Request for Information

.gov TLD services

The Cybersecurity and Infrastructure Security Agency (CISA) is conducting market research to gain technical feedback on, and identify potential vendors to, support the secure and reliable operation of the .gov top-level domain (TLD). This includes:

1. A **registry services provider** to manage core Domain Name System (DNS) infrastructure for the TLD, including authoritative DNS hosting for individual domains.
2. A **registrar** providing web registration and management of .gov domains; offering supporting services to improve the security, privacy, reliability, accessibility, and speed of .gov domains and the services hosted within them; and supporting end-users. The registrar will also serve as the TLD's website.

Background

Under the DOTGOV Act of 2020, CISA is the .gov TLDs policy and management authority: the agency is responsible for global DNS resolution and administration of the .gov zone. This includes managing requirements for the issuance and maintenance of .gov domain names, evaluating registrants' eligibility for a given domain name, and overseeing the general utility and security of the .gov namespace.

.gov is a unique TLD:

- *It is one of the six original TLDs in the internet's DNS.*
- *It is a "sponsored TLD"*, meaning it is only available to bona fide U.S.-based government organizations. .gov is actively used by each branch of the federal government, every state in the nation, hundreds of counties and cities, many tribes and territories, as well as publicly controlled entities as each serves the public on the internet.
- *The .gov zone is relatively small*, composed of approximately 6,500 domains. CISA anticipates consistent growth over the next few years.
- *CISA intends to not charge fees to end-users for domain registration or other services*.
- *.gov has no registry agreement with* the Internet Corporation for Assigned Names and Numbers (ICANN). CISA anticipates close alignment with the norms followed by registries and registrars that are bound by publicly available agreements with ICANN, but seeks to use this flexibility to test and promote emerging good practices while maintaining useful established practices. Certain features of the registrar may require it to be accredited by ICANN in the future.

Because the TLD is central to the availability and integrity of thousands of online services relied upon by millions of users .gov TLD is critical infrastructure for governments throughout the country and all aspects of its administration have cybersecurity significance. CISA seeks to increase security and decrease complexity for government organizations and public users of .gov – including by increasing CISA's and registrants' insight into important security-relevant information derived from the maintenance of a ".gov inventory", as described in the DOTGOV Act.

CISA seeks to administer the TLD transparently, in the spirit of public accessibility, privacy, and security, and are looking to partner with others that hold and display these values.

This request for information is to increase CISA's understanding of the capabilities within the marketplace to deliver services to the .gov TLD's users. The core requirements are for *registry services* and a *registrar*, which may be provided by one or more service providers.

- CISA anticipates registry services, including authoritative DNS hosting, being managed by a service provider.
- For the registrar, CISA is interested in assessing how the objectives align to current market offerings – or whether CISA, acting as the product owner, would lead the creation of a new, open source registrar with an agile software development team.

Objectives for the .gov TLD

1. **Registry services**: Given its unique role, .gov requires a U.S.-based provider whose core competency is DNS services. The registry is anticipated to be a FIPS 199 high impact system and a high value asset. The provider will prepare and manage security compliance documentation.

   Characteristics of the service include:

   - Authoritative nameservers for the .gov TLD, and global, always-available DNS resolution of the DNS Security Extensions (DNSSEC)-signed .gov zone. Average query load is currently between 10 and 20 billion queries per month.
   - Authoritative DNS hosting for registered domains and child zones (while retaining the ability for registrants to delegate to nameservers they manage). Wide support for useful and emergent resource records. Application programming interfaces (APIs) are exposed to enable an infrastructure-as-code approach to DNS management.
   - Authoritative DNS hosting for government-managed domains that are not on .gov (after CISA's approval in the registrar).
   - Offers best current and useful emergent practices in DNS security or the security of applications via DNS (e.g., authoritative-to-recursive encryption, message digest for DNS zones, DMARC extension for public suffix domains).
   - Registration data directory services: WHOIS, Registration Data Access Protocol (RDAP).
   - Interface with the registrar over industry-standard protocols (e.g., Extensible Provisioning Protocol [EPP] over TCP, with TLS) in order to support program management or implement policy (e.g., the registrar places a registration on server hold

until policy requirements are met). Provide and maintain any additional access, APIs, or information, including documentation, needed to support all useful registrar activities.

