Click to prove you're human

How to use USWDS If possible, enable HTTP/2 support on your server for dramatic performance gains. When using HTTP/2: What is HTTP/2? HTTP/2 is the next version of HTTP (described on Wikipedia), the protocol that powers the web. HTTP/2 was originally known as SPDY (described on Wikipedia), a protocol invented by Google that was safer, faster, and more efficient than HTTP 1.1. Once SPDY gained traction among browser and server makers, the Internet Engineering Task Force adopted it as the basis for HTTP/2. How it differs from HTTP 1.1 HTTP/2s biggest difference is its transmission of data. Rather than sending data in plaintext, HTTP/2 transfers messages using a binary format. This binary format allows for much faster transmission as it requires fewer bytes to transfer from server to client. This, combined with HTTP/2s new multiplexing feature, can significantly speed up website speed when downloading resources. Multiplexing is HTTP/2s ability to send data back and forth in parallel over one existing open connection. In HTTP 1.1 each resource (with a unique URL) requires a separate connection, and most clients limit the number of simultaneous connections to each domain. Additionally, if the server isnt configured to keep connections open after each request, each resource must go through a multi-step handshake process before transmission, further increasing its download time. HTTP/2 changes this by allowing multiple resources to be downloaded in parallel over a single connection. Another prominent feature of HTTP/2 is that, at least in practice, it strengthens security because browsers have only implemented HTTP/2 support for sites that are served over HTTPS. While the HTTPS handshake can add some loading time, you can reduce some of that by configuring HTTPS. Regardless, the dramatic performance gains from using HTTP/2 will likely outweigh any additional HTTPS overhead. For more information on HTTP/2, see High Performance Browser Networking. HTTP/2 and performance HTTP/2 changes how resources affect a pages download speed and how resources are downloaded from the server to the browser. Some performance improvement techniques are no longer relevant when switching from HTTP 1.1 to HTTP/2, such as domain splitting and file concatenation. Domain splitting One common performance improvement pattern for sites that require lots of resources (such as tiled web maps) is to split requests for resources over multiple domains. This effectively works around browser limits on the number of simultaneous requests per domain and allows more resources to be fetch in parallel. Under HTTP/2 this pattern effectively becomes an anti-pattern, and using CDNs or servers with different domains to serve assets is no longer necessary. Servers can stream many more requests simultaneously over a single HTTP/2 connection than over a browser-limited number of parallel HTTP 1.1 connections. Concatenation Concatenation is the process of combining similar file types into one file, often to reduce the number of HTTP requests necessary for a given page. Concatenating (or bundling) scripts and stylesheets is most common and easiest to automate, but its also possible to combine multiple images into a single image, or sprite (described on css-tricks.com), which can reduce both the number of HTTP requests and the total page weight by better leveraging image compression algorithms. Unlike domain splitting, concatenation is not necessarily an anti-pattern with HTTP/2. Under HTTP/2, its good practice to keep individual files small and ensure that resources are only served when needed. That being said, other factors can affect the the speed tradeoffs of individual resources. For example, when Khan Academy served over 300 individual JavaScript files to HTTP/2 users, they saw a degradation in performance due to less efficient compression over multiple files, and server delays related to reading each file from disk. For more information, see Khan Academys article and Smashing Magazines HTTP/2 guide. Generally speaking, organizing your resources into smaller, logical files rather than bundling them one large file offers the best performance over HTTP/2. The number of files that you can serve over HTTP/2 for a single URL without degrading performance depends heavily on the codebase and the server. We suggest keeping the number of files below 50 per URL, as that seems to be the point at which many servers suffer from having to read so many individual files from disk. How to upgrade to HTTP/2 Before upgrading, you should check to see if your server already supports HTTP/2. You can submit any public URL to this tool HTTP/2 Test, and it will tell you if thats the case. If not, read on! Upgrading to HTTP/2 requires that you have administrative access to either the server or CDN that hosts your website and its assets. If your site is on a CDN not directly under your control, here are instructions for enabling HTTP/2 on some of the most common CDNs: Cloudflare Amazon CloudFront How to speed up HTTPS There are several common techniques for improving HTTPS performance under both HTTP 1.1 and HTTP/2. Most of them require direct access to your sever(s) and/or hosting environment, and specific knowledge of the tools or platforms in use. The Igvita article, Optimizing nginx TLS