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 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

Configure email security technologies – Implement email authentication to allow message recipients to verify the system sending messages. Configure email servers to support message encryption.

Use only authorized email addresses with official government domain names – Use of official email addresses gives users greater assurance in the authenticity of messages.

Protect email accounts and systems with strong authentication and access control – Require multi-factor authentication and disable or lock accounts when suspicious activity is detected.

Use automated tools to monitor and scan all incoming and outgoing email – Detect and isolate incoming malware. Prevent leakage of personally identifiable and other sensitive information.

Educate email users on safe and smart email use – Teach users not to click on suspicious attachments or links. Ensure users understand not to put sensitive information in email.

HOW TRUSTWORTHY EMAIL SUPPORTS CYBERSECURITY OBJECTIVES

The recommendations in this guide can help achieve **NIST Cybersecurity Framework** outcomes related to access control, training, data security, monitoring, and anomaly and event detection.

IMPORTANT RESOURCES

- NIST Cybersecurity Framework
- NIST Special Publication (SP) 800-45, Guidelines for Electronic Mail Security
- NIST SP 800-177, Trustworthy Email
- NIST Usable Cybersecurity video: You've Been Phished!

For more information on this Trustworthy Email guide and to view other guides in this series, visit: vote.nist.gov

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