of the outgoing e-mail should be set to an e-mail account monitored by election officials. Election officials should closely monitor this e-mail account for any error messages that indicate a message was not properly received by the voter. Some types of e-mail error messages were described in Section 2.2.2.2. Election officials should read the error message to determine the nature of the problem and remedy it if possible, as it may be a sign of a technical malfunction. If the problem cannot be remedied, election officials should apply the same procedures used by the jurisdiction when it has evidence that a mailed ballot did not reach its destination.

4.5 Web-Based File Repositories

Jurisdictions may post blank ballots on Web sites. This method offers security benefits over electronic mail, as there are widely deployed and used technologies (e.g., TLS) that can be used to protect the confidentiality and integrity of information in-transit.

Blank electronic ballots should be prepared as described in Section 4.2.5 to ensure the files contain the accurate candidate and ballot question information. Election officials should follow their standard procedures for ensuring these ballots are correct prior to loading them on the server. Access control mechanisms should be used on the server to protect the forms from unauthorized access or modification. The server operating system and Web server application should be configured and deployed according to widely accepted computer security best practices. For example, ballots should be delivered to voters using the HTTPS protocol using SSL 3.0 or TLS 1.0 or higher and NIST-approved cipher suites. NISTIR 7682 provides an overview of the security best practices for procuring, configuring and administering these systems.

Voters will need to identify themselves to the system in order to allow the system to provide the correct ballot to each voter. As discussed in Section 4.2.1, voter authentication may or may not be necessary, depending on state law and local procedures. However, some form of authentication is required in circumstances where voters will receive return identification information that will be used as a secondary voter authentication mechanism when processing return ballots.

4.6 Online Ballot Markers

Section 2.2.3.3 discussed various technologies for implementing Web-based applications for marking a ballot. Options such as Flash and Java require third-party plug-ins that, while widely deployed, are not present or enabled on all personal computers. DHTML, Javascript, and Ajax Web applications are supported in nearly all modern Web browsers, although these technologies are sometimes disabled for security reasons.

The Web server's operating system and election application should be configured and deployed according to widely accepted computer security best practices. Voters should interact with Web applications over an HTTPS connection using SSL 3.0 or TLS 1.0 or higher and NIST-approved cipher suites. The ballot marking tool is also a potential source for vulnerabilities in the system. The tool should be developed in accordance with widely

accepted best practices for Web application development, being careful to block common Web application vulnerabilities. NISTIR 7682 provides an overview of the security best practices for procuring, configuring and administering these systems.

The system will need access to voter lists that tell the system what ballot style should be delivered to each voter. In many cases, this information will be exported from the state or local jurisdiction's voter registration database and imported into the online ballot marking system. Maintaining the accuracy and availability of this data is critical, and jurisdictions should protect this information using similar technical and procedural controls to how they protect pollbooks and the voter registration database. If these voter lists contain sensitive information, possibly to facilitate voter identification or authentication, then it will also be important to protect the confidentiality of this information.

The system will need access to ballot definition files. These files should be produced and tested using the same procedures that jurisdictions use to produce and test ballot definition files for polling place systems. For instance, jurisdictions should implement technical and procedural controls to ensure the accuracy and integrity of the information on in the files. After loading the ballot definition files in the ballot marking tool system, election officials should test the system to ensure the proper candidate and ballot question information will be displayed to voters.

As with Web-based file repositories, voters must identify themselves to the system in order to allow the system to provide the correct ballot to each voter. As discussed in Section 4.2.1, voter authentication is not necessarily required, particularly if voters are not restricted from downloading their ballots multiple times. However, voters will need to be authenticated in circumstances where voters receive return identification information that will be used as an authentication mechanism when processing return ballots.

To protect ballot secrecy, the printable ballot should be constructed using software that runs solely on voters' computers. At no point should the ballot marking application transmit voter selections to the Web-server. However, Web applications may send information about the voter to the Web server, in order to supply proper candidate and ballot question information, and potentially to support return identification and ballot tracking mechanisms.

Printed ballots may contain machine-readable encodings of information on the ballot, such as ballot style, ballot ID, ballot questions and selections. Machine-readable encodings could take the form of barcodes, or text printed in a font compatible with optical character recognition. Any machine-

readable ballot information should also be available in human-readable form as well, except for information intended to protect the integrity of the machine-readable encoding (e.g., digital signatures, checksums, message authentication codes, or error correcting codes).

5 Other Resources

EAC Election Management Resources

- Election Assistance Commission. *Election Management Guidelines*. http://www.eac.gov/election_management_resources/election_management_guidelines.aspx
- Election Assistance Commission. *Best Practices for Facilitating Voting by U.S. Citizens Covered by the Uniformed and Overseas Citizens Absentee Voting Act*. September 2004. http://www.eac.gov/research/uocava_studies.aspx
- Election Assistance Commission. *Quick Start Guides*. http://www.eac.gov/election_management_resources/quick_start_guides.aspx

Additional EAC election management resources can be found on the EAC Web site at http://www.eac.gov.

NIST Computer Security Resources

Guidelines

- Draft NIST IR 7682, *Information System Security Best Practices for UOCAVA Supporting Systems*, April 2010.
- NIST Special Publication 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. February 2010.
- NIST SP 800-60 Rev 1. *Guide for Mapping Types of Information and Information Systems to Security Categories* (2 Volumes). August 2008.
- NIST SP 800-53 Rev. 3. *Recommended Security Controls for Federal Information Systems and Organizations*. May 2010.
- FIPS 199. *Standards for Security Categorization of Federal Information and Information Systems*. February 2004.
- NIST Special Publication 800-44, *Guidelines on Securing Public Web Servers, Version 2,* September 2007. http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf
- NIST Special Publication 800-123, *Guide to General Server Security*, July 2008. http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

- Draft NIST Special Publication 800-63 Rev. 1, Electronic *Authentication Guideline*, December 2008. http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1_Dec2008.pdf
- NIST Special Publication 800-45, *Guidelines on Electronic Mail Security, Version 2, February 2007*. http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf
- NIST Special Publication 800-122*, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010. http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf

Other NIST Resources

- National Checklist Program (NCP). http://checklists.nist.gov/
- National Vulnerability Database (NVD).
- Security Content Automation Protocol (SCAP) Specifications. http://scap.nist.gov/

A wide range of additional computer security resources are available on the NIST Computer Security Resource Center Webpage at .