time to first byte, describes how to improve HTTPS performance with nginx, but the techniques are applicable in other environments. Official websites use .gov A .gov website belongs to an official government organization in the United States. Secure .gov websites use HTTPSA lock (Locked padlock) or https:// means youve safely connected to the .gov website. Share sensitive information only on official, secure websites. The relevant laws and policies for delivering better digital services Understanding Section 508 of the Rehabilitation Act of 1973, Section 508 standards, and OMB M-24-08. Understanding Executive Order 14058 and OMB Circular A-11, Section 280 (2024). Understanding the 21st Century Integrated Digital Experience Act and OMB M-23-22. Understanding the DOTGOV Online Trust in Government Act and OMB M-23-10. Understanding Executive Order 13166, Attorney General memorandum, and Title VI of the Civil Rights Act. Understanding the Program Management Improvement Accountability Act and OMB M-18-19. This 2019 memorandum sets forth the federal governments Identity, Credential, and Access Management (ICAM) policy. Links to relevant laws, policies, and regulations for federal agencies. Learn how Federal Source Code Policy supports reuse and public access to custom-developed federal source code. Learn how to strengthen customer experience and service delivery within your federal agency. Learn how to implement Section 508, and strengthen and maintain your agencys commitment to digital accessibility. Learn how to implement the DOTGOV Online Trust in Government Act and understand how to register federal internet domain names. Learn how to strengthen and improve meaningful language access for all people in the U.S., regardless of the language they speak. The Digital Experience (DX) Council plays a critical role in coordinating governmentwide efforts and assisting agencies in delivering digital experiences that meet the publics needs and expectations. Guidance on meeting security requirements for federal websites. What is an Authorization to Operate? Before you use software in government, you need to make sure it is allowed. You should know what an ATO is, and when you need one. What do the control families of NIST 800-53 mean? Heres an overview of the control families that create the foundation of federal security compliance. Provides requirements and recommendations to support agency integration of digital accessibility into their missions and operations, helping government technology and information resources better serve a diverse public and federal workforce. M-23-07 updates the previous target dates described in M-19-21 to June 24, 2024. Provides guidance to all federal agencies on the acceptable use and registration of Internet domain names as required by the DOTGOV Online Trust in Government Act of 2020. This handbook aims to give CIOs important information needed to be a technology leader at their respective agency. Title IX of Public Law No. 116-260, 901-907 (DOTGOV Act of 2020), which outlines responsibilities, authorities, duties, strategies, and requirements related to the process of creating top-level .gov domains, authorizes the Cybersecurity and Infrastructure Security Agency (CISA) to manage the domain registration process for federal, state, local, tribal, and territorial governments. Harnessing Technology to Support Mission Continuity As defined in 21st Century IDEA, the Design System incorporates federal standards to improve federal websites and digital services. Guidance on how to measure customer experience, including questions on satisfaction and confidence and trust in section 280.7 The Office of Management and Budget (OMB) provided this guidance to implement the Government Paperwork Elimination Act (GPEA). GPEA required Federal agencies, by October 21, 2003, to allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically, when practicable, and to maintain records electronically, when practicable. This memo dated October 6, 2011, from the Federal CIO to the CIOs of Executive Departments and Agencies, mandates that agencies are to begin leveraging externally-issued credentials, in addition to continuing to offer federally-issued credentials. View or download the OMB Memo on Testing and Simplifying Federal Forms Openness in government strengthens our democracy, promotes the delivery of efficient and effective services to the public, and contributes to economic growth. As one vital benefit of open government, making information resources easy to find, accessible, and usable can fuel entrepreneurship, innovation, and scientific discovery that improves Americans lives and contributes significantly to job creation. This final rule provided a new policy for the .gov domain that will be included in the Federal Management Regulation. The Digital Millennium Copyright Act (DMCA) is a United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO). United States trademark law is mainly governed by the Lanham Act. The head of the agency delegates to the CIO a number of information security responsibilities. The CIO in turn designates a senior agency information security officer. The World Wide Web (WWW) is a system for exchanging information over the Internet. At the most basic level, the Web can be divided into two principal components: