DNS Purchasing Guide for Government Procurement Officers

ICANN Office of the Chief Technology Officer

David Huberman
OCTO-013
24 July 2020

TABLE OF CONTENTS

This document is part of the OCTO document series. Please see the OCTO publication page for a list of documents in the series. If you have questions or suggestions on any of these documents, please send them to octo@icann.org.

1 Introduction

This guide is intended to help government procurement officers make good domain name and Domain Name System (DNS) procurement choices to help ensure the security, stability, and resiliency of the naming of services and hosts of your government's networks. Expertise about the DNS is not required to use this guide. It is written in accessible language to help you work with both your IT department and your vendors.

This document is published by the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a not-for-profit public-benefit corporation that, on behalf of the Internet community, oversees the technical coordination of the top-most level of the Internet's Domain Name System (DNS), helping to ensure its security, stability, and resiliency.

This guide suggests good operational technologies and practices. Not all vendors will provide every service or technology we list. But to help you make a fully informed procurement decision, you should know which of our recommended technologies they support and which they don't.

This guide focuses on three phases for obtaining and operationalizing domain names:

- Choosing a domain name
- Registering a domain name
- DNS operations: hosting for your domain name

2 Choosing a Domain Name

Domain names end in a suffix. Some examples of these suffixes include *.com*, *.gov*, *.uk*, and *.asia*. There are over 1,300 of these suffixes in the DNS, and they are called top-level domains, or *TLDs*. When choosing a domain name, you first have to decide which TLD to use, be it a generic name (suffixes like ".com" or ".asia" that have a generic meaning) known as a *gTLD*, or a two-letter country code top-level domain, called a *ccTLD*, from a recognized territory (suffixes such as *.fr* for France or *.za* for South Africa, where each suffix corresponds to territory codes listed in the ISO-3166-2 standard).[1]

In many cases and in order to follow established local rules and policies, government agencies may need to use a domain name under their nation's ccTLD (e.g., *go.jp* for a government agency in Japan). Different governments operate their ccTLDs in different ways. We recommend that you speak with the operator of your government's domain name services, ask about the policies in place, and check their functionality, security features, and business continuity plans (as described below) so you can compare them with any other TLD options that may be available to you. Contact information for the managers of each TLD, including for each ccTLD, is published in a directory located at https://www.iana.org/domains/root/db (to get to the contact info, you have to click on the link for the TLD).

ICANN has a contract with each gTLD that specifies many rules. Specifically, gTLDs are required to abide by the terms and conditions of the ICANN registry agreement to which they

[1] See https://www.iso.org/iso-3166-country-codes.html for more information on the ISO-3166-2 standard. ICANN does **not** assign ISO-3166 codes; that is the role of the ISO-3166 Maintenance Agency.

are signatory.[2] These terms and conditions place certain technical and policy requirements on gTLD managers, aimed both at improving the health of the DNS ecosystem and protecting domain name holders. In contrast, ccTLDs do not have signed agreements with ICANN. Any legal remedies a domain name holder might need would likely depend on the legal jurisdiction in which the ccTLD registry operates.

Whether you are registering a domain name in a ccTLD or in a generic TLD, there are four features a TLD may offer that we think are important: support for DNSSEC, support for IPv6, implementation of some form of registry lock, and the reputation of the TLD.

2.1 DNSSEC Support

Users are better protected if domain names are cryptographically signed by the domain name owner, i.e., your organization. Your organization can digitally sign your domain names via a technology called Domain Name System Security Extensions (DNSSEC). ICANN's document "DNSSEC: Securing the DNS" gives more information on why DNSSEC is important.[3]

To sign your domain, the TLD you choose needs to support *DNSSEC signing*. The good news is most TLDs (including all generic TLDs) support DNSSEC. If DNSSEC support is not shown as an option with the TLD of your choice, however, then you should inquire about their current or planned support for this option. Admittedly, learning how well a TLD supports DNSSEC isn't always straightforward. Some TLDs will publish this information on their website; others will not. You might be able to do some web searches to find this information, or you may even need to email or call them to talk about it.

2.2 IPv6 Support

Machines on the Internet use Internet Protocol (IP) addresses to identify themselves to other machines. There are two types of IP addresses: IPv4 and IPv6. IPv4 addresses are the most common types of IP addresses. IPv6 is a newer type of IP address designed to help the Internet continue to grow as more and more devices are added.