Federal Voting Assistance Program (FVAP) Resources

- FVAP. *United States Postal Service Mail Guidelines*. http://fvap.gov/leo/usps-mail-guidelines.html
- FVAP. *Fax & E-mail Guidelines.*
- FVAP. *Guidelines for the Help America Vote Act.* http://fvap.gov/leo/hava-guidelines.html

The Federal Voting Assistance Program has set up a portal for election officials to obtain UOCAVA voting-related information and resources at http://fvap.gov/leo/index.html.

6 References

[1] National Institute of Standards and Technology Interagency Report 7551, *A Threat Analysis on UOCAVA Voting Systems*, December 2008. http://vote.nist.gov

[2] Draft National Institute of Standards and Technology Interagency Report 7682, *Information System Security Best Practices for UOCAVA Supporting Systems*, April 2011. http://vote.nist.gov

[3] EAC. (2010). UOCAVA Pilot Program Testing Requirements, March 24, 2010. Accessed May 10, 2010 at http://www.eac.gov/program-areas/voting-systems/docs/requirements-03-24-10-uocava-pilot-program

[4] FVAP. (2010). Federal Post Card Application. Accessed May 10, 2010 at http://www.fvap.gov/resources/media/fpca.pdf

[5] Testimony of Bob Carey, Director of FVAP. (2010) EAC Public Meeting, Dec. 3 2009. Accessed April 5, 2010 at http://www.eac.gov/public_meeting_12032010/

[6] National Institute of Standards and Technology Interagency Report 7770. *Security Considerations for Remote Electronic UOCAVA Voting*. Whitepaper for the Technical Guidelines Development Committee. February 2011.

[7] Internet Engineering Task Force. (2010). S/MIME Mail Security. Accessed April 3, 2011 at http://www.ietf.org/wg/concluded/smime.html

[8] Callas, J., Donnerhacke, L., Finney, H. and R. Thayer, "OpenPGP Message Format", RFC 2240, November 1998.

[9] NIST SP 800-45 Version 2. Guidelines on Electronic Mail Security, February 2007

[10] Hansen, T., et. al., "DomainKeys Identified Mail (DKIM) Development, Deployment, and Operations", RFC 5863, May 2010.

[11] Sender Policy Framework (2010). Project Overview. Accessed June 18, 2010 at http://www.openspf.org/

[12] Lyon, J., and M. Wong, "Sender ID: Authenticating E-mail", RFC 4406, April 2006.

[13] Messaging Anti-Abuse Working Group. (2010). MAAWG Sender Best Commmunications Practices Version 2.0. Accessed June 18, 2010 at

[14] Dierks, T., and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[15] NIST SP 800-60 Rev 1. Guide for Mapping Types of Information and Information Systems to Security Categories (2 Volume). August 2008.

[16] NIST SP 800-53 Rev. 3. Recommended Security Controls for Federal Information Systems and Organizations. May 2010.

[17] Draft NIST SP 800-128. Guide for Security Management of Information Systems. March 2010.

[18] Draft NIST SP 800-34 Rev. 1. Contingency Planning Guide for Federal Information Systems. October 2009.

[19] FIPS 199. Standards for Security Categorization of Federal Information and Information Systems. February 2004.

[20] "Uniformed and Overseas Citizens Absentee Voting Act", P.L. 99-410

[21] ISO 32000-1:2008, Portable Document Format—Part 1: PDF 1.7.

[22] Microsoft. (2010). Microsoft Office File Format Documents. Accessed May 10, 2010 at http://msdn.microsoft.com/en-us/library/cc313105.aspx

[23] Accessibility and Usability Considerations of Remote Voting Systems. Whitepaper for the Technical Guidelines Development Committee. http://vote.nist.gov

[24] GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, May 2008.

[25] NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010.

[26] Federal Trade Commission. (2008). FTC Consumer Alert: FTC Cautions Consumers About Voter Registration Scams. Accessed May 10, 2010 at

[27] Committee on State Voter Registration Databases; National Research Council. (2010). Improving State Voter Registration Databases. Accessed June 3, 2010 at

[28] Election Assistance Commission. (2010). Election Management Best Practices. Accessed June 18, 2010 at

[29] Election Assistance Commission. (2004). Best Practices for Facilitating Voting by U.S. Citizens Covered by the Uniformed and Overseas Citizens Absentee Voting Act. Accessed June 18, 2010 at

[30] Election Assistance Commission. (2006). Quick Start Guide: Ballot Preparation/Printing and Pre-Election Testing. Accessed Jun 18, 2010 at

Appendix A: General Computer Security Best Practices

A variety of system components will play a role in transmitting election materials electronically. Some of these components will likely serve multiple functions within a jurisdiction, and most are likely to be managed by technical personnel who also maintain information technology (IT) systems which are unrelated to the transmission of election materials. Close coordination will be required between election officials and technical personnel to ensure that sufficient process and technical controls are in place for the secure deployment of such a system.

Security requirements for systems that contain election materials will differ according to local regulations and practices as well as according to the nature of the materials contained on the system. Even so, certain basic practices need to be followed to secure any important IT system.

This section outlines those general best practices and will help election officials understand the points of coordination required for a secure, functional system. Once the security objectives are identified as part of the system characterization process, a set of security controls will be established to meet these objectives. Some of the controls will be common to many or all systems within the organization, and some may be specifically deployed in support of the election system.

A.1 System Characterization

The first step in securing any system is the establishment of security objectives. In order to select appropriate security measures, election and IT personnel need to have a common understanding of the confidentiality, integrity and availability requirements for the system's data and functions. This requires a thorough description of the system's purpose, data, components and boundaries.

Election officials should work with technical staff to identify or create documentation of the purpose and scope of every system. The resulting characterization will drive planning for fulfilling the system's security objectives. For example, a system whose purpose is delivering information on application deadlines may contain only public domain information that is readily available through other channels, and therefore would not have any confidentiality requirements, might have moderate integrity requirements, and low availability requirements. A system that allows voters to view and modify their registration information might introduce moderate or high confidentiality requirements, depending on the sensitivity of the information displayed.

