Springbrook
www.springbrooksoftware.com

.gov

Time to get .gov!

The .gov designation is a Top Level Domain (TLD) developed as a unique identifier for government entities.It is only available to bona fide US government organizations to help government entities establish and maintain online trust for its digital properties (websites, emails, etc.) as a legitimate source of government information.

While the security advantages of a .gov domain are not inherent to the domain itself, there are several security benefits associated with its use. Here are some advantages:

Enhanced Trust

The .gov domain is exclusive to government agencies, which lends credibility and trust to websites utilizing this domain. Visitors are more likely to trust information and services provided through official government channels.

Authentication and Verification

Obtaining a .gov domain requires a stringent verification process to confirm the legitimacy and authority of the government entity. This verification process helps prevent malicious actors from posing as government agencies or institutions.

Protection against Impersonation

The .gov domain helps protect against domain spoofing and impersonation attacks. It makes it more difficult for threat actors to create fraudulent websites that imitate official government sites, reducing the risk of phishing and other social engineering attacks.

Prioritized Security Measures

Government entities often implement robust security measures to protect their online presence. This can include measures like multi-factor authentication, advanced encryption, intrusion detection systems, regular security audits, and compliance with security standards and regulations.

Government-Level Security Expertise

Government agencies usually have dedicated IT departments or cybersecurity teams with expertise in implementing and managing security measures. These teams focus on protecting the integrity, confidentiality, and availability of government systems and services.

Collaboration and Information Sharing

Government agencies often work together on security initiatives and share information about emerging threats, vulnerabilities, and best practices. This collaborative approach can enhance the overall security posture of government entities, benefiting those using the .gov domain.

Ongoing Monitoring and Incident Response

Government agencies typically have mechanisms in place for monitoring their systems and networks, as well as responding to security incidents promptly. This proactive approach helps identify and mitigate security breaches or vulnerabilities effectively.

It's important to note that while a .gov domain can provide certain security advantages, it does not guarantee absolute security. Government entities still need to implement appropriate security controls, keep their systems up to date, educate their personnel about security best practices, and stay vigilant against emerging threats.

How does it work? According to CISA.gov:

The .gov registrar requires the use of two-step verification for all users and user accounts, and user accounts cannot use passwords that have been found in known data breeches.

Web browsers now allow domains to be preloaded as HTTPS-only. Preloading lets web browsers know to always use HTTPS to connect with any website on that domain.

The Cybersecurity and Infrastructure Security Agency (CISA), GSA and the National Institute of Standards and Technology (NIST) help monitor for issues in the namespace.