Web servers, which are applications that make information available over the Internet (in essence, publish information), and Web browsers (clients), which are used to access and display. This memorandum provides updated instructions for agency reporting under the Federal Information Security Management Act of 2002 (FISMA). Subchapter B of the CFR specifies polices for federal agencies records management programs relating to proper records creation and maintenance, adequate documentation, and records disposition. View Code of Federal Regulations (CFR), Parts 1220-1238 Related Links NARA guidance for implementing Section 207(e) of the E-Gov Act NARA guidance on managing web records NARA Bulletin 2014-02 Guidance The Rule imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. This Appendix describes agency responsibilities for implementing the reporting and publication requirements of the Privacy Act of 1974, 5 U.S.C. 552a. This Memorandum requires Federal agencies to take specific steps to protect individual privacy whenever they use third-party websites and applications to engage with the public. The No FEAR Act requires a Federal agency to post on its public Web site summary statistical data pertaining to complaints of employment discrimination filed under 29 CFR part 1614 by employees, former employees and applicants for employment. This memorandum provides Resource Management Offices and PMA Initiative Leads with instructions for preparing for the quarterly PMA scorecard meetings to discuss agencies status and progress in implementing the PMA for the period January 1, 2008 through March 31, 2008. Executive Order 13571 requires agencies that provide significant services directly to the public to identify and survey their customers, establish service standards and track performance against those standards, and benchmark customer service performance against the best in business. Memo M-11-24 is guidance to Implement Executive Order 13571. On January 21, 2009, the President issued a memorandum calling for the establishment of a system of transparency, public participation, and collaboration. The memorandum required an Open Government Directive to be issued by the Director of the Office of Management and Budget (OMB), instructing executive departments and agencies to take specific actions implementing the principles The Section 508 Standard for Electronic and Information Technology requires that when a federal agency shares information digitally, individuals with disabilities seeking information or services from a federal agency, must have access to and be able to use the information and data, unless an undue burden would be imposed on the agency. The Plain Language Action and Information Network (PLAIN) put together these federal guidelines to help implement the Plain Language Act of 2010. The purpose of the E-Government Act of 2002 includes improving the management and promotion of electronic government services and processes, and establishing a framework of measures that require using Internet-based information technology to improve citizen access to government information and services. The Web Content Accessibility Guidelines (WCAG) documents explain how to make web content more accessible to people with disabilities. Web content generally refers to the information in a web page or web application, including: natural information such as text, images, and sounds code or markup that defines structure, presentation, etc. View the Web Accessibility Guidelines Components Banners identify official websites of government organizations in the United States. They also help visitors understand whether a website is official and secure. Passed WCAG 2.1 AA About the banner component Note: Banners and identifiers are core components. We recommend using both core components on most sites. Together, they are the most recognizable and standardized design elements of a government site. You should use the banner to identify your site as an official government site. The banner explains how to identify an official .gov or .mil domain and that these sites have secure HTTPS connections. Using the banner component is the best way to assure visitors that theyre connected to an official site. Most government sites should use the banner, but some should not use the banner. Do NOT use the banner on non-government domains such as a .com or .org. If you are unable to update to USWDS 2.8.0 (described on GitHub) or higher but still want to include the new language in your banner, we recommend editing your content to the language outlined in the component preview. Default banner This is the default banner. USWDS 3.0.0 through 3.12.0 only provide this version. Official websites use .govA .gov website belongs to an official government organization in the United States. Secure .gov websites use HTTPSA lock (Locked padlock icon) or https:// means youve safely connected to the .gov website. Share sensitive information only on official, secure websites. Official websites use .milA .mil website belongs to an official U.S. Department of Defense organization. Secure .mil websites use HTTPSA lock (Locked padlock icon) or https:// means youve safely connected to the .mil website. Share sensitive information only on official, secure websites. Los sitios web oficiales usan .govUn