Because some governments have requirements that Internet infrastructure support both IPv4 and IPv6 addressing, check with the TLD operator to ensure both IPv4 and IPv6 addresses are supported for your DNS servers. Specifically, the TLD operator needs to support you having authoritative name servers that have IPv6 addresses. If this is the case and your TLD operator doesn't support IPv6, the world will not be able to reach sites in your domain.

2.3 Registry Lock

Another important consideration when choosing a TLD is to ask the TLD operator if they support a feature called *registry lock*.

[2] There are multiple versions of ICANN's Registry Agreement, and different TLDs are signatory to different versions. The current version is known as "the 2017 base registry agreement", and it is found at: https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html

[3] See https://www.icann.org/en/system/files/files/octo-006-en.pdf

A TLD operator manages “a registry” that contains all the second-level domains, e.g., example.tld, within the TLD.[4] Registry lock allows domain name owners, known as registrants, to tell the TLD operator to “lock” the domain name, just like locking your car doors. When your domain is locked, no one can make changes to it, delete it, or transfer it to another registrant without some sort of authorization process that you have defined with the TLD operator. Note, however, that there are no industry-wide standards for how registry lock is implemented, so you should ask the TLD operator if they offer registry lock, and if they do, how it works.

In general, we think the best process to authorize changes involves “out of band” authorization, where all parties do not rely on Internet-centric communication, but instead, rely on phone calls or some other method that attackers would have a difficult time penetrating. Changes to the basic characteristics of a domain name should be very uncommon, so relying on a slower process like out of band authorization is acceptable. At the same time, however, it is probably good to ensure that your TLD operator has a clearly written escalation procedure in the even less common case that some DNS data needs to be changed on an emergency basis.

We strongly encourage all registrants to use TLDs that support registry lock as it prevents known attacks that can compromise entire domains.

2.4 Reputation

Lastly, before you choose a TLD, consider investigating its reputation. According to the anti-abuse company Spamhaus,[5] a TLD has a bad reputation if too many of the domain names registered in it are related to activities such as spam and malware distribution. While there will always be some malicious domain names registered in every TLD, companies like Spamhaus measure entire TLD name portfolios to determine the “badness” or “goodness” of a TLD.

What’s important is to choose a TLD that does not have a significant number of malicious registrations. When a TLD has a poor reputation in the technical community, it may be blocked by Internet service providers (ISPs) and enterprise network operators. If the TLD you use has a poor reputation, you may, for example, not be able to send email using your domain as many mail servers are automatically configured to block email originating from domains on blocklists.

There are numerous anti-abuse companies that publish rankings of the reputation of TLDs, including Spamhaus and SURBL.[6]

3 Choosing a Domain Name Registrar

Once you have chosen a TLD for your agency, you then register a domain name under it. You can register domain names in some ccTLDs directly through the TLD operator. For many ccTLDs and most gTLDs, however, you register a domain name via a domain name

[4] Confusingly, a TLD operator can also be referred to as a registry
[5] See https://www.spamhaus.org/
[6] See http://www.surbl.org/

"registrar."[7]In this section, we list some criteria we suggest you investigate when choosing a potential domain name registrar.

3.1 Accreditation

ICANN offers registrars official accreditation. Successfully obtaining and maintaining accreditation signifies that the registrar has demonstrated that it met all the technical, operational, and financial criteria necessary to qualify as a registrar business.[8] Importantly, the registrar is bound to the terms and conditions of the Registrar Accreditation Agreement,[9] which includes many protections for domain name registrants.

If you are registering a domain name in a gTLD, make sure you are choosing an ICANN-accredited registrar. A list of accredited registrars is found on the ICANN website.[10] The agreement that registrars sign with ICANN also allows them to work with "resellers", which are third-party companies that offer domain name registration services on behalf of a registrar. However, for high-value domains, we recommend working directly with accredited registrars when possible because it reduces the number of parties involved if there is a need to address an urgent issue.

If you are registering a domain name in a ccTLD, make sure you are using a registrar or reseller who is authorized by the ccTLD registry.

