EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

September 22, 2023

M-23-22

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: SHALANDA D. YOUNG

SUBJECT: Delivering a Digital-First Public Experience

I. INTRODUCTION

This memorandum provides guidance to agencies on how to design and deliver websites and digital services to the public and to assist agencies as they continue to implement the 21st Century Integrated Digital Experience Act[1] (21st Century IDEA). It summarizes relevant statutory requirements, clarifies policy requirements, and expands best practices for agency websites and digital services. This memorandum rescinds Office of Management and Budget (OMB) Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services* (Nov. 8, 2016), and supersedes any guidance provided in the Digital Government Strategy, *Digital Government: Building a 21st Century Platform to Better Serve the American People*, released by OMB in 2012.

Each year, the Federal Government provides information, services, benefits, and programs to more than 400 million individuals, families, businesses, and organizations. The majority of the public accesses Federal information and services online and increasingly from mobile devices.[2] Because digital channels are now the primary way the public interacts with the Federal Government, executive agencies must design and develop websites and digital services to meet the public's expectations for high-quality digital experiences that are simple to use, seamless across journeys, and secure by design to improve customer experience, satisfaction, and trust.

To ensure the Federal Government is meeting the needs of all people, the 21st Century IDEA directs agencies to maximize the number of Federal services available to the public in a digital format and establishes or reiterates requirements for accessibility, design, usability, security, and overall customer experience of Federal websites and digital services. The

[1] Pub. L. No. 115-336, the 21st Century Integrated Digital Experience Act.
[2] As measured via the Digital Analytics Program (https://analytics.usa.gov/), as of the publication of this memo.

implementation guidance for the 21st Century IDEA contained in this memorandum builds on previous efforts to create a digital government by helping executive agencies further harness user-centered design and agile delivery practices to provide integrated digital experiences and interactions across agencies, services, and channels.

II. SCOPE AND APPLICABILITY

Except as otherwise provided, this memorandum applies to all executive agencies ("agencies") as defined in 5 U.S.C. § 105 and applies to agency websites and digital services, including web applications and mobile applications, that: (1) are maintained by an agency directly or by a contractor or other entity on behalf of an agency; and (2) are intended for use by the public. Agencies are also encouraged to apply the requirements of this memorandum to internal-facing websites and digital services to the greatest extent practicable. This memorandum does not apply to third-party websites or digital services, such as social media sites, that are designed to facilitate online sharing of text or other media among communities of users, and that are used by an agency for that purpose.

A. Definitions

For the purposes of this memorandum, the following definitions are applicable:

1. "Customer" means any individual, business, or organization (such as a grantee or State, local, or Tribal entity) that interacts with an agency or program, either directly or through a Federally-funded program administered by a contractor, nonprofit, or other Federal entity.[3]
2. "Digital form" means a web application that has the capability to capture, validate, submit, and process structured information digitally and in an automated manner.
3. "Digital service" means a transactional service (e.g., online form, account management tool) or an informational service that is delivered over the internet across a variety of platforms, devices, and delivery mechanisms (e.g., mobile applications, text/SMS).
4. "Mobile application" or "native mobile application" means a software application designed and developed to be used on a mobile device (such as a smart phone or tablet) that uses the mobile device's operating system (e.g., Apple iOS, Google Android). This does not include websites and web applications that are optimized for mobile devices and are only accessed using a web browser on a mobile device.
5. "Public-facing" or "customer-facing" means intended to be accessed and used by a member of the public or a customer. By contrast, "internal-facing" means intended to be accessed and used by Federal Government employees or contractors on behalf of an agency.
6. "User" means any individual that interacts with a website or a digital service, often to complete a task or transaction.

[3] *See* OMB Circular No. A-11, § 280, "Managing Customer Experience and Improving Service Delivery."

7. "Web-based application" or "web application" means a software program that is accessible using a web browser.[4]
8. "Website" means a group of globally accessible interlinked web pages under a unique host name that is accessible using a web browser.