sitio web .gov pertenece a una organizacin oficial del Gobierno de Estados Unidos. Los sitios web seguros .gov usan HTTPSUn candado (Locked padlock icon) o https:// significa que usted se conect de forma segura a un sitio web .gov. Comparta informacin sensible slo en sitios web oficiales y seguros. Los sitios web oficiales usan .milUn sitio web .mil pertenece a una organizacin oficial del Departamento de Defensa de EE. UU. Los sitios web seguros .mil usan HTTPSUn candado (Locked padlock icon) o https:// significa que usted se conect de forma segura a un sitio web .mil. Comparta informacin sensible slo en sitios web oficiales y seguros. .gov domains An official website of the United States government Heres how you know Heres how you know Official websites use .govA .gov website belongs to an official government organization in the United States. Secure .gov websites use HTTPSA lock (Lock Locked padlock icon) or https:// means youve safely connected to the .mil website. Share sensitive information only on official, secure websites. .gov domains (Spanish) Un sitio oficial del Gobierno de Estados Unidos As es como usted puede verificarlo As es como usted puede verificarlo Los sitios web oficiales usan .govUn sitio web .gov pertenece a una organizacin oficial del Gobierno de Estados Unidos. Los sitios web seguros .gov usan HTTPSUn candado (Lock Locked padlock icon) o https:// significa que usted se conect de forma segura a un sitio web .mil. Comparta informacin sensible slo en sitios web oficiales y seguros. .gov domains An official website of the United States government Heres how you know Heres how you know Official websites use .govA .gov website belongs to an official government organization in the United States. Secure .gov websites use HTTPSA lock (Lock Locked padlock icon) or https:// means youve safely connected to the .mil website. Share sensitive information only on official, secure websites. .gov domains (Spanish) Un sitio oficial del Gobierno de Estados Unidos As es como usted puede verificarlo As es como usted puede verificarlo Los sitios web oficiales usan .govUn sitio web .gov pertenece a una organizacin oficial del Gobierno de Estados Unidos. Los sitios web seguros .gov usan HTTPSUn candado (Lock Locked padlock icon) o https:// significa que usted se conect de forma segura a un sitio web .mil. Comparta informacin sensible slo en sitios web oficiales y seguros. Guidance This default banner was the only variant available until USWDS 13.3.0. The primary difference is that the default is more customizable but can add steps when updating USWDS versions. To identify as an official government site. Most government sites should use the banner, though non-federal government sites will need to change the text to be more accurate. If you dont use a .gov/.mil domain and HTTPS. The Design Systems banner text identifies .gov and .mil domains and HTTPS as indicators that a website is an official government website. Use this banner only if your site uses both the proper top-level domain (TLD) and HTTPS. Any time it would be misleading. The banner should be used to reduce confusion. Avoid using the banner on any site meant only for testing or otherwise not meant to be identified as an official government website. Use the provided text without customization. The banner is most effective as an identifier and a learning tool when its message is consistent across government sites. With only a few exceptions (described in our Implementation guidance), sites should use the top-level domain (TLD)-appropriate text provided, unaltered. Use the Spanish version of the banner for Spanish-language websites. Use the version appropriate to your websites top-level domain (TLD). If your project uses a .mil top-level domain, use the .mil banner text. Show the banner on every page. Use the banner at the top of every page of a site. It can be confusing or misleading if it appears on some pages and not others. Avoid distraction. The banner should appear on every page of your site. Choose background colors that fit with your site theme, and avoid color combinations that draw excessive attention to the banner. Keep the text up to date. Use the most current version of the banner. Use aria-label to give the banner a useful name. Our default markup uses aria-label="Official website of the United States government" or aria-label="Un sitio oficial del Gobierno de Estados Unidos" to distinguish the banner header from the main header. The banners accordion uses JavaScript to set the aria-hidden value of its content area. To ensure your content remains accessible in the event the JavaScript does not load or is disabled, you should not set aria-hidden="true" on usa-banner__content. Some .gov websites dont represent the federal level of the U.S. government. These sites should adapt the An official website of the United States government and Official websites use .gov sections to use more accurate language specific to the site. Some .mil websites dont belong to an official U.S. Department of Defense organization. These sites should adapt the Official websites use .mil section to use more technically accurate language: A .mil website operates under the approval of the U.S. Department of Defense. The banner should directly follow the skipnav component. Set the banner background