NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Election Security Series

IMPLEMENTING TRUSTWORTHY EMAIL

Overview

Election officials rely on email to communicate with election staff, technology partners, and voters, making email a target for malicious actors attempting to influence elections. Malicious actors could forge emails claiming to be from an election official, read and modify email messages to/from election officials, and use email as a vector for other types of computer attacks. This guide provides an overview of how implementing **trustworthy email** can help election officials have confidence in the email they send and receive.

WHAT IS TRUSTWORTHY EMAIL?

Email was not designed with security in mind and is inherently vulnerable to forgery, interception, and manipulation. Some sensitive information should never be sent through email. However, characteristics of trustworthy email should include:

- **Authentication:** Validation of the identity of servers that send or receive email.
- **Encryption:** Protection of emails in transit between email servers and clients.
- **Scanning and Monitoring:** Detection and blocking of emails with malicious or inappropriate content.

HOW TO IMPLEMENT TRUSTWORTHY EMAIL

Ensuring trustworthy email requires technical expertise to properly configure various email system security technologies and related applications. Local election offices may operate their own email systems, rely on state or county systems, or contract out to third-party providers for email services. Regardless of who is running the email systems, officials should work with their information technology (IT) staffs, email service providers, and other technical and security experts to verify that the email systems they use are configured to support trustworthy email.

Below are some considerations for election officials when implementing trustworthy email:

- **Configure email security technologies—**Implement email authentication technologies (e.g., Domain-based Message Authentication, Reporting & Conformance [DMARC], DomainKeys Identified Mail [DKIM], Sender Policy Framework [SPF]) to allow recipients to verify the domain of the organization that sent the messages. Configure email servers to support encryption of messages in transit to ensure message confidentiality and integrity (e.g., using Transport Layer Security), and manage certificates as appropriate.
- **Use only authorized email addresses with official government domain names—**Coupled with the email authentication technologies mentioned above, use of official email addresses gives users greater assurance in the authenticity of messages. All emails, including bulk messages sent from third-party providers, should use these official addresses.

- **Protect email accounts and systems with strong authentication and access control—**Access to email accounts and systems should require multi-factor authentication, with accounts disabled or locked when they are no longer needed or when suspicious activity is detected.
- **Use automated tools to monitor and scan all incoming and outgoing email—**Scan incoming emails to detect and isolate malware and other forms of attack. Consider data loss prevention tools to prevent leakage of personally identifiable information (PII) and other sensitive information.
- **Educate email users on safe and smart email use—**Teach email users not to click on suspicious attachments or embedded links. Provide a mechanism for users to report suspicious emails. Ensure users understand what information is appropriate in emails, such as prohibiting sensitive PII from email.

HOW TRUSTWORTHY EMAIL SUPPORTS CYBERSECURITY OBJECTIVES

While email should not be used to send or receive sensitive information, it nonetheless is a vital way for election officials to communicate with staff, technology partners, and voters. Implementing trustworthy email practices can help recipients verify that messages came from the election office, providing greater assurance in the reliability of that information. Sending all election-related email from official addresses makes it less likely that this email will be marked as SPAM by receiving email systems. Encrypting emails in transit provides some protection against eavesdropping, which could otherwise be used to harvest information about election officials or voters. Use of malware scanning can help block malicious or inappropriate content. Data loss prevention technologies can prevent sensitive information from leaving via email. The **NIST Cybersecurity Framework** provides guidance on the Protect and Detect Functions applicable to trustworthy email, such as access control (Subcategory PR.AC-7), training (PR.AT-1), data security (PR.DS-2), monitoring (PR.DS-5 and PR.DS-6), and anomaly and event detection (DE.CM-4).

Important Resources

- **NIST Cybersecurity Framework** – a voluntary framework, based on existing standards, guidelines, and practices, for reducing cybersecurity risks to critical infrastructure.
- **NIST Special Publication (SP) 800-45, Guidelines for Electronic Mail Security** – a NIST publication that offers foundational security recommendations for operating email systems.
- **NIST SP 800-177, Trustworthy Email** – a NIST publication that offers detailed technical guidelines for configuring specific security technologies to enhance trust in email.
- **NIST Usable Cybersecurity video: You've Been Phished!** – a NIST video showcasing research that reveals how context plays a critical factor in why users click or don't click on a phishing email.

To view other guides in the NIST Election Security Series, visit: vote.nist.gov