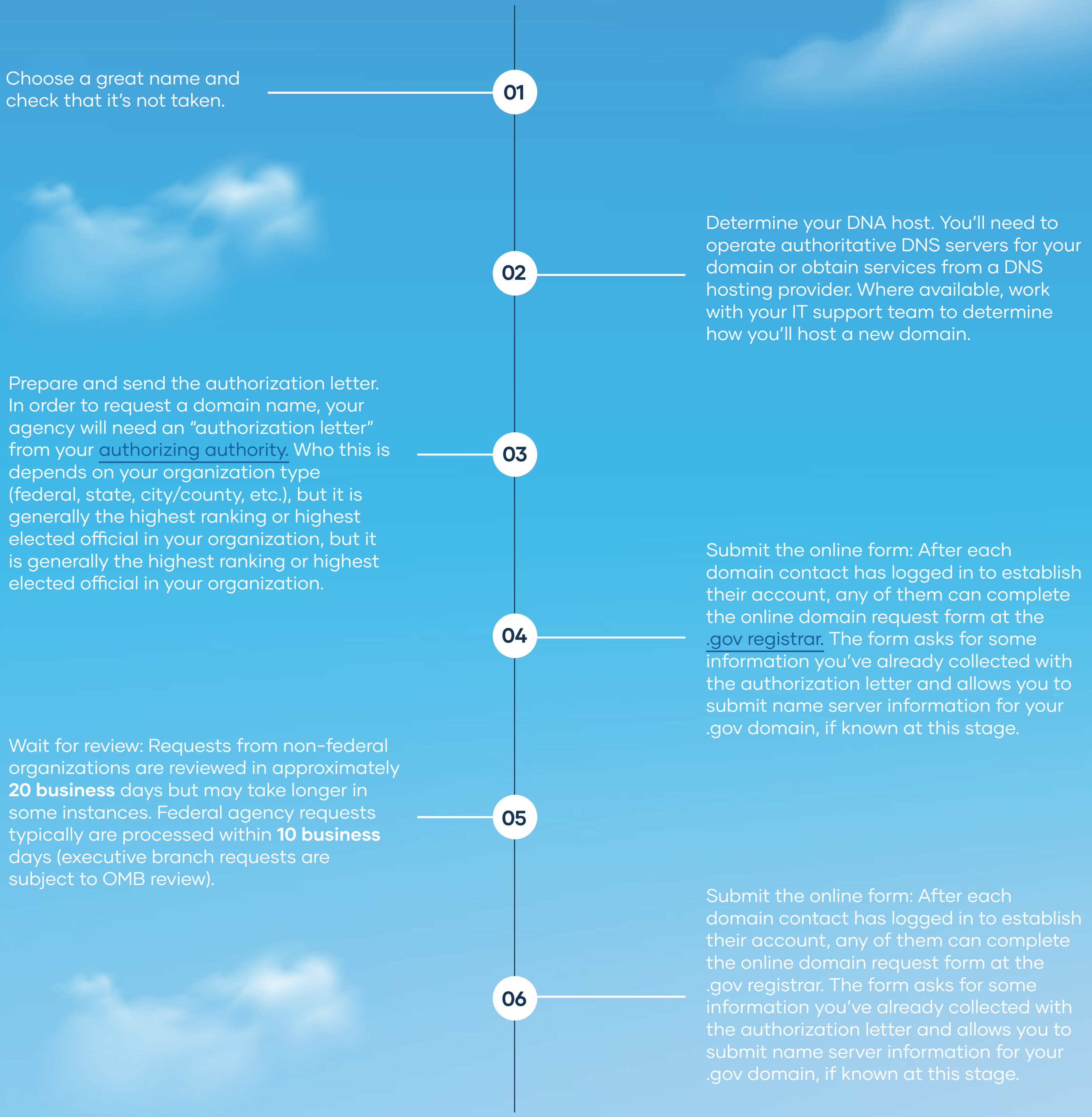
How does an agency obtain a .gov domain?

.gov domains are now available free of charge to eligible government organizations.

Only U.S.-based government and public sector organizations are eligible to obtain a .gov domain. This includes any federal, state, local, or territorial government entity, or other publicly controlled entity. It also includes any tribal government recognized by the federal government or a state |government. Eligibility is determined by the DotGov Program, which will be informed by the United States Census Bureau’s criteria for classifying governments.

Complete eligibility requirements can be found here.

Attaining a .gov domain is a multi-step process. Here is the information from get.gov:



01 Choose a great name and check that it's not taken.

02 Determine your DNA host. You'll need to operate authoritative DNS servers for your domain or obtain services from a DNS hosting provider. Where available, work with your IT support team to determine how you'll host a new domain.

03 Prepare and send the authorization letter. In order to request a domain name, your agency will need an "authorization letter" from your authorizing authority. Who this is depends on your organization type (federal, state, city/county, etc.), but it is generally the highest ranking or highest elected official in your organization, but it is generally the highest ranking or highest elected official in your organization.

04 Submit the online form: After each domain contact has logged in to establish their account, any of them can complete the online domain request form at the .gov registrar. The form asks for some information you've already collected with the authorization letter and allows you to submit name server information for your .gov domain, if known at this stage.

05 Wait for review: Requests from non-federal organizations are reviewed in approximately **20 business** days but may take longer in some instances. Federal agency requests typically are processed within **10 business** days (executive branch requests are subject to OMB review).

06 Submit the online form: After each domain contact has logged in to establish their account, any of them can complete the online domain request form at the .gov registrar. The form asks for some information you've already collected with the authorization letter and allows you to submit name server information for your .gov domain, if known at this stage.

Review security best practices before launching your domain: Domain management is about more than just DNS. It's also about ensuring a safe experience for your organization and your users. Here are the domain security best practices your agency should be aware of: Domain Security Best Practices.

Ready to start your journey to establishing your .gov domain? Here's where you begin.

For more information on cybersecurity: The Springbrook Cybersecurity Resource Center.

www.springbrooksoftware.com