color with $theme-banner-background-color. Banner text color will update automatically. Note: We recommend loading uswds-init.js when using banner, header, or modal components to assist in preventing flashes of unstyled content (FOUC) as well as cumulative layout shift (CLS). This small JavaScript file (less than 1 KB minified) helps the browser know if the USWDS JavaScript library is loading properly. To add uswds-init to your site, simply copy uswds-init.js into your site assets from either the uswds-core/src/js package or the dist/js directory in the downloadable package. Then, reference the file in the of your HTML files. Alternatively, you can inline its contents directly into a tag in your HTML files.A banner variant that may be easier for some teams to implement and keep up to date. Web Component VariantWeb Component Variant (Spanish)Web Component Variant (.mil domain, customized) A .mil website belongs to an official U.S. Department of Defense organization. Web Component Variant Web Component Variant (Spanish) Web Component Variant (.mil domain, customized) A .mil website belongs to an official U.S. Department of Defense organization. USWDS 3.13.0 introduces an HTML Web Component variant of banner. Both options exist in components/banner, as well as in dist/components/usa-banner. We recommend most implementations use the compiled version in dist at this point, though this version is less customizable. Use the Web Component variant of the banner anywhere you would use the default banner. The Web Component variant may be easier to add to your site, but it is also less customizable than the default banner. If you need more customizability than the Web Component variant of the banner offers. Some .gov websites dont represent the federal level of the U.S. government. These sites should adapt the An official website of the United States government and Official websites use .gov sections to use more accurate language specific to the site. Some .mil websites dont belong to an official U.S. Department of Defense organization. These sites should adapt the Official websites use .mil section to use more technically accurate language: A .mil website operates under the approval of the U.S. Department of Defense. The banner should directly follow the skipnav component. We realize this documentation wont cover all use cases, build environments, or tooling. If you have questions, you can ask USWDS community members in our GitHub discussions or Slack channel, or contact us directly at uswds@gsa.gov. Well be expanding this documentation in the future and your questions and feedback will help us understand what you need to get started with this variant and its implementation. Web Component Settings Attributes Attribute Description lang The element's language. Defaults to en label The custom aria label users can override. tld The top level domain for the site. Defaults to .gov Slots Slot Description banner-text The text for official government website text. banner-action Action text label "Here's how you know." domain-heading Heading text for the domain section. domain-text Body text for domain section. https-heading Heading for HTTPs section. https-text Body text for HTTPs section. Custom Properties Custom Property Description --theme-banner-text-color --theme-banner-background-color Sets banner background color. --theme-banner-font-family --theme-banner-link-color Sets the default link/button color. --theme-banner-link-hover-color Sets the default link/banner hover color. --theme-banner-chevron-color Sets the default chevron color. Note: As this is the first Web Component shipping in USWDS, we are still working on the best way to document its usage. We want to hear from users about challenges with adding this component to your projects. Please let us know what works, what doesnt, and what additional documentation might be helpful in this discussion thread. Variable Description $theme-banner-background-color Background color of the banner and its content. $theme-banner-font-family The font family of the banner. $theme-banner-link-color The color of banner link. Add the link color and the system will generate the hover state. Default uses the default link settings calculated from your background color. $theme-banner-max-width Maximum width of the banner content. Variant Description An HTML Web Component version of Banner. Easier to implement and update but potentially harder to customize. See above for details. The USWDS team did 14 tests based on WCAG 2.1 AA success criteria. Clear and consistent use of .gov and .mil domains is essential to maintaining public trust. Follow these domain security best practices to ensure a safe experience for your organization and your users. Learn what steps you can take to avoid security certificates from expiring during a lapse in operations. Government websites with official domain names help build trust with the public. A .gov domain instantly conveys credibility and trustworthiness, and proper domain management practices ensure that your website is secure and accessible. Learn how to implement the DOTGOV Online Trust in Government Act and understand how to register federal internet domain names. If youre moving to .gov from another top-level domain, like .com, .org, or .us, here are some best practices to help you plan