A.1.1 Functional Description

As a first step to characterizing the system, each function provided by the system must be defined along with who will access that function. In most cases, any technical details expressed in the functional description should be very high-level. For example, election officials may be able to load ballot configuration files on a system, or voters may be able to update their voter registration information on the system. For each function provided by the system, assess the risk posed by failure to provide it. In assessing this risk, it is important to consider legal and procedural requirements unique to the jurisdiction, as these will influence and may even explicitly define the impact of unavailability for some election-related functions.

A.1.2 Data Categorization

In order to provide the functions documented in the functional description, the system will require access to various types of data. Determine what data must be stored on or processed by the system in order to provide each function. Here also, any technical details expressed in the data characterization will be very high-level. Each type of data should be described according to confidentiality, integrity, and availability requirements. For each, establish the impact of improper disclosure, modification or destruction of that data. As with availability of system functions, each jurisdiction may have specific circumstances or legal requirements that help determine this impact. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories* [15] details preliminary characterizations for certain types of data, which may provide a useful starting point. For all other data, this document provides readers with a list of common considerations to use when determining impact levels.

As a general best practice, systems should not store or access any data beyond that which is required to provide an election function identified in the functional description if that data has any confidentiality or integrity requirements.

A.1.3 System Architecture

The description of the system architecture will contain more granular technical details than either the functional description or the data categorization. Election officials should work with IT personnel to describe the components (e.g., servers, routers, workstations) that will be used to deliver the system functions previously enumerated. It is important to understand the role of each component in delivering the system's functions along with what data will be stored in or processed by each. The system

architecture description should account for how component failures could compromise availability, confidentiality or integrity.

All physical and logical boundaries should be established in the system architecture. These should include both technical and organizational considerations. So, for example, any common resources shared across boundaries (e.g., network storage used for both election and other county data) should be identified so that sufficient technical and procedural controls can later be defined.

A.2 Identification of Common Controls

The IT system deployed to support the transmission of election materials will most likely be one of many systems managed by the jurisdiction. In this case, the organization responsible for the operation of the IT systems will have established certain common security controls that apply to all systems and hosting facilities controlled by that organization. These controls should be analyzed in conjunction with the security requirements established during the system characterization for the election system. Election officials should work with the IT management organization to understand which common security controls exist. Together, they should identify both how these common controls can be used to support the voting system security requirements and where new controls need to be deployed along with the new system.

Because system management services will most likely be shared with non-election systems, certain management policies will most likely be common across the organization. Several of these are relevant to system security and merit specific consideration in the context of a system used to process election data:

- Personnel screening is the process by which the organization determines that individuals are suitable for performing specific duties. Election officials should ensure that this process complies with any relevant regulatory requirements governing personnel with access to the types of data identified in the data characterization.
- Configuration Management is the set of policies and processes for controlling system and documentation modifications. Related controls are discussed in detail appendix A.4.
- Contingency Planning is the set of policies and processes intended to maintain and restore election operations in the event of emergencies, failures or disasters. Related controls are discussed in further detail in appendix A.5.

- Physical Access Controls are policies and procedures that govern how personnel gain physical access to systems and facilities. For some components of the system, physical access may imply access to election data which should be identified in the system architecture. Election officials should confirm that the organization's physical access controls on such components are sufficient to meet local requirements.
- User Identification and Authentication controls govern how the system determines a user's identity. The technical details of using these controls to verify identity claims are discussed in NISTIR 7682 [2] and are outside the scope of this document. Election officials should examine the process the organization uses to issue the credentials used for user identification for those users who might have access to sensitive system data and confirm that this process meets applicable regulatory requirements.
- Hardware and Software Acquisition channels are likely to be shared across the organization. Election officials should confirm that this process meets any election-specific requirements.
- Incident Response Procedures are intended to detect, respond to, and limit consequences of IT security compromises. These are discussed in greater detail in appendix A.6.

Certain technical controls are also frequently applicable on a facility-wide basis and therefore tend to be shared by many unrelated systems. These include:

- Physical/environmental aspects of the facility such as availability monitoring, backup power supplies, fire suppression, and media storage.
- Local and remote network access for jurisdiction personnel.
- Network Infrastructure Protections, such as those described in the Appendix B.

In addition to common security controls, many jurisdictions will use existing network infrastructure to service some of the functional requirements for the election system. For example, some systems existing as DNS servers, e-mail servers or Web servers will likely be used. Just as with components specific to the election system, the architecture description developed during the system characterization should identify functions provided by and data processed by or stored on the shared components. For this shared infrastructure, election officials should coordinate with those systems' managers to ensure that the system-specific controls are sufficient to meet the security objectives defined for those functions and data.

A.3 Network and Communications Protections

Even with effective security controls configured for those hosts which provide election-related functionality, certain network and communications infrastructure protections need to be in place to support the secure operation of the overall system. In many cases, the network infrastructure owned by a jurisdiction may be used to support both election and non-election functions. The system architecture description developed during the system characterization should identify security objectives for the shared components. Election officials should work with IT management to examine the protections in place on these shared components and ensure that they are adequate to provide the required availability, confidentiality and integrity guarantees for the election system.

Appendix B provides a more detailed discussion of proper network and communication protections that are appropriate for use with a voter registration, ballot request, or blank ballot delivery system.

A.4 Configuration Management

Any IT system that provides a mission-critical function for an organization should have a formal, documented set of policies and procedures for security configuration management. In many cases, the policies will not be system-specific, but will be organization-wide. Existing policies and procedures should be examined and assessed to determine whether they are adequate for meeting the security objectives of the election system or whether system-specific augmentations are required. Whether or not the policies and procedures need to be changed, election officials need to be identified as stakeholders in the configuration management process and play an active role in planning and validating configuration changes.

NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* [16], details Configuration Management controls that may be appropriate to differing levels of security objectives, and NIST SP 800-128, *Guide for Security Configuration Management of Information Systems* [17], describes how specific parts of the configuration management process support these controls.

A.4.1 Configuration Management Planning

Election officials should review the plan for managing the security configurations of systems that will be used to support the transmission of election materials. Although the IT management organization will generally own the plan, as stakeholders, election officials should review the plan at a high level to ensure that it includes:

- Well-defined roles and responsibilities for personnel involved in proposing, testing, approving and implementing configuration changes
- A description of how configuration items are selected for management control
- A process for establishing a secure baseline configuration
- A process for managing updates to the baseline configuration

In many cases, if an organization has a mature, formal configuration management plan in place, the only augmentation required will be the addition of election officials to key planning, approval and testing roles.