III. DELIVERING A DIGITAL-FIRST PUBLIC EXPERIENCE

A. Requirements for Websites and Digital Services

Federal websites and digital services serve agencies' missions and help users find the information and support they need. Agencies should ensure their websites, including web applications, digital services, and mobile applications, conform to the requirements and principles described below to design and deliver a high-quality, integrated digital experience that is simple, seamless, and secure across agencies for all users.

1. Accessible to People of Diverse Abilities

The Federal Government serves people of all abilities. In designing their websites and digital services, agencies must strive from the start to maximize access and usability so the widest possible range of people may reach and interact with the government through its websites and digital services.

- **Design accessible experiences:** Agencies should design websites and digital services to be usable by all people, including those with disabilities, without the need for adaptation or specialized design, to the greatest extent possible.
- **Follow accessibility standards:** Agencies subject to Section 508 of the Rehabilitation Act of 1973 must make electronic and information technology accessible to people with disabilities in accordance with statute and must comply with accessibility standards as specified by Section 508.[5] In addition to the accessibility standards required by Section 508, agencies should apply the most current Web Content Accessibility Guidelines

[4] All web applications are a website, but not all websites constitute a web application. The term "website" should be read to apply to websites (including web applications); however, when the term "web application" is used then the requirements may only be appropriate for web applications. A website or a web application is typically designed to be read or used by a human. The term "web service" is occasionally used elsewhere. A web service is a specific type of web application (or web application component) that uses a standardized format like XML to interact with other web applications over the internet. A web service is often designed to be machine-readable and used for applications to interact with each other. Agencies should be aware of the distinctions between web sites, applications, and services when attempting to apply the principles of this memorandum to web services, since it may be technically inappropriate or technically unfeasible.

[5] 29 U.S.C. § 794d; *see* 36 C.F.R. part 1194. The scope of Section 508 differs from the scope of this memorandum. For example, Section 508 applies broadly to "electronic and information technology," not just websites and digital services. See 29 U.S.C. § 794d(a)(1)(A). Agencies are responsible for determining the extent of their responsibilities under Section 508 and the associated accessibility standards.

(WCAG) published by the World Wide Web Consortium (W3C) to websites and web applications, where possible.[6]

- **Test for accessibility:** Agencies should incorporate accessibility testing into website updates and release processes to address issues detected in testing before code is released. Accessibility testing should include automated scanning, manual testing of websites, and usability testing with people with disabilities, as well as testing with users of adaptive technologies. Because automated testing tools are limited and can only detect some accessibility issues, agencies should incorporate manual testing of websites and digital services to cover all accessibility requirements.
- **Conduct inclusive research:** Agencies should incorporate the needs of individuals with disabilities into the design and development of websites and digital services, and should include individuals with disabilities in usability testing of new tools or features. Considering the needs of individuals with disabilities early and often through user research demonstrates a commitment to accessibility that goes beyond baseline compliance.
- **Promote accessibility and welcome feedback:** Agencies should develop and publish an accessibility statement that provides a public feedback mechanism to contact the agency in case a user encounters problems and wishes to seek assistance or report an accessibility issue.[7]

2. Consistent Visual Design and Agency Brand Identity

Members of the public depend on the Federal Government for authoritative and trustworthy information and services that they cannot get from any other entity. It is critical that the public knows when they are accessing information from the Federal Government, utilizing a Federal Government service, or communicating with someone who represents the Federal Government.

Trust in Federal Government information and services depends on the public's ability to distinguish between government and non-governmental entities and information. Clear and consistent use of an agency's brand identity and the visual design of its websites and digital services helps the public to identify official Federal Government entities, information, and services. This includes consistent and standardized use of everything that comprises the look and feel of an agency's product or service (such as a logo or seal, color palette, typeface, imagery, voice and tone, or product or service name). Design systems are tools for standardizing and maintaining brand identity and ensuring a consistent look and feel across channels, including websites and digital services.

---

[6] *See* World Wide Web Consortium (W3C) Accessibility Standards (https://www.w3.org/WAI/standards-guidelines/). As of the publication of this memo, the most current version of the Web Content Accessibility Guidelines (WCAG) would be 2.1, with Web Content Accessibility Guidelines (WCAG) 2.2 pending release.
[7] *See* OMB's "Strategic Plan for Improving Management of Section 508 of the Rehabilitation Act" (Jan. 24, 2013), https://obamawhitehouse.archives.gov/sites/default/files/omb/procurement/memo/strategic-plan-508-compliance.pdf.