that transition. Provides guidance to all federal agencies on the acceptable use and registration of Internet domain names as required by the DOTGOV Online Trust in Government Act of 2020). Title IX of Public Law No. 116-260, 901-907 (DOTGOV Act of 2020), which outlines responsibilities, authorities, duties, strategies, and requirements related to the process of creating top-level .gov domains, authorizes the Cybersecurity and Infrastructure Security Agency (CISA) to manage the domain registration process for federal, state, local, tribal, and territorial governments. Official websites use .gov A .gov website belongs to an official government organization in the United States. Secure .gov websites use HTTPSA lock (Locked padlock) or https:// means youve safely connected to the .gov website. Share sensitive information only on official, secure websites. Understand how digital services impact trust in government. The federal website standards help agencies provide high-quality, consistent digital experiences for everyone. They cover common visual technical elements and reflect user experience best practices. Trusted digital services meet customer expectations, and they are easy to find, understand, and use. Understand how digital services impact trust in government. Delivering a digital-first public experience is a significant opportunity to improve the lives of millions by making it easier to access the information and services they use and count on each and every day. A list of key considerations and practical actions you can take to earn trust with users. Host your site on a .gov or .mil domain to assure users its an official government site. Trust is built up with good experiences, and broken with bad ones. Build sites that build trust by considering user needs, respecting peoples time, and avoiding customer experience pitfalls. Learn how to implement 21st Century IDEA to design and deliver better websites and digital services. A .gov domain instantly conveys credibility and trustworthiness, and proper domain management practices ensure that your website is secure and accessible. Learn how to strengthen customer experience and service delivery within your federal agency. Introductory guidance on implementing privacy protections for users of federal websites. Guidance on how to build government websites that people can trust. A more simple, seamless, and secure customer experience for the American public. Official websites use .gov A .gov website belongs to an official government organization in the United States. Secure .gov websites use HTTPSA lock (Locked padlock) or https:// means youve safely connected to the .gov website. Share sensitive information only on official, secure websites. Ideas and resources for delivering better digital experiences Explore fundamental best practices for delivering federal websites and digital services. The federal website standards help agencies provide high-quality, consistent digital experiences for everyone. They cover common visual technical elements and reflect user experience best practices. Understand how to adopt the design system incrementally and build better digital experiences. The Digital Analytics Program (DAP) offers advanced, easy web analytics for federal agencies. All public-facing federal websites can participate. A checklist of requirements for people who are presenting at a Digital.gov event. If youre moving to .gov from another top-level domain, like .com, .org, or .us, here are some best practices to help you plan that transition. Founded on three key pillars of successful cloud adoptionsecurity, procurement, and workforcethe Cloud Smart strategy includes 11 action items from the Chief Information Officers (CIO) Council. Innovative work, news, and ideas from people and teams in government Components The identifier communicates a sites parent agency and displays agency links required by federal laws and policies. Passed WCAG 2.1 AA About the identifier component Default domain.gov An official website of the <Parent agency> About <Parent shortname> Accessibility statement FOIA requests No FEAR Act data Office of the Inspector General Performance reports Privacy policy Looking for U.S. government information and services? Visite USAGov en Espaol Multiple parents and logos domain.gov An official website of the <Parent agency> and the <Other agency> About <Parent shortname> Accessibility statement FOIA requests No FEAR Act data Office of the Inspector General Performance reports Privacy policy Looking for U.S. government information and services? Visite USAGov en Espaol No logos domain.gov An official website of the <Parent agency> About <Parent shortname> Accessibility statement FOIA requests No FEAR Act data Office of the Inspector General Performance reports Privacy policy Looking for U.S. government information and services? Visit USA.gov Taxpayer disclaimer (Spanish) domain.gov Un sitio web oficial de <Parent agency> . Producido y publicado con dinero de los contribuyentes de impuestos. Acerca de <Parent shortname> Declaracin de accesibilidad Solicitud a travs de FOIA Datos de la ley No FEAR Oficina del Inspector General Informes de desempeo Poltica de privacidad Necesita informacin y servicios del Gobierno? Visit USA.gov Default (Spanish) domain.gov Un sitio web oficial de <Parent