A.4.2 Secure Baseline Configurations

A secure baseline configuration is a documented set of specifications for a system or component that has been reviewed and agreed upon by the stakeholders of a system. The secure baseline configuration can only be updated by following the process outlined in the secure configuration management plan, and should always reflect the state of the current system.

IT organizations are likely to have secure baselines that apply to many components of a particular type (e.g. fileservers). These configurations may then need to be supplemented to meet the security requirements established during the system characterization. The system architecture description should identify each component of the system along with the functions it provides and data it stores or processes. Election officials should work with technical personnel to review each component against the standard secure baseline configuration and determine whether the security objectives are met by the baseline, or to develop a new baseline specific for the election system.

All configurable components which play a role in maintaining the security or availability of the system should have secure baseline configurations.

A.4.3 Change Control

Change control is the documented process by which configuration changes are proposed, justified, implemented, tested and reviewed. Every organization needs to have a change control process which applies to all components involved in the transmission of election materials. This should include changes made to hardware, software, operating systems and applications. Election officials need to ensure that they are involved in the testing and approval of changes that could impact the security or availability of these systems.

Jurisdiction-specific regulatory and procedural requirements may influence the level of scrutiny and approval required for system changes. Election

officials should verify that the change control process meets their jurisdiction requirements.

A.5 Contingency Planning

Contingency planning refers to the collection of plans, procedures and technical measures which will be used to ensure continued availability of system functions in the event of potentially disruptive events. This covers a broad scope of planning activities aimed at ensuring resiliency of system functionality. Election officials should work with technical staff to ensure a solid mutual understanding of system availability requirements and gain assurance that adequate contingency plans are in place.

In most cases, contingency planning activities will cover all critical systems managed by an IT organization and hosted in a particular facility. Election officials should consult with technical staff to ensure that the plans in place are commensurate with the availability requirements described in the system characterization documentation, and that these plans do not compromise the confidentiality or integrity requirements established for the data. So, for example, if local requirements state that access to voter records must be logged, officials should ensure that access to off-site backups containing voter records is similarly logged. NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems* [18], gives examples of contingency planning strategies that map to the impact levels described in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* [19].

A.5.1 Preventative Controls

Preventative controls are established in advance of an event and are aimed at preventing that event from causing a disruption to system functionality. Examples of these controls include short-term, and possibly long-term, backup power supplies, duplicate or backup communication lines, fire suppression systems and regular preventive maintenance. These preventive controls should be commensurate with system availability requirements. In most cases, the fact that a system transmits election data will not impart special requirements for preventive controls in a facility that houses other mission-critical systems.

A.5.2 Backup and Recovery Strategies

Backup and recovery strategies cover those plans and procedures used to restore system operations following a service disruption. Election officials need to understand the allowable downtime for their application and work with technical staff to develop a backup and recovery plan which can restore service without exceeding that threshold. One practice common to all backup

approaches is storage of backup data at a location distinct from the live system.

Backup and recovery strategies need to address outages caused by events from a variety of failures, from simple equipment failure to major natural disasters. Recovery strategies from major long-term failures will rarely be system-specific. For more localized disruptions, there is a substantial advantage to using standard hardware across the IT organization where possible and ensuring that enough spare equipment is available to quickly replace the system and restore the software and data on the system using the backup media. In addition to standardizing equipment and verifying the availability of spares, election officials should ensure that backup hardware is acquired for any election system-specific equipment that could cause an outage to exceed the availability requirements in the event of a failure.

A.5.3 Plan Testing

Contingency plans need to be tested according to availability requirements established when characterizing the system. The goal of testing is to ensure the availability targets are maintained. Election staff should work with IT staff to participate in the tests. This provides the opportunity to confirm that all roles and responsibilities are identified and well understood, prior to an actual disaster. The organization's contingency plan should provide for regularly scheduled testing and should define events that trigger a new test exercise (e.g. turnover of key personnel, facility change, etc.).

A.6 Incident Response

Jurisdictions should ensure that a computer security incident response plan is in place prior to system deployment. Both election officials and IT personnel will have key roles in the incident process.

The incident response plan should clearly define which systems are covered and what constitutes a security incident for each one. Any system involved in the transmission of election data should be covered by an incident response plan. There should be a process for defining an incident's severity and establishing the priority for responding to that incident. Jurisdiction officials should have input into the criteria for severity and priority.

Roles, responsibilities and authority should be clearly documented for various classes of security incidents. Individuals should be identified, and the plan should include details of on- and off-hours communications channels to be used according to incident severity and priority. The plan should also establish a process for approving discontinuation of service in the event of an ongoing incident. Both IT and election representatives will need to be

involved in this process. In most incident response plans, because the initial response will focus on halting an active incident and preserving evidence for later analysis, the initial response will primarily be handled by the technical staff charged with operating and monitoring systems. After the incident, election representatives are likely to have a more central role, as decisions will need to be made on technical or procedural changes to the system as service is restored. Election officials will need to be familiar with any local, state or federal requirements governing notification of affected individuals in the event of a data breach.

Election officials should ensure that the incident response plan addresses any specific legal issues that arise from the nature of the system. For example, some states have specific disclosure procedures that need to be followed in the event of compromise of Personally Identifiable Information.

As with contingency plans, incident response plans should be tested prior to system deployment and periodically thereafter.

A.7 Continuous Monitoring

All security controls should be assessed prior to system deployment. For critical systems, a subset of management, operational and technical security controls should be continuously monitored in several ways, all with the goal of ensuring that system security and availability objectives are met on an ongoing basis as operations continue. Many IT organizations may include continuous monitoring provisions in various plans and policies rather than consolidating these activities under one plan.

Automated network and system monitoring tools should be used and monitored to detect integrity or confidentiality breaches. These tools may monitor log files, network traffic, file changes, etc. IT organizations should have a documented process for responding to output from these tools.