- **Use the United States Web Design System:** Agencies should use the United States Web Design System (USWDS) to ensure a consistent appearance across public-facing websites and digital services. All public-facing websites and digital services must comply with the Federal website standards[8] published by the Technology Transformation Services of the General Services Administration (GSA) which incorporate the USWDS.[9]
- **Establish and maintain agency brand identities:** Agencies are responsible for establishing and maintaining appropriate brand identities (e.g., use of an agency's seal or logo) for themselves (or their individual components, offices, or programs)[10] and their respective websites and digital services. Agencies should not establish unnecessary brand and product identities, or multiple uncoordinated identities, that could create public confusion (such as using an internal-facing project or program name for the name of a public-facing digital service).
- **Apply agency brand design consistently:** Agencies should ensure that websites and digital services use appropriate brand identity in a consistent manner, including when an agency uses a third-party website or web application (such as a social media platform) to communicate.[11] Agency websites and digital services should have a cohesive, consistent look and feel that is aligned with agency design and branding guidelines. Agencies should establish internal control processes to ensure that all public-facing websites and digital services are checked for consistency prior to public release.
- **Centralize visual design and brand identity resources:** Agencies should maintain a design page (e.g., [agency].gov/design or design.[agency].gov) that centralizes information about the agency's visual design and brand identity standards with relevant policies and guidelines on how to use various design elements (e.g., logos, seals, emblems, insignia, name, color specifications, typography, imagery) to ensure the design standards are used appropriately and consistently within and across the agency.
- **Use a government domain name:** Agencies generally must use a .gov or .mil domain name for public-facing websites and digital services that are used for official communication.[12] Agencies may use third-party services whose domain names do not end in .gov or .mil for official communications when doing so is necessary to effectively interact with the public. Examples of such third-party services include social media services, source code collaboration, and vulnerability disclosure reporting systems. When utilizing third-party services for official communication, agencies should use appropriate brand identity as well as use and expose a .gov or .mil email address to verify for the

[8] 21st Century IDEA, § 3(e).
[9] See General Services Administration, U.S. Web Design System: Federal Website Standards, https://designsystem.digital.gov/website-standards/.
[10] Agencies, departments, components, offices, or programs may establish independent organizational brands, as appropriate. However, all public-facing websites and digital services within a single organization should use the same brand identity and visual design. When an organization establishes an independent brand, agency-led reviews or other processes should be conducted at the organizational level that established the brand, using such internal controls to ensure the brand is consistently applied prior to public release.
[11] *See* OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*.
[12] *See* OMB Memorandum M-23-10, *The Registration and Use of .gov Domains in the Federal Government*.

public which entity is communicating or providing the underlying information or service.[13]

- **Understand user perception:** Agencies should conduct customer and user research, qualitatively and quantitively, to better understand their customers' and users' interpretations and understanding of their brand and other trusted elements of their individual components, offices, or programs across channels, especially for websites and digital services, email, text/SMS, and social media, because these are the primary channels the public uses to engage and interact with government online.
- **Reduce user friction by limiting warnings:** Agencies should simplify the user experience to reduce friction for users. In general, agencies should avoid the use of unnecessary pop-ups, modals, overlays, interstitials, and other messages that interrupt the user experience and impede the user from completing a task, unless it is a necessary part of the design of the user experience (e.g., a warning before permanently deleting an item) or is otherwise required by law. When determining whether or not to use a warning, agencies should consider the urgency of the information and whether a user action is required as a result of the message.
- **Do not alarm or frighten your users in ways that erode trust:** Agencies should consider how legal, security, and error messages are presented and conveyed to users. Agencies should avoid using a tone in their notices to users (such as about access, authorized use, or monitoring) that may have the unintended consequences of eroding trust and impacting the ability of users to successfully transact or engage with government.[14] Instead, agencies should provide notice in a way that communicates the information clearly and with a tone that still welcomes appropriate engagement with the website or digital service. To the extent appropriate, agencies should convey necessary legal and other required information (such as about acceptable use and access conditions, government responsibilities to the user, or other responsibilities associated with using the website or digital service) in a centralized manner.[15]