agency> Acerca de <Parent shortname> Declaracin de accesibilidad Solicitud a travs de FOIA Datos de la ley No FEAR Oficina del Inspector General Informes de desempeo Poltica de privacidad Necesita informacin y servicios del Gobierno? Visit USA.gov Multiple parents and logos (Spanish) domain.gov Un sitio web oficial de <Parent agency> y <Other agency> Acerca de <Parent shortname> Declaracin de accesibilidad Solicitud a travs de FOIA Datos de la ley No FEAR Oficina del Inspector General Informes de desempeo Poltica de privacidad Necesita informacin y servicios del Gobierno? Visit USA.gov Taxpayer disclaimer domain.gov An official website of the <Parent agency> . Produced and published at taxpayer expense. About <Parent shortname> Accessibility statement FOIA requests No FEAR Act data Office of the Inspector General Performance reports Privacy policy Looking for U.S. government information and services? Visite USAGov en Espaol Guidance To identify the highest-level agency associated with a site or service. The identifier is a complement to the USWDS banner. Use the identifier to tell users what parent agency is responsible for your website. Consider the parent agency the highest-level agency associated with a site or service. If your site is the primary site associated with an agency, you can still use the identifier. To display links required by federal laws and policies. The identifier includes links required on all government sites. Any time it would be misleading. The identifier should be used to reduce confusion. Avoid using the identifier on any site meant only for testing or otherwise not meant to be identified as an official government website. Redundant content. Dont add the identifier without removing any duplicate links from your existing site footer. Favor the common links and content in the identifier over any equivalent content in your site footer. Use the identifier component for required links. If your site already includes the federally required links in its site footer, remove them in favor of the links in the identifier. This assures that site visitors find the required links in a consistent location from site to site. Consider the parent agency the highest-level agency associated with a site or service. In some cases, your site may not have a parent agency. If your site is the primary site for your agency, use your agency name in place of [Parent Agency]. For example, [agency.gov] An official website of [Agency]. Display the parent agency logo, not the product logo. The identifier is meant to identify a websites parent agency as a complement to the site footer. Site-specific logos, like a product logo, should be in the site footer, not the identifier. You may omit the logo in the identifier if it is redundant with the agency logo in your sites footer. Display multiple parents and logos in hierarchical order. If a site has more than one parent agency, you may display a reference and a logo for each parent in hierarchical order, highest first. For example, An official website of [Grandparent Department] and [Parent Agency]. Avoid distraction. The identifier appears on every page of your site. Choose background colors that fit with your site theme and avoid color combinations that draw excessive attention to the identifier. Keep the text up-to-date. Use the most current version of the identifier. Use proper landmarks for each identifier section. Each identifier section should be either a section or a nav, and include an appropriate aria-label property. Add an alt attribute to each logo image. Use [Agency shortname] logo as the alt text for each logo image you add. Use image role for any SVG images. Use role="img" with any SVG logo image. Except where noted, use the entire component without deletions or additions. With rare exceptions, if you use the identifier, include the entire identifier. That is, dont delete sections or required links or change any link text beyond the customizations mentioned in the implementation section. Use a background color darker than that of the footer. Anchor the identifier to the bottom of the page and distinguish it from other site content by adding a background color that is darker than the footer. Use primary or base family background colors of grade 80 or higher, or black. Use an SVG logo if possible. Ensure the logo is high resolution. We recommend using the SVG version of any logo if you have one. Otherwise, use an image thats at least 120 pixels tall. Use logos intended for dark backgrounds if possible. The identifier has a dark background. If your agency has a version of its logo intended for dark backgrounds, use that version. Update the required links to point to the proper URLs. The identifier includes links required of any federal website, and these links are specific to a department, agency, or website. Weve linked each section below to the guidance on Digital.gov to provide further context. About [Official parent agency acronym]: Update the link text to include the parent agencys official acronym. Link to the About page of your parent agencys principal website. If your site includes multiple parents, include only the organization highest in the hierarchy in this link. Example: Accessibility statement: Link to your website or services accessibility statement, or to your parent