Network and host configurations should be periodically inspected and assessed to ensure they are compliant with current secure baseline configurations. This should involve both automated testing using some combination Security Content Automation Protocol (SCAP)-based tools and the automated system monitoring tools for other purposes and periodic audits. In particular, election officials should ensure an individual is identified and tasked with reconciling log entries which identify security-relevant system configuration changes with configuration management records. This is intended to ensure no change is made to the system without following the required testing and approval process established in the configuration management plans. IT staff should identify which configuration settings can

be automatically monitored and which require manual action by the auditor to inspect the settings and confirm that they match the most recent configuration management records for the deployed system.

Election officials should verify that the IT department identifies an individual or a team tasked with monitoring for public reports of vulnerabilities in the components that comprise the system, as well as common components that serve to support the system. This enables the organization to respond to potential vulnerabilities even in the interval between public disclosure and vendor response.

The continuous monitoring plan should provide for periodic security testing. Some tests can be conducted using only automated tools, which is both inexpensive and beneficial to all the systems managed by the jurisdiction, not solely those used to support elections. Other security tests require specialist expertise which is both quite costly and frequently system-specific. Election officials should work with the IT organization to prioritize and schedule tests according to the impact of a potential security breach on the system.

If any of these mechanisms detects an exception, the monitoring plan should include a process for assessing whether or not the exception is also a security incident. If it meets that definition, the incident response plan should be invoked. Otherwise, there should be a flaw remediation plan in place for reporting and addressing the issue, and updating the secure baseline configuration if necessary.

The continuous monitoring process should be periodically tested, to ensure that exceptions are properly flagged and remedied by the organization.

Appendix B: Component Security Considerations

This appendix offers security considerations for specific components likely to be used in the delivery of election materials to voters, such as network infrastructure, Web servers, e-mail servers and e-mail clients. This is not intended to be a comprehensive guide to all security considerations inherent in configuring such components. Rather, it seeks to reference other materials and identify considerations that are likely to pertain to these system components when they're used to transmit election materials and to guide election officials in collaborating with technical staff to ensure that components are configured and operated in a manner consistent with the security objectives of the system.

This appendix is directed toward readers with a high-level technical understanding of the components used to deliver the business functions of the system. It should assist such a reader in interacting with the technical personnel charged with implementing and managing the system. Prior to considering the guidance in this appendix, the reader should understand the System Characterization and the resulting security objectives.

The information in this appendix is intended to supplement, not replace, the best practices in NISTIR 7682. The security practices discussed in that document are critical for all of the systems discussed here. This information is intended only to help the reader better understand the application of those practices for this purpose.

Decisions about which technical controls and protections apply to various system components are driven by the system characterization. Some of these protections will be common, applied to every system the IT organization operates. Others may be specific to components of systems used to deliver election materials. Election officials and technical staff will need to identify areas where existing controls may need to be augmented in order to comply with relevant federal, state and local regulations for protection of the information stored on or accessible via these systems.

The system characterization will have defined the components necessary to fulfill its intended functions. In general, secure deployment of these systems implies that they do exactly what's specified in the characterization and no more. This means that the systems should only store the minimum amount of data necessary to perform their function, only be connected to those other systems required by the characterization, and only be accessible by those individuals who are authorized to have access.

B.1 Network Infrastructure Protections

B.1.1 Establishing Security Boundaries

The system architecture and security objectives produced during the system characterization can then be used to identify specific network infrastructure components and their roles in protecting the system. These components (routers, switches, hubs, firewalls, etc.) can then be classified. Election officials should work with technical staff to identify the security controls which are active for these components, and confirm that these are sufficient to maintain the system's overall security objectives. This enables the establishment of boundaries to control the flow of sensitive information.

The system architecture should be analyzed with an eye toward information flow. Each information object that traverses a piece of network infrastructure should be identified along with the security requirements for that information and the security controls in place for that infrastructure. Information should only traverse network infrastructure with controls sufficient to protect it. If information needs to be sent through infrastructure without sufficient controls to protect it (for example, PII needs to be sent across an organization's general business network) additional measures, such as encryption should be identified and put into place. Threats to information and measures which address those threats are identified in detail in section 4 of NISTIR 7682. Technical protections for network infrastructure are addressed in section 5 of NISTIR 7682.

Components with differing security requirements should be connected to physically distinct networks when feasible. For example, a jurisdiction's Web server and voter registration database will generally have incompatible confidentiality requirements. Ideally, these should not be connected to the same network infrastructure. In many cases such an "air gap" will be impractical or even impossible, due to business considerations. In such cases, additional network protections such as firewalls and application proxies should be used to enforce logical separation at these boundaries.

The business and technical teams need to collaborate to devise rules for exactly what information should be allowed across these boundaries and configure the network protections accordingly. So, for example, two unrelated systems that need to be colocated for budgetary reasons but have no need to share data with each other might be placed onto separate Virtual LANs (VLANs) using a managed network switch. A public server that needs access to portions of a protected database of record might be granted limited access to that database using firewall rules and a back-end application server.

