CyberOhio

Challenges for Local Governments:

Addressing web and email migration hurdles of adopting a .gov internet domain

February 2026

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

Introduction **2**
Email Security Risks Without .gov **2**
Proposed Solution: A Holistic Approach to .gov and Email Migration **3**
Conclusion **3**
Sample Implementation Plan **4**
Step 1: Assess Readiness 4
Step 2: Apply for .gov Domains 4
Step 3: Set Project Scope, Budget, and Timeline 4
Step 4: Plan Email System Migration 4
Step 5: Plan Internet Domain Migration 4
Step 6: Plan for Migration of Non-Digital Assets 5
Step 7: Email Migration 5
Step 8: Website Migration 5
Step 9: Public and Staff Communication 5
Step 10: Final Cutover and Decommissioning of Old Domain(s) 5

INTRODUCTION

This white paper explores the barriers local governments face in adopting a .gov domain. While a .gov domain enhances public trust and cybersecurity, many municipalities face technical, administrative, and budgetary hurdles, particularly when migrating existing email systems to the new domain. This paper outlines key challenges and practical solutions to facilitate a smooth transition for both web and email services, positioning governments for stronger public engagement and resilience against cyber threats.

A key component to helping Ohio build cyber resilience is the Ohio Comprehensive Cybersecurity Plan (OCCP).[1] This plan consists of all five functions of the cybersecurity framework: identify, protect, detect, respond, and recover. Existing plans, structures, and other relevant efforts have been incorporated to develop and maintain this plan, enabling Ohio to provide governance and a framework that meets critical cybersecurity needs while maximizing the use of available resources.

CyberOhio coordinates the State of Ohio's cybersecurity capabilities and adopts a "whole-of-state" approach, leveraging existing and new committees, partnerships, and working groups to mature cybersecurity practices and incident response capabilities across Ohio.[2]

The Ohio Comprehensive Cybersecurity Planning Committee (OCC-PC) is a working group made up of local government entities, state agencies, , cybersecurity experts, and representatives from other public entities. The committee oversees the creation of the OCCP, the implementation of its goals, and the allocation of the State and Local Cybersecurity Grant Program (SLCGP) dollars for Ohio.[3] The OCC-PC continues to support. gov migration projects for Ohio local governments.

In 2024, CyberOhio received 58 applications from local governments requesting assistance supporting .gov migration projects. The CyberOhio Local Government Grant Program set aside over $330,000 to fund these efforts and will continue to support projects in the future.[4] As local governments in Ohio become more aware of the importance of .gov domains, adoption is expected to increase. The article, "Securing Our Digital Neighborhood – Your local government should switch to a .gov domains," explores the benefits a .gov domain provides for the public.[5]

EMAIL SECURITY RISKS WITHOUT .GOV

Local governments using non-.gov domains (e.g., AnytownOhio.org) are likely targets of email spoofing and phishing, which can lead to fraudulent requests for payments, theft of personal data, and ransomware attacks.

A concerning statistic is that 57% of U.S. county election websites operate on non-.gov domains.[6] This heightens the potential for these sites to be spoofed by bad actors and used for phishing scams, misinformation campaigns, or other malicious activities.

[1] Our Strategy | CyberOhio, 2025
[2] CyberOhio | CyberOhio, 2025
[3] State and Local Cybersecurity Grant Program (SLCGP) | CyberOhio, 2025
[4] CyberOhio Dot Gov Domain Grant | CyberOhio, 2025
[5] Securing Our Digital Neighborhood – Your local government should switch to a .gov domain, Dave Hatter, November 1, 2024
[6] Security Flaws on U.S. County Election Websites Raise Concerns Ahead of Election Day, November 5, 2024

PROBLEM STATEMENT

Although .gov domains provide security and authenticity, many local governments delay adoption due to concerns about the following:

- Email system migration complexities, including existing user accounts, archives, and integrations with other services.
- The cost of updating email licenses, reconfiguring systems, and notifying stakeholders.
- Technical challenges in configuring secure email (SPF, DKIM, DMARC, MTA-STS, and TLS-RPT) on the new domain.
- Fear of service disruptions during migration that could interrupt critical operations.
- Public communication risks, such as confusing constituents and partners during the transition.

Email represents one of the most mission-critical systems in many local governments, and uncertainty around migrating safely often leads to paralysis in broader .gov adoption efforts.