agencys accessibility statement if your website or service does not have its own. Example: FOIA requests: Link to a page that includes information about how the public can request information under the Freedom of Information Act on your parent agencys principal website. Example: No FEAR Act data: Link to the Equal Employment Opportunity Data Posted Pursuant to the No Fear Act page on your parent agencys principal website. Example: Office of the Inspector General: Link to your parent agencys Office of the Inspector General. Example: Performance reports: Link to a Budget and Performance page that includes the parent agencys strategic plan among other financial and performance documentation. Example: Privacy policy: Link to the Privacy page most specific to your website. For example, if both your product website and your parent agencys principal website have privacy pages, link to your product websites privacy page here. Example: Use the Spanish version for Spanish-language sites. If you have an official Spanish-language website, use the Spanish version of the identifier. Duplicate the logo element if using multiple logos. If youre using multiple logos, duplicate the usa-identifier__logo element and link the image to your image source. If applicable, include any taxpayer disclaimer after the standard text. If the organization must provide a taxpayer expense disclaimer, include it following the Official website text, as a separate sentence. For example, An official website of [Department]. Produced and published at taxpayer expense. Variable Description $theme-identifier-background-color The background color of the identifier. Use a color of grade 80 or higher, darker than the section that precedes it. $theme-identifier-font-family The font family of the identifier. $theme-identifier-identity-domain-color The color of your domain text in the identifier masthead. This should be grade 20-30 in the same family as the $theme-identifier-background-color. $theme-identifier-max-width The maximum width of the content within the identifier. Use the same max-width as your site footer. $theme-identifier-primary-link-color The color of the links in the masthead section. Default uses either the standard or reverse link color set with $theme-link-color and $theme-link-reverse-color. $theme-identifier-secondary-link-color The color of the links in the required links section. This should be grade 20-30 in a gray family. This component has no variants. Accessibility test status The USWDS team did 16 tests based on WCAG 2.1 AA success criteria. Learn more on the identifier accessibility tests page. Package Package usage: @forward "usa-identifier"; Dependencies: uswds-fonts, uswds-core Latest updatesMeaningful code and guidance updates are listed in the following table: Date USWDS version Affects Breaking Description 2024-11-07 N/A No Added clarification on parent agency. We added guidance to cover cases where a site has no higher-level agency. More information: uswds-site#2591 2024-10-04 3.9.0 No Updated the USA.gov link in Spanish versions of the identifier. The link text now reads Visite USAGov en Espaol and the link url is now . More information: uswds#5892 2024-08-13 N/A No Added WCAG compliance tag and accessibility test status section. More information: uswds-site#2754 2024-05-31 3.8.1 No Fixed a bug that mistakenly added the English word An to Spanish variants in the component preview. More information: uswds#5857 2023-11-09 3.7.0 No Updated the screen reader readout in English versions of the component. When read out on a screen reader, the statement An official website of [Agency name] can sound like UNofficial website of [Agency name]. Users should update their markup to improve the screen reader experience. More information: uswds#5491 2023-06-09 3.5.0 Breaking Breaking Updated Accessibility statement link text. Updated the identifier to use the text Accessibility statement (EN) / Declaracin de accesibilidad (ES) for the required link to an accessibility statement. More information: uswds#5278 2023-06-09 3.5.0 No Updated Accessibility statement link guidance. Updated and clarified the identifier guidance for accessibility statements. We also improved the accessibility statement example links. More information: uswds-site#2097 2022-10-19 3.2.0 Breaking Breaking Used valid element for identitys aria-label. We updated the identity section of the identifier to use a section instead of a div so its aria-label will apply to a valid element. More information: uswds#4964 2022-04-28 3.0.0 Breaking Breaking Updated to Sass module syntax and new package structure. More information: uswds#4656 2021-03-17 N/A No Added identifier guidance and documentation. More information: uswds-site#1180 Official websites use .govA .gov website belongs to an official government organization in the United States. Secure .gov websites use HTTPSA lock (Locked padlock icon) or https:// means youve safely connected to the .gov website. Share sensitive information only on official, secure websites.

Polynomial functions graph. Domain of a polynomial. Domain for polynomial functions.

- http://cancercareresearch.com/userfiles/file/fixapi.pdf
- past tense live worksheet for class 3
- what is hidden in the vatican
- best high school cheers
- xehuruwetu
- hitocope
- speed hack for nitro type