- Regular publication of the .gov zone file via e.g., ICANN's Centralized Zone Data Service.
- Track, and make available via API or automated means, useful performance metrics and trends for the .gov zone (e.g., query load, zone count).
- "Tier 3", 24x7 engineering support to CISA and the .gov registrar provider to remedy issues related to the registry or DNS hosting.
- Demonstrated commitment to the security and stability of the internet, including through contributing or meaningfully participating in relevant internet standards or in internet operations, research, or security groups.
- At minimum viable product (MVP), the service provider supports a seamless transition from the incumbent registry services provider (as necessary).

2. **Registrar**: A modern, user-centered, responsive web application, in alignment with the requirements of the 21st Century Integrated Digital Experience Act, to enable .gov registrants to manage their domain's registration lifecycle, DNS settings, and useful supporting services. The registrar will also be the central .gov hub for CISA, supporting registrant management and tracking technical performance indicators for the TLD. For CISA and registrants, the registrar will help generate insights into the security of an organization's internet-accessible systems.

    - The registrar is anticipated to be a FIPS 199 moderate impact system. The provider will assist in preparing and managing security compliance documentation.
    - CISA anticipates the registrar being deployed in a cloud environment that CISA or another government agency manages, not in a registrar provider's environment.
    - CISA seeks an experienced provider of digital services with a documented commitment to continuous user research and the incremental delivery of new features to enhance functionality and improve user experience, including user documentation. CISA envisions the registrar will be developed as open source software by an agile software development team (with CISA acting as product owner) or by a provider of commercial registrars.

The following sections describe the key elements of the registrar:

- **Public website**: General information about the TLD and the registrar function is currently split between home.dotgov.gov, the TLDs homepage, and domains.dotgov.gov, the registrar.
    - Pre-authentication, the registrar will serve as the public website for the .gov TLD. Content will be managed by CISA.

    - The site allows the public to learn about .gov's management, policies, impact, history, and other relevant documentation.
    - Enable potential registrants to check the availability of a domain of interest or submit a question about .gov.
    - Publish domain data and relevant metadata in e.g., .csv, .json.
    - Updates to public content will not require downtime to the registrar functions, nor vice-versa.

- **Registration, renewal, retiring**: A "simple and secure" registration process that works to "ensure that domains are registered and maintained only by authorized individuals" (DOTGOV Act).
    - In alignment with the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-63A, help re-envision and digitize a legacy enrollment and identity proofing process. (The process currently revolves around a signed letter that is created and submitted outside of the registrar.)
        - Provide decision support to help CISA verify and adjudicate domain claims (e.g., is the requesting government organization eligible for a domain?; is the request from the appropriate authority for the organization?; is the person making the request actually that authority?, does the requested domain name meet .gov's naming requirements?).
        - Support useful technical measures to facilitate additional assurance in the authorization of a potential registrant organization (e.g., domain-validating a government organization's current domain via a string in TXT record at a specific DNS location).
    - Manage domain requests as an issue, allowing a CISA team to respond to questions, assign requests to CISA team members, make comments, adjudicate the request, and document decisions (e.g., approval/rejection). In-app or emailed notifications are made on relevant changes.
    - Support for distinct approval flows, including notifications to appropriate parties, for different domain types (e.g., certain domain types, like those from federal agencies, may require additional scrutiny or approval).
    - Maintain metadata about current and historic domain requests in the registry (e.g., names, domain type, registrant organization, contact information.
    - Interface with the .gov registry over industry-standard protocols (e.g., EPP over TCP, with TLS).
    - Manage the domain renewal process: notify registrants annually before a domain needs to be renewed. Require registrants review/update contact information for key personnel before renewal. Facilitate domain deletion requests in-registrar.