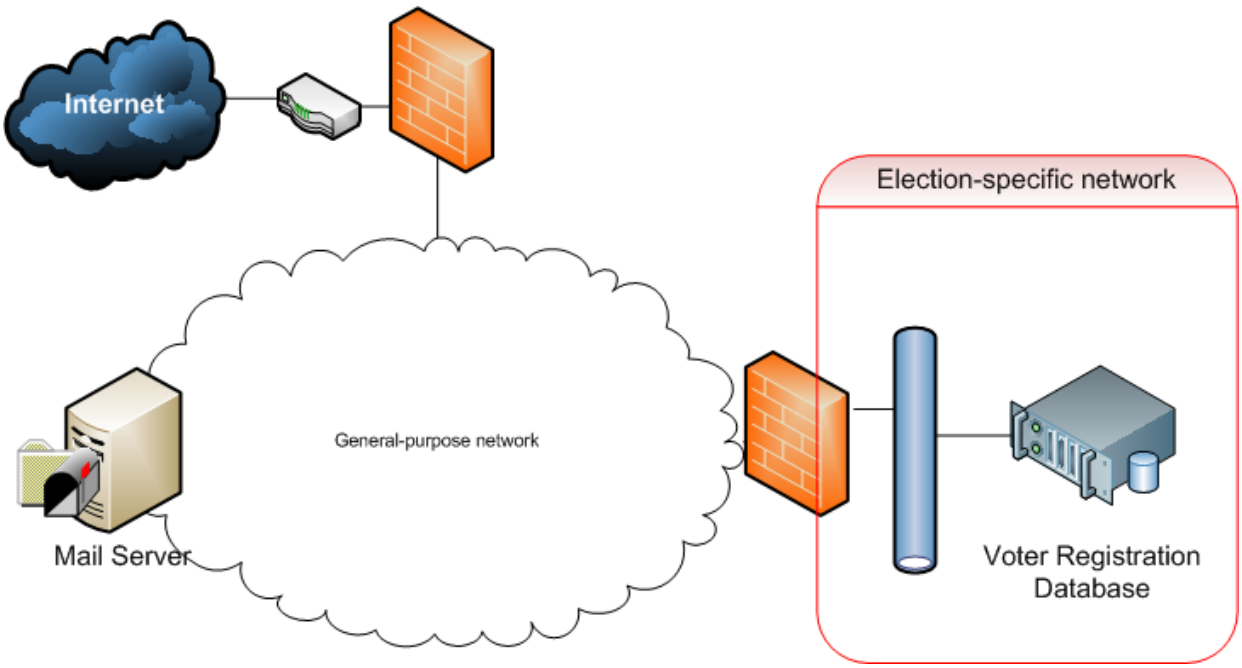

Figure 1. Segmenting election-specific infrastructure from the general-purpose network

B.1.2 Considerations for Shared Infrastructure

In most cases, some components of the system for transmitting election information will support multiple systems. The security-relevant functionality of these shared infrastructure components should be identified. The jurisdiction and the IT organization should work together to understand the security controls that are in place for the existing infrastructure, and evaluate whether these match the security requirements for the election system. For example, on most systems, a compromised or incorrectly configured DNS server, switch or router could cause e-mailed ballots to be improperly delivered, or grant an attacker the ability to alter them in transit. In such a case, security controls on these shared components should be analyzed against the security objectives of ballot delivery. Election officials should verify that the controls on security-critical shared components meet the security objectives identified for all election-specific functionality that depends on these components. So, in the example above, configuration controls need to meet the security objectives identified for e-mail availability and integrity.

Components that are likely to be shared include Web servers, e-mail servers, DNS servers, workstations, switches, firewalls and routers. Web servers and e-mail servers are discussed in more detail in later sections of this appendix as well as in NISTIR 7682 and in Special Publications 800-44

and 800-45, respectively. Workstations are discussed in the context of e-mail clients later in this appendix and more generally in NISTIR 7682. For detailed guidance on DNS security, see SP 800-81. Best practices for securing all of these infrastructure components are covered in NISTIR 7682.

Both election and IT stakeholders should ensure that common controls discussed in section 3.2 are considered for all shared infrastructure.

In cases where it is impractical to apply protections required by the sensitivity of the election system to the general-purpose infrastructure, jurisdictions should consider deploying dedicated infrastructure components in support of the election application.

B.2 E-mail Server Security

As part of the system characterization, application owners should identify the role of e-mail in transmitting election information. Specifically:

- What kind of election information will be transmitted outside the organization via e-mail?
- What election information will be received from the public via e-mail?
- What election information might be stored (generally temporarily) on an e-mail server?

B.2.1 Outbound E-mail Security

In most cases, the transmission of election information will bring no unique security requirements for outgoing e-mail. The best practices described in SP800-45 will all apply to the server that process outbound e-mail.

Because the public will consider e-mail originating from election officials to be trusted, care should be taken to verify that only authorized entities can use the organization's outgoing e-mail server to send messages, and that all outgoing messages are scanned for malware.

In order to increase the likelihood that election information will be correctly delivered via e-mail and increase the likelihood that forgeries from external parties will be flagged as such, jurisdictions should configure forgery countermeasures such as Domain Keys Identified Mail (DKIM) on servers that send election materials via e-mail. While not all voters' mail providers will recognize such protections, delivery reliability will be significantly improved when communicating with those providers that do process the additional verification data.

Organizations should ensure that all outbound e-mail connections require authentication with at least a user name and password.

Organizations should avoid transmitting information via e-mail if it's considered sensitive to disclosure according to local, state or federal regulations.

The outbound e-mail server should return any error notifications it receives to the sender of the e-mail for further analysis. Most servers will do this by default.

System owners should confirm that the maintenance process specifically ensures that malware signatures are kept current.

B.2.2 Inbound E-mail Security

In applications where election officials receive completed forms from voters, additional specific considerations may be relevant. In particular, users of the mail server will need to open attachments received from the public over the Internet in order to perform their job functions. This increases the organization's exposure to malware. Additionally, such completed forms are likely to be stored on a mail server at least until they have been processed. This storage may introduce specific requirements, depending on local, state or federal regulations.

Election officials should work with the IT organization to ensure that access to the mail server is sufficiently controlled to meet these requirements. It may make sense for officials who receive such information to have mailboxes located on a server dedicated to election information.

Whether or not such a dedicated server is necessary, these considerations suggest that an architecture which incorporates an incoming mail gateway is preferred when e-mail is used for inbound election materials.

Incoming SMTP connections from the Internet should be routed through the mail gateway. The mail gateway should scan message content and filter or quarantine suspicious messages prior to delivering them to the internal mail server. If possible, this gateway should be configured to verify that attachments are of the expected type and fall into the expected size range, in addition to checking for malware. These gateways should also be configured to verify DKIM signatures on inbound messages. Ideally, the internal mail server should scan the message content a second time, using anti-malware software from a different source than the mail gateway. This architecture serves to reduce potential exposure to malware as well as to

ensure that messages are not stored on a machine which accepts connections from an untrusted network.

