The .gov Domain: Helping Mitigate Election Office Cybersecurity and Impersonation Risks

Transitioning to the .gov Domain: Why It Matters

Foreign adversaries and cyber threat actors have demonstrated the intent to target U.S. elections and election infrastructure in previous election cycles, and we expect the threat these actors pose to future elections will continue.[1] These actors may use a variety of tactics, including engaging in cyber threat activity targeting election office websites and email accounts, as well as conducting influence operations that seek to impersonate election offices or election officials.

The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) recommend all election offices adopt a .gov domain to help election offices and other state, local, tribal, and territorial (SLTT) government entities mitigate impersonation and cybersecurity risks. Similar to .com, .org, or .us domains, organizations use the .gov domain for online services, like websites or email. Unlike other domains, .gov is only available to official U.S.-based government organizations and publicly controlled entities. This means that users visiting a .gov website or receiving an email from a .gov email address can be more confident that the content is genuine government information. Similarly, use of the .gov domain can help the public better recognize official government sites and emails while avoiding phishing attempts and websites that impersonate government officials.

.gov registration is available to election offices at no cost. Learn more at https://get.gov

Understanding the .gov Domain

Similar to .com, .org, or .us domains, .gov is a top-level domain (TLD). Individuals and enterprises use a TLD to register a domain for their online services. Unlike many TLDs, where anyone can register by simply paying a fee, .gov is available *only* to U.S.-based government organizations and publicly controlled entities. In addition to federal agencies, this includes all election offices and other SLTT government organizations. CISA administers the .gov TLD and, since 2021, has made it available at no cost to election offices and other qualifying government organizations. An increasing number of election offices and other SLTT government organizations have already transitioned to a .gov domain. Among election offices, nearly all state and territorial election offices (52 of 56) have transitioned their websites to .gov; local election office adoption continues to increase as well.[2]

Mitigating Risk of Impersonation

Foreign adversaries and cybercriminals may seek to impersonate official election websites and email addresses to disseminate false or misleading information; gather usernames, passwords, email addresses, or other personally identifiable information of those visiting the website; or spread malware. A common form of impersonation is known as "typosquatting," where malicious actors create seemingly legitimate websites based on common user typos (e.g., using a slightly misspelled word, such as "electon" instead of "election" or a different TLD such as "[.]com" instead of "[.]gov"). This may also include phishing attempts that impersonate legitimate email addresses of election officials.

---

[1] Department of Homeland Security Office of Intelligence and Analysis: Homeland Threat Assessment 2024.
[2] Use rates are not provided due to data limitations (e.g., .gov TLD registrar data currently does not disaggregate between local government office websites and local election office websites).

In 2020, the FBI identified multiple typosquatting domains potentially intended to maliciously influence U.S. elections. Examples include the domains "www.votepa.com" and "www.votespa.com" which were likely intended to trick visitors seeking the Pennsylvania state election office website. Later, after the Pennsylvania state election office completed its transition to a .gov domain, "www.vote.pa.gov," the FBI observed typosquatting websites that replicated the original election website and others that redirected network traffic to entirely different websites, such as U.S. retailers. Impersonation efforts like this are part of why CISA recommends maintaining former non-.gov domains in perpetuity, ensuring old domains do not fall into the hands of threat actors. Maintaining former non-.gov domains also enables redirection for users who follow old links or send email to old email addresses to the new domain.

Typosquatting is a form of targeting that leads internet users who incorrectly type a website address into their browser to an alternative and potentially malicious site. The alternative website may imitate the look of the intended website and contain malicious software or attempt to steal personally identifiable information. The alternative website may also be used in phishing operations.

Phishing is a form of social engineering in which a cyber threat actor poses as a trustworthy colleague, acquaintance, or organization to lure a victim into providing sensitive information or network access. The lures can come in the form of an email, text message, or even a phone call. If successful, this technique can enable threat actors to gain initial access to a network and affect the targeted organization and related third parties. The result can be a data breach, data or service loss, identity fraud, malware infection, or ransomware.