- **DNS management**: Tying DNS hosting managed by the registry services provider to the .gov registrar should enable "one-click" compliance with best current practices and federal standards related to DNS.
    - Consistent with the NIST SP 800-63B, the registrar shall have strong user authentication. In general, sensitive domain- or account-impacting actions must be initiated in-registrar, post-authentication (e.g., domain deletion requests).
        - Different than commercial registrars, where individual administrative, billing, or technical contacts are associated with a *domain*, user accounts should primarily be associated with *an organization that has domains*. An organizational superuser shall manage users and their permissions (e.g., limit which user may take certain actions on a domain).
    - Allow registrants to manage .gov domains' DNS in the web UI (e.g., manage resource records and their values, create subdomains), or delegate to nameservers they manage.
    - Interface with authoritative nameservers via API to support an infrastructure-as-code approach to DNS provisioning and management.
    - After CISA approval, enable government-managed non-.gov domain names to use the registry provider's hosted DNS service and manage DNS settings in the web UI.
    - Facilitate government-registered non-.gov domain names to be transferred into the .gov registrar, and manage registry lock requests to major gTLD registries (for non-.gov domains; .gov domains may not be transferred out of the .gov registrar).

- **.gov inventory**: Under the DOTGOV Act, CISA will "inventory all hostnames and services in active use within the .gov internet domain and provide the data... to domain registrants".
    - Develop, use, and/or contribute to open source tools to regularly collect hostnames and service data via public and non-public sources (as CISA provides or directs), including from hosted nameservers, into an organized inventory.
    - Capture useful metadata that cannot be obtained from e.g., internet scans, like associating multiple hostnames and services together in a system, or documenting a system's purpose.
    - Make the inventory available through the registrar to registrants and share relevant information with stakeholders and/or the public, in alignment with the DOTGOV Act.

- **"Supporting services"**: The DOTGOV Act allows CISA to offer "supporting services" that "support the security, privacy, reliability, accessibility, and speed of registered .gov internet domains".
    - Using the .gov inventory and e.g., conducting network scans or using third-party APIs, produce data, insights, or managed alerts for registrants and CISA on:

        - Exposure monitoring (e.g., Crossfeed)
        - Uptime monitoring
        - Summary statistics (e.g., crawler.ninja)
        - Support the reporting of potential security incidents to registrants
    - For domains that do not use .gov’s hosted DNS services, provide data/alerts to registrants regarding their nameserver infrastructure (e.g., notify on lame delegations, when a dependent domain is or may soon be registrable).
- **End-user support**: The registrar shall optimize for self-service, including in password resets, username reminders, certificate verification, or domain metadata updates. If necessary to support the registrar objectives, operate an online help desk to provide “tier 1” customer support for questions about e.g., DNS, registration and naming requirements, or account management.

RFI Response

CISA invites feedback from all interested service providers, U.S.-based government organizations, and others on the utility and feasibility of the above objectives at the web form available here. Responses shall be provided via form here. The form will close on **July 21, 2021 at 5:00 PM Eastern Time**.

Some sections require a longer answer, and we recommend that you draft responses in a document editor and paste them in the appropriate field.

This RFI is for information and planning purposes only and is not to be construed as a commitment by the Government. No award will be made as a result of this RFI and the Government is not obligated to release a future solicitation based on this market research.

Information submitted must be available at no cost or obligation to the Government. Submissions become Government property and will not be returned, including any proprietary information; any information you consider proprietary should be clearly marked as such.

The Government may consider additional communication as part of the ongoing market research and may reach out at a later date requesting more information. Service providers who do not respond to this RFI are not excluded from any resulting solicitation(s).