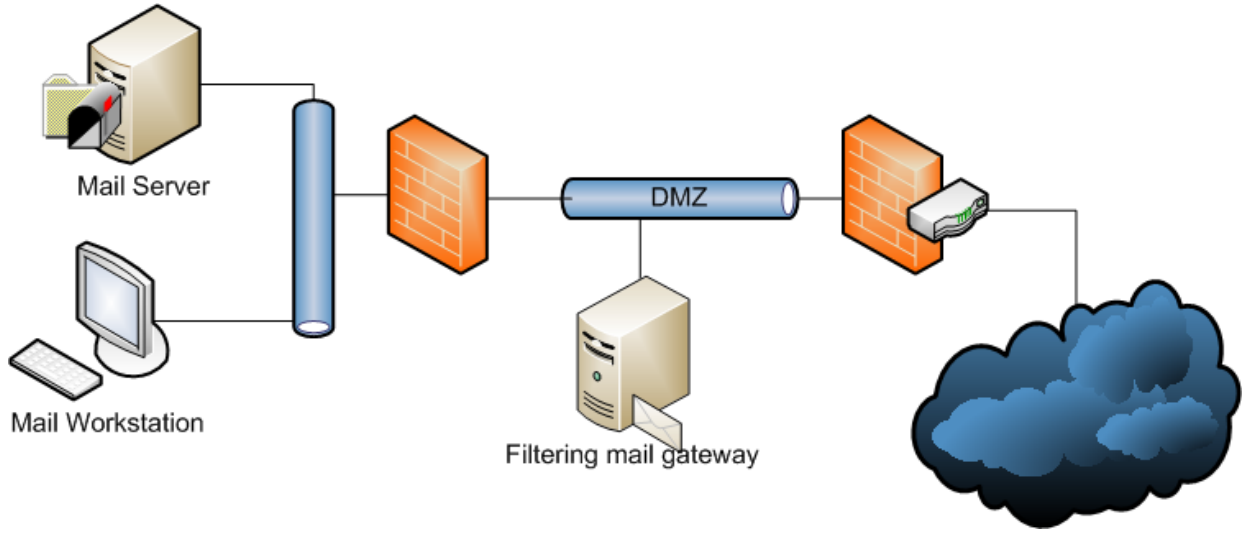

Figure 2. Common architecture for incoming e-mail

System owners should confirm that the maintenance process specifically ensures that malware signatures are kept up-to-date.

SP 800-45 details additional security best practices for e-mail servers.

B.3 E-mail Client Security

As with other components, information categorized as part of the system characterization will determine specific e-mail client security concerns. The best practices documented in NISTIR 7682 for workstation security and in SP 800-45 for e-mail client security will apply to all clients. Because e-mail clients need to interact with untrusted data, these security practices are particularly important. Care should be taken to ensure that configuration management practices are actively maintained, especially with regard to patching the OS and applications and maintaining the currency of malware signatures. Those workstations which receive completed forms as attachments, sent by the general public over the Internet, merit additional considerations.

First, it's almost inevitable that a workstation used to retrieve such e-mail will store voter information, even if only temporarily. Election officials should verify that the workstation meets any specific local, state or federal requirements for systems used to store such information.

Additionally, since such attachments may be constantly solicited (and therefore will always be expected by the workstation operator) and are received through an untrusted channel, the risk of malware infection is elevated. To counter this risk, election officials and administrators should verify that up-to-date, active malware protection is installed on the system. It is further beneficial if this protection uses signatures from a different source than the protection installed on the mail server.

As with all e-mail clients, active features like scripting support, automatic opening of e-mail and e-mail previews should be disabled. When attachments are used, system owners should pay similar attention to disable these features in any software used to process these. So, for example, in Microsoft Word, macros should be disabled. In PDF processing software, javascript, ActiveX and the execution of external applications should be disabled. Future versions of PDF-processing software continue to incorporate additional security features. As part of the continuous monitoring process, an individual should be identified to monitor new releases of any software used to process attachments and fast-track versions with new security features into production.

To further mitigate the threat of malware, it is a good practice to use a dedicated machine for monitoring a mailbox that actively solicits messages from the general public. Sensitive data and critical applications should be kept to a minimum on this workstation, and it should not be used for other important election functions.

As with all applications, proper user training is a key factor in the security of the system. In this case, the users who retrieve and read these attachments should be trained to recognize the expected type and size of attachment and seek assistance prior to opening any that fall outside these parameters.

B.4 Web Server Security

Security considerations for Web servers will vary greatly depending on the role the server plays in delivering election information. For most systems, the Web server's role in the system will be broadly characterized in one or more of the following ways:

- Delivers non-personalized election information to the public
- Delivers personalized election information to the public
- Receives information from the public.

Certain common security practices for Web servers will apply to a server in any of these roles, including:

- Minimize software installed on the Web server
- Keep server software up-to-date
- Validate all user-supplied input
- Minimize the use of active content
- Restrict the privilege of the server process
- Separate the privileged administrator interface for managing the Web application from the unprivileged user interface.

Detailed guidelines for securing public Web servers can be found in SP 800-44. Additional general guidelines for Web application security are summarized in section 5.10 of NISTIR 7682. This section will not generally aim to repeat those, but will focus on specific concerns relative to the above functions.

B.4.1 Encryption

Because members of the public will consider the jurisdiction a trustworthy source of information, all Web servers supplying the public with election information should use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to provide authentication of the server's identity even in cases where the information being served is not sensitive. Domain-verified TLS server certificates are available inexpensively or without cost, depending on the vendor, and will assure voters that information was not modified in transit.

Organizations should ensure that Web servers are configured to allow only NIST-approved SSL/TLS configurations. Specifically, only SSL 3.0 or later and TLS 1.0 or later should be used, and the cipher suites should be restricted to those identified in section 4 of NIST special publication 800-57 (part 3). Key sizes should be selected using the guidance in section 2 of the same special publication.

B.4.2 Delivery of Non-Personalized Information

In most cases, servers containing only non-personalized election information will not have additional specific technical concerns. Election officials should verify that proper procedures are followed for publishing this information so as to comply with relevant local, state and federal regulations. Information owners should work with IT staff to use technical controls that enforce these procedures.

B.4.3 Delivery of Personalized Information

Servers that deliver personalized information to the public may require access to information deemed sensitive. In this case, some verification that information is only being delivered to the correct individual will be required.

Election officials should ensure that this verification meets applicable regulations.

If the personalized information being supplied to the voter is not public, measures should be taken to prevent automated processes from attempting to brute-force this verification process. Such measures might include:

- Challenge-response tests such as CAPTCHA which require human intervention before a server will process a request
- Limitations on the number of times a specific voter's information may be queried within a pre-determined timeframe
- Requiring the user to supply a pre-shared response sent through another channel, e.g. to a voter's previously registered e-mail address, postal address or phone

If the Web server requires access to sensitive information, the repository (usually a database) containing this should be stored on a protected network which is not directly accessible from the Internet. An example of such an architecture is in found in the figure below.