3.2 Basic Security Features

Any domain name registrar you choose should support strong passwords (typically long strings with some combination of one upper-case letter, one lower-case letter, and at least one symbol) and offer multi-factor authentication (a password plus some sort of security token, which is often a SMS code sent to a mobile phone) for users logging to their account portals.

You should also verify with the registrar or reseller you're using that the customer account portals are running on a website for which communication is encrypted using HTTPS. This helps ensure confidentiality of electronic communications between your IT staff and the registrar/reseller.

3.3 DNSSEC Support

If you have gone to the effort to ensure your registry supports DNSSEC, it is important that you choose a registrar that allows you to supply the necessary DNSSEC-related information and, if you are not managing your zones directly, to DNSSEC-sign your zones. Registrars should generally publish DNSSEC services they support on their website. You may also want to have

[7] You can view the registry/registrar split as similar to the wholesale/retail split, i.e., just as people buy stuff at retailers who source from wholesalers, registrants buy domain names from registrars who obtain their inventory from registries.

[8] A description of accreditation qualifications can be found at https://www.icann.org/resources/pages/policy-statement-2012-02-25-en#IIA

[9] The current RAA is published at: https://www.icann.org/resources/pages/registrars/registrars-en

[10] See https://www.icann.org/registrar-reports/accreditation-qualified-list.html

your technical staff discuss with the registrar the level of DNSSEC support offered to ensure that your technical requirements are met.

3.4 IPv6 Support

The domain name registrar must support using both IPv4 and IPv6 addresses, that is, allow you to manage the address ("A" and "AAAA") resource records for all devices you want to name within your domain name.

3.5 Data Export

Thinking long-term, you don't want to get locked into using your domain name registrar forever. Your technology needs may change, or the registrar's service may degrade, or something else may happen in the future that prompts you to transfer your domain names to a different registrar. As such, it would be helpful if the registrar allows you to "export your zone data," that is, it allows you to download all the DNS data associated with your domain names. This gives you control over the DNS data for your domains, and allows the IT staff to quickly transfer services to a new registrar.

3.6 Reputation

Any domain name registrar you choose should have both a good anti-abuse reputation and a proven track record of working cooperatively with national and international law enforcement agencies when DNS abuse is reported to them. For example, you should ensure that the registrar is running a strong anti-fraud program that allows them to detect and stop domain name registrations involving the use of stolen credit card information.

4 DNS Operations: Third-party Hosting for your Domain Name

Once you have registered a domain name, it needs to be hosted somewhere. It may be hosted by your government IT department or it may be possible or even necessary to choose a third-party vendor to host your domain names in their data centers. This hosting may be offered as part of a bundle of services that you purchase from an IT provider. This section focuses on helping you choose a third-party vendor, and suggests a few aspects we think are important.

4.1 Domain Name Management

It is important that you are able to quickly and easily create subdomains. A subdomain is a domain name that looks like *mail.department.za* or *elections.government.co.jp* or similar. You should inquire about how easy it is to create, modify, and delete sub-domains, especially in bulk. It is also important that you are able to create modern DNS record types, for example the TLS Authentication (TLSA) record type which is used by a security technology called DNS Authentication of Named Entities (DANE).

4.2 Security of Operations

One of the most important considerations when purchasing DNS services is security. It is critical that your organization *maintain control* of all your domain names and the services hosted on them at all times. The best way to maintain this control is by always working with vendors - from the domain name registrar down to all IT providers - who have a strong culture of, and commitment to, security. When you lose control of any portion of your DNS technologies, attacks can happen very quickly, and data breaches can occur.

For a third-party hosting provider, we note three security elements that are crucial for providing strong security:

- They must offer multi-factor authentication for account logins. If access to the technologies is available via a single factor (e.g., a password), it is not secure.
- The provider should have comprehensive published security practices and policies.
- The provider should also offer detailed security monitoring of infrastructure elements and for DNS data. This monitoring should be performed regularly to ensure any changes made by an attacker are spotted quickly. When anomalous activity is detected, the provider should have a system of escalating alerts in place to notify technical staff.

As a general practice, it is also important to ask about support for *BCP 38.*[11] BCP 38 is a document that specifies the operational practices that providers should follow to reduce the amount of network routing fraud on the Internet. All network providers should support BCP38. In some exceptional cases, there may be reasons why BCP38 cannot be followed, but in the context of typical domain hosting organizations, these cases would be unusual and you should ask for detailed explanations.