As .gov domains are only provided to U.S.-based government organizations and publicly controlled entities, internet users visiting a .gov website or receiving an email from a .gov email address can be more confident that the content is genuine government information. Similarly, use of the .gov domain can help the public recognize and avoid phishing attempts and websites that impersonate government officials. For example, an internet user may have trouble distinguishing between two .com websites purporting to be the same local election office website; however, the user would likely have less trouble distinguishing between an illegitimate .com website and a legitimate .gov website.

Mitigating Cybersecurity Risk

Protecting against and building resilience to cyber threats targeting election office websites and related systems is a core component of election infrastructure cybersecurity risk management. Election office websites provide information about voting and elections, including unofficial election results, and often host applications that provide services to voters, such as polling site look-up tools and online voter registration portals. This makes them attractive targets for cyber threat actors seeking to disrupt or undermine confidence in election processes.

Use of the .gov domain helps mitigate cybersecurity risks to websites and related systems in the following ways:

- Unlike commercial registrars, multi-factor authentication is enforced on all accounts in the .gov registrar. This protects domain registrar accounts against unauthorized access by threat actors that have illicitly acquired user credentials.
- CISA "preloads" all new .gov domains, which requires browsers to only use a secure HTTPS connection with the website. This protects visitors' privacy and ensures the integrity of the published content.
- Security researchers regularly share reports with CISA about potential security issues on individual .gov domains, and CISA subsequently shares any actionable information with the registrant. Additionally, governments can add a security contact for their domain, making it easier for the public to report a security issue directly.

Transitioning to .gov

Transitioning to a .gov domain is a multi-step process informed by organization-specific requirements. CISA's guidance on .gov transition includes branding and public communication considerations, and technical tasks such as identifying domain name system hosting, maintaining previous non-.gov domain registration, managing web redirects, and converting email.

The transition process will likely require substantial effort in the beginning, but administrators can prioritize actions they deem most important based on their organization's needs. Simple steps, like setting up redirection from an old domain to the new .gov domain, are helpful to users and can help protect election offices against impersonation.

While CISA has eliminated the cost of registration, resource and staffing constraints can make a transition more challenging. For example, costs associated with transitioning to a .gov domain may include paying IT staff or contracted IT service providers to facilitate the switch, or indirect costs like replacing printed marketing materials and informing the public of the change. Election officials may be able to receive assistance from their state government, including financial and technical assistance (e.g., subdomain delegations or web hosting), or financial assistance through federal grant funding to help offset costs.

Federal grants can be used to support costs associated with a .gov transition. Certain federal grant funds, including the Homeland Security Grant Program, the State and Local Cybersecurity Grant Program, and Help America Vote Act funds, can be used to support transitioning to .gov. Learn more at each program's website.

.gov Domain Management Best Practices

In addition to transitioning to the .gov domain, consider adopting these additional best practices to further advance your security posture:

- ***Publish a list of all legitimate state and local election office domains*** on the state's election website.
- ***Add a security contact***: A security contact provides the public a way to report observed or suspected security issues on a domain. This could include notifications about compromised accounts, unsolicited email, routing problems, or reporting a potential vulnerability.
- ***Develop a vulnerability disclosure policy (VDP):*** A VDP outlines how an organization prefers to receive vulnerability reports and what it will do with them, the scope of systems covered by the policy, and legal authorization for those who follow the policy and report in good faith.
- ***Preload your domain***: Web browsers allow domains to be "preloaded." This means that web browsers will always use HTTPS to connect with those websites.
- ***Establish a DMARC (Domain-based Message Authentication, Reporting, and Conformance) policy*** to make it more difficult for malicious actors to successfully spoof your domain in email.
- ***Report cyber incidents and suspicious activity*** to FBI, CISA, EI-ISAC, and relevant state and local authorities.
    - **Report to CISA's** 24/7 Operations Center at report@cisa.gov or (888) 282-0870
    - **Report to FBI**:
        - Local FBI Field Offices: fbi.gov/contact-us/field-offices
        - FBI Internet Crime Complaint Center (IC3): ic3.gov
    - **Report to EI-ISAC**: soc@cisecurity.org or (866) 787-4722