PROPOSED SOLUTION: A HOLISTIC APPROACH TO .GOV AND EMAIL MIGRATION

Governments can reduce risk and cost by taking a phased approach to .gov adoption that includes early planning for email migration. Key components of this strategy include:

- Pre-migration assessment of existing email systems, vendors, and user needs.
- Technical assistance partnerships to guide the setup of secure email protocols.
- Gradual email migration strategies (e.g., dual-delivery, alias forwarding) to reduce disruption.
- Clear staff and public communication plans to manage expectations and ensure continuity.
- Resources from federal programs and peer governments to guide the process.
- Consider applying for a CyberOhio .gov Domain Migration grant through the CyberOhio Local Government Grants Program.

CONCLUSION

Migrating to a .gov domain is a strategic investment in public trust and cybersecurity. Although the process involves technical and operational challenges, structured planning, technical assistance, and clear communication can help ensure a smooth transition. Governments that adopt .gov domains and secure email demonstrate professionalism, safety, and legitimacy, positioning themselves as trustworthy stewards of public digital services.

SAMPLE IMPLEMENTATION PLAN

Step 1: Assess Readiness

- Inventory existing email systems, domains, user accounts, and connected services (e.g., payment portals).
- Audit current website content, services, and connected platforms (e.g., payments, permitting).
- Identify mission-critical services and webpages that must remain functional during the migration.
- Identify third-party systems using existing email or website integrations.
- Inventory documents, posters, business cards, and other materials that will need updated with the new domain name.
- Identify critical contacts and communications to prioritize.
- Engage IT staff and/or external vendors early.
- Allocate budget for hosting, software, security tools, and vendor support.

Step 2: Apply for .gov Domains

- Register domains and review available resources at https://get.gov.[7]
- Obtain both web and email subdomains (e.g., citynameOhio.gov, mail.citynameOhio.gov).

Step 3: Set Project Scope, Budget, and Timeline

- Define phases and deadlines for email and website migration.
- Allocate a budget for hosting, software, security tools, and vendor support.
- Don't forget to include costs for keeping the old domain name so it does not fall into the wrong hands.
- Assign roles and responsibilities across IT, communications, and leadership teams.

Step 4: Plan Email System Migration

- Choose an email provider that supports modern security standards.
- Design an email migration strategy:
  - Dual delivery/alias set up to forward from the old domain temporarily.
  - Gradual creation of new .gov email addresses by department or priority.
  - Migration of archives and distribution lists.
- Configure multi-factor authentication (MFA) for all users.
- Set up DNS records for SPF, DKIM, DMARC, MTA-STS, and TLS-RPT to prevent spoofing and secure email traffic.

Step 5: Plan Internet Domain Migration

- Select a secure hosting provider.
- Set up DNS records for the .gov domain.
- Install SSL/TLS certificates for HTTPS.
- Design an internet domain migration strategy
  - Creation of the new website
  - Migration of documents that may require updates
  - Migration of archives

[7] CISA, get.gov, 2025

Step 6: Plan for Migration of Non-Digital Assets

- Design a migration strategy for non-digital assets
  - Letterhead
  - Business Cards
  - Signage, etc.

Step 7: Email Migration

- Plan a phased migration or “big bang” cutover (by department or all at once).
- Set up dual delivery/forwarding from the old domain to .gov for a grace period.
- Migrate email archives, contacts, and calendars.
- Test email sending and receiving, alias routing, and any applicable integrations.
- Test MFA.

Step 8: Website Migration

- Transfer website content, media, and documents to the new hosting site.
- Install SSL/TLS encryption certificates.
- Rebuild interactive tools, payment systems, and forms.
- Update all email addresses listed on the old website to .gov addresses.
- Set up 301 redirects from old site URLs to the .gov site.
- Test redirects and encryption.

Step 9: Public and Staff Communication

- Conduct internal briefings and staff training on the use of the new email addresses.
- Consider using public announcements, such as website banners, newsletters, and social media, to explain the change.
- Establish a grace period during which both old and new emails can coexist in parallel to minimize friction.
- If possible, coordinate email and website migrations for a unified rollout.

Step 10: Final Cutover and Decommissioning of Old Domain(s)

- Begin phased account migration.
- Monitor delivery success, bounce rates, and security reports.
- After stabilization, retire the old email domain or maintain only minimal forwarding for stragglers.
- Review and audit for residual uses of the old domain in official communications.
- Monitor website analytics for usability and access issues.
- Don’t forget to retain the old domain(s) to prevent malicious use in the future.

CyberOhio