4.3 Authoritative Name Service

Authoritative name service is how you tell the world that your domain name resolves to particular IP addresses, which mail server you are using for incoming mail, how your organization's namespace is laid out, etc. Whether you are going to set up your own authoritative name servers or you are going to pay a third-party vendor to host the authoritative name servers on your behalf, there are a few considerations to keep in mind:

- The best practice is to have multiple, distinct authoritative name servers on separate, geographically, and network-topologically distinct networks.
- Ensure that any name server hosting service fully supports DNSSEC, including uploading DNSKEY and/or DS records to your domain name registrar.
- Make sure there is good support for large-scale additions, modifications, or deletions of DNS data, including resource records and subdomains.
- Understand the measures used to protect against distributed denial of service attacks, regardless of whether you decide to operate your own name servers or set them up with a third party provider.

[11] See https://datatracker.ietf.org/doc/bcp38/

4.4 IPv6 Support

It is increasingly critical that the third-party hosting vendor supports IPv6 in its software and services. The Regional Internet Registries (RIRs), who are the top-level allocators of IP addresses, have produced numerous materials to help you make good procurement decisions related to services that make use of IP addresses. Among them:

- AFRINIC, the RIR for Africa, has an IPv6 guidebook for governments.[12]
- ARIN, the RIR for North America and parts of the Caribbean, has produced a 6-minute video explaining what IPv6 is and why it's important.[13]
- LACNIC, the RIR for Latin America, published a 12-step IPv6 deployment guide for governments and enterprises.[14]
- RIPE NCC, the RIR for Europe and parts of west Asia, has published an IPv6 requirements guide for ICT equipment.[15]

5 Summary

We have covered a lot of material in this guide. Again, not all vendors will be able to offer every one of the services we've listed here that we think are important. But the overarching messages we are hoping to convey are that:

- Security is important, and is a lot more than just a well-chosen password.
- DNSSEC support and IPv6 support should be a baseline requirement.
- Companies you work with should be committed to maintaining good reputations for mitigating abuse and handling abuse complaints.

12 See https://afrinic.net/guidebook-gov-ipv6
13 See https://youtu.be/bkLs5_geTM4
14 See https://www.lacnic.net/innovaportal/file/3635/1/10-12-steps-government-ipv6-v3.pdf
15 See https://www.ripe.net/publications/docs/ripe-554

Appendix: Procurement Checklist

Choosing a TLD Registry

- ❑ Supports DNSSEC
  Domain names registered in this TLD can be DNSSEC-signed
- ❑ Supports both IPv4 and IPv6
  Name server records of the TLD can be issued with both IPv4 and IPv6 addresses
- ❑ Offers registry lock
  Has a process to lock down records and requires out of band authorization to make changes to locked records
- ❑ Has a good reputation
  The TLD actively combats abusive domains registered in the TLD

Choosing a Domain Name Registrar

- ❑ Is an accredited or authorized registrar
  If a gTLD, is accredited by ICANN, and if a ccTLD, is authorized to offer domains
- ❑ Practices good cyber hygiene
  Requires multi-factor authentication for user account logins and web pages use HTTPS
- ❑ Supports DNSSEC
  Domain names can be DNSSEC-signed
- ❑ Allows domain names to be hosted by third-parties
  Supports just the registration of domain names and does not force you to host the domain name on their web servers
- ❑ Allows data export
  DNS data can be exported by your IT staff so you can easily transfer to a new registrar
- ❑ Supports both IPv4 and IPv6 addresses
  Name server records can be issued with both IPv4 and IPv6 addresses
- ❑ Has a good reputation
  Is proactive in preventing, detecting and mitigating abuse, and responding to complaints

Choosing a Third-Party Hosting Provider

- ❑ Supports both bulk subdomain management and modern DNS record types
  Can add, modify, or delete subdomains in bulk and add resource records like TLSA
- ❑ Has secure operations
  Multi-factor Authentication for user logins, published security practices and policies, proactively monitors DNS data, and supports BCP38
- ❑ Support for authoritative DNS services
  Geographically disparate name servers, good protection from attacks, and more
- ❑ Supports both IPv4 and IPv6 addresses
  Access to the provider's servers and name server updates support both IPv4 and IPv6