Best Practices for Emailing Military and Overseas Voters

Use a voter's personal email address.

This can be more successful than using military, government or corporate email addresses because links and attachments may be stripped before the recipient receives it.

Format links so they are written out rather than embedded.

- Write out https://www.fvap.gov, not FVAP.
- Sometimes [bracketing the link] may also avoid its removal or non-delivery.

When sending an email with links or attachments, follow up with a second, text-only email telling the voter to look for the first email and to contact you if it is not received.

Send a link rather than an attachment when possible.

If sending an attachment is the only option, ensure the file name does not contain spaces or special characters. Files names can include hyphens (-) and underscores (_).

Set aside a separate "sandbox computer" in your office for opening attachments to reduce security risks.

See this article on sandboxing techniques in South Carolina for more information on this option.

Whether using a mass-email service – like Mailchimp or Constant Contact – or sending emails one by one, be sure the email is authenticated using DomainKeys Identified Mail, or DKIM, and that the servers you use to send mail are authorized to do so using Sender Policy Framework, or SPF.

Additionally, setting up Domain-based Message Authentication Reporting and Conformance, or DMARC, gives other mail servers a way to handle messages that fail the previous authentication checks and helps prevent your domain from being used for email spoofing, phishing and other email-related threats. Work with your IT professionals to ensure these safeguards are correctly configured.

CSG
Overseas Voting Initiative
THE COUNCIL OF STATE GOVERNMENTS