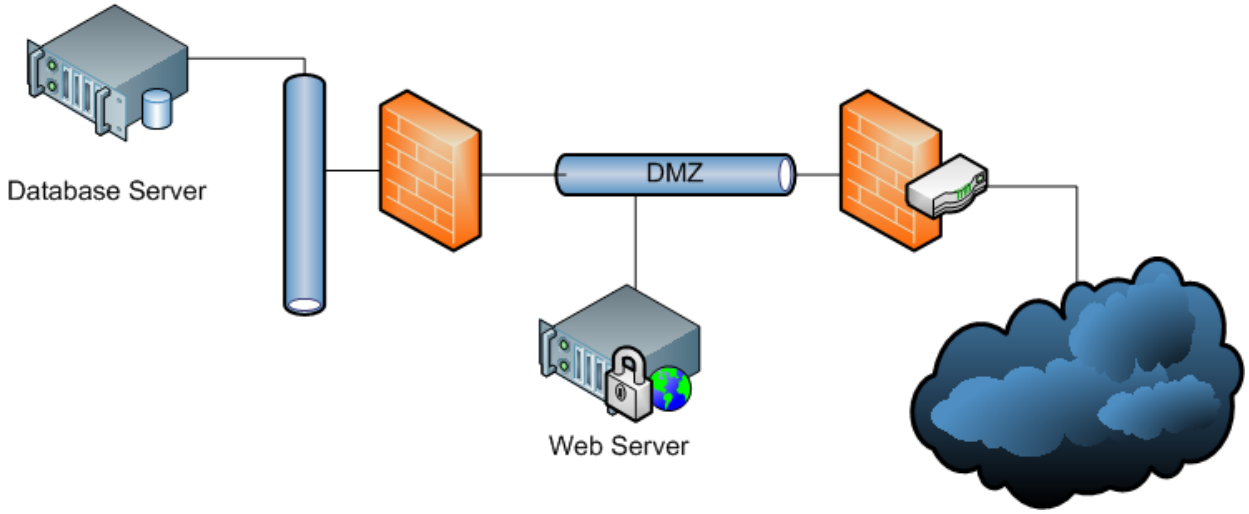

Figure 3. Common network architecture for an Internet-accessible Web server

Care should be taken to ensure that access by jurisdiction officials to any sensitive information stored in the database also complies with any relevant regulations.

B.4.4 Receipt of Information

Web servers used to receive information from the public have three unique security considerations which may vary depending on the type of information transmitted.

- Confidentiality of submitted information – If voters are submitting sensitive information to the jurisdiction using the Web server, controls must be established to prevent this data from being improperly disclosed.
- Protection of jurisdiction systems – Submitted information must be properly validated to guard against introduction of malicious content onto the jurisdiction's protected network.
- Protection of other external system users – Information submitted by one untrusted user should not be viewable by other users.

The common security practices described in SP 800-44 and NISTIR 7682 aimed at protecting confidentiality and preventing active injection attacks (SQL injection, cross-site scripting, CSRF, etc.) all serve to address these considerations.

One common case that is of particular concern interest in the context of election systems is the submission of files for processing by election officials, especially PDF forms. When a user uploads a file, it should be quarantined in a location that is not readable by the Web server. This could be a filesystem directory to which the Web server context only has write access, a "drop box" on another server, or even a form which is submitted to a dedicated upload server. As with files received via e-mail, these files should be scanned for malware prior to processing by election officials.

Ideally, as with e-mail clients, initial processing of these files would occur on a workstation dedicated to this purpose. If possible, these files should be scanned for malware both at the time they are stored and at the time they are retrieved, preferably by different scanning engines. The same precautions outlined for e-mail clients should be followed when processing received files that may contain active content.

In addition to ensuring that these files cannot be served to other Web users, officials should work with technical staff to establish controls on the file repository which limit internal access to duly authorized personnel.

Appendix C: Glossary

Access Control	The process of granting or denying specific requests for obtaining and using information and related information processing services.
Certificate	Also known as a digital certificate. A digital representation of information which at least 1. identifies the certification authority issuing it, 2. names or identifies its subscriber, 3. contains the subscriber's public key, 4. identifies its operational period, and 5. is digitally signed by the certification authority issuing it.
Certificate Revocation List (CRL)	A list of revoked public key certificates created and digitally signed by a Certification Authority.
Certification Authority (CA)	A trusted entity that issues and revokes public key certificates.
Commercial-Off-The-Shelf (COTS)	Hardware and software IT products that are ready-made and available for purchase by the general public.
Cross-Site Request Forgery (CSRF)	A type of Web exploit where an unauthorized party causes commands to be transmitted by a trusted user of a Web site without that user's knowledge.
Demilitarized Zone (DMZ)	A network created by connecting two firewalls. Systems that are externally accessible but need some protections are usually located on DMZ networks.
Denial of Service (DoS)	The prevention of authorized access to resources or the delaying of time-critical operations.
Distributed Denial of Service (DDoS)	A Denial of Service technique that uses numerous hosts to perform the attack.
Hash-based Message Authentication Code	A message authentication code that uses a cryptographic key in conjunction with a hash

(HMAC)	function.
Identification and Authentication (I&A)	The process of establishing the identity of an entity interacting with a system.
Intrusion Detection System (IDS)	Software that looks for suspicious activity and alerts administrators.
Intrusion Prevention System (IPS)	System which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.
Man-In-The-Middle (MITM)	An attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them.
Message Authentication Code	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.
Metacharacter	A character that has some special meaning to a computer program and therefore will not be interpreted properly as part of a literal string.
Out Of Band	Used to refer to information transmitted through a separate communications channel.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Token	A physical object a user possesses and controls that is used to authenticate the user's identity.
Transport Layer Security (TLS)	An authentication and encryption protocol widely implemented in browsers and Web servers. HTTP traffic transmitted using TLS is known as HTTPS.
UOCAVA	Uniformed and Overseas Citizens Absentee Voting Act.
UOCAVA Systems	Information technology systems which support various aspects of the UOCAVA voting process?

XSS	Cross-Site Scripting (XSS) is a security flaw found in some Web applications that enables unauthorized parties to cause client-side scripts to be executed by other users of the Web application.