



VA Online Presence Management Guidelines

Purpose:

This document serves as the official policy for managing domain names used by the Department of Veterans Affairs (VA). It defines the rules, standards, and decision criteria that govern the acquisition and use of ".gov" domains, the structuring of VA-related subdomains and subdirectories in support of VA's brand consolidation vision and the 21st Century Integrated Digital Experience Act (21st Century IDEA).

Scope:

These guidelines apply to all VA staff, offices, programs, and partners involved in the creation, management, or oversight of any VA-related websites and online services.

Policy Guidelines:

1. Use of the va.gov domain

All public-facing VA websites and services must reside on the va.gov domain. If a rare case arises for considering an alternative .gov domain, the requester must provide for review a clear and compelling case that the domain is necessary to meet a need that the va.gov domain cannot and demonstrably better serves Veterans. Requests for non-va.gov domains must include documented justification grounded in user needs, legal requirements, or technical constraints.

2. Subdomains vs. subdirectories

VA entities must prioritize the use of subdirectories rather than creating new subdomains (e.g. onlinesafety.va.gov).

Decisions to use a subdomain will be based on technical constraints, unique nature of audience, distinct or independent nature of mission, and user experience. Specific criteria are documented on <https://design.va.gov/ia/domain-structure>.

Examples of acceptable subdomains:

Design.va.gov – used by VA's design system team to publish design standards, UI components, and front-end guidance for product teams.

Developers.va.gov – serves as the central platform for VA software developers to share code, access developer tools, and explore the agency's API catalog. It supports a technically distinct and developer focused mission separate from public-facing service

3. Authority to Request or Approve New Domains

The authority to request and approve new .gov domains is delegated by the Chief Information Officer (CIO) to the Chief Technology Officer (CTO). The CTO will rely on the Chief Architect and the Digital Experience Lead for guidance. These roles are responsible



for ensuring that all requests are consistent with this policy and in the best interests of Veterans and the VA enterprise. All requests for new top-level (non VA.gov) domains will be assessed by these delegated members, who will analyze the request and provide a recommendation to the Assistant Secretary for Information and Technology regarding allowing the new top-level .gov domain. The CIO holds decision rights for all new top-level VA .gov domains.

4. Authority to Request or Approve New Subdomains or Level 1 Subdirectories

The authority to request and approve new subdomains or Level 1 subdirectories is delegated by the Chief Information Officer (CIO) to the Chief Technology Officer (CTO) and the Digital Experience Lead. These roles are responsible for ensuring all requests are consistent with this policy, meet all standards, and are in the best interests of Veterans and the VA enterprise.

5. Oversight and Governance

The Web Governance Board will use these guidelines to review requests for new web initiatives.

In addition, the Office of the CTO is responsible for enforcing this policy and supporting its implementation. This includes limiting unnecessary domain proliferation, ensuring naming consistency, and maintaining an enterprise-wide information architecture that prioritizes the Veteran and family member experience.

Conclusion:

These guidelines serve as the authoritative policy for all VA domain decisions. Adherence ensures a unified, trustworthy, and user-centered digital presence, reduces duplication and confusion, and enables scalable web management across the enterprise. All new or revised VA web initiatives must comply with this policy.

Approval:

Sam Kaldawi
Chief Architect
Office of the Chief Technology Officer (OCTO)