3. Content That Is Authoritative and Easy to Understand

The Federal Government produces a large amount of official and authoritative information not available from other entities. This content serves many purposes and audiences, helping the public obtain services from agencies or answers to their questions. Agencies are responsible for the content they disseminate and should take affirmative steps to maximize its

[13] For example, to the extent practicable, an agency should add its seal or emblem to its profile page on a social media website to indicate that it is an official agency account. Similarly, to the extent practicable, an agency may leverage a third-party service on a non-governmental domain to host websites or content for official communication or delivery of services on behalf of the government, but the agency should perform domain name masking with a .gov or .mil domain name to verify to the public that they are interacting with the government and not a non-governmental actor. *See* OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*.

[14] Specifically, agencies should not interpret related controls in the National Institute of Standards and Technology (NIST) Special Publication 800-53 (such as AC-8 in SP 800-53 revision 5) as requiring the display of warning banners on digital services designed for access by the general public.

[15] Agencies should consult USWDS and Digital.gov for more specific guidance on how best to display required links and other relevant information on websites and digital services.

quality, objectivity, utility, and integrity.[16] Poor information quality reduces public trust, introduces confusion that could negatively impact individuals who seek government information and services, and hinders government operations.

For agency websites and digital services, content can easily become outdated or abandoned over time without strong internal agency controls to ensure that information is timely and accurate. Duplicative websites and content can also be problematic because they may cause public confusion (about, for example, which answer is the right one) or obscure the most appropriate content (by, for example, making it unclear which agency is positioned to give an authoritative answer). Regular agency review (and interagency coordination and review, as appropriate) of content is necessary to ensure that outdated, inaccurate, or duplicative information does not negatively impact the public. Proper content strategy should provide consistent answers to commonly asked questions and other top-trafficked web content, and those answers should be accurate, targeted to the appropriate audience, and non-duplicative.

a. One Answer

- **Remove outdated content:** Agencies should address outdated and inaccurate content as soon as practicable. At the same time, agencies should be cognizant of potentially relevant obligations and policies,[17] such as the need to provide adequate notice when initiating, substantially modifying, or terminating significant information that the public may be using (such as historical information); removal of information that is useful to the public can also negatively impact trust.[18] When removing content, where appropriate, agencies should create redirects (e.g., an HTTP 301) to direct the public and search engines to new or more accurate content.
- **Do not publish duplicative content:** Agencies should avoid unnecessary duplication and repetition of content or similarly related content and should establish processes to review and deduplicate content across websites within their agency as well as across government for cross-agency information and services, whenever possible. Similar content on multiple websites may be appropriate when those websites serve different audiences or user needs.[19] However, duplication can create confusion when the information is not consistent, and can impose extra cost and effort to maintain.
- **Retire duplicate websites and digital services:** Agencies should decommission or consolidate websites and digital services that duplicate content or functionality. Each website, digital service, and piece of content should serve the express purposes of the organization and identified wants and needs of users, and users should feel confident that

[16] *See* OMB's *Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies*, 67 Fed. Reg. 8452 (Feb. 22, 2002).
[17] Agencies are reminded of their obligation to comply with applicable laws and OMB guidance for information quality. See OMB's *Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies*, 67 Fed. Reg. 8452, and guidance from the National Archives and Records Administration for the management of electronic records.
[18] *See* OMB Circular No. A-130, *Managing Information as a Strategic Resource* (2016); 44 U.S.C. § 3506(d).
[19] For example, when a website or digital service is focused on improving access for a unique and specific class of people within or across agencies.

they are being directed to appropriate content and tools when they seek to take advantage of an agency's informational or transactional services.

- **Get user feedback on content:** Agencies should provide a feedback mechanism for users to report satisfaction or dissatisfaction with each web page or piece of web content, which enables the public to identify potentially inaccurate, outdated, confusing, or duplicative content. Agencies are encouraged to continuously monitor, measure, and optimize content for performance so the public get the answers they need.

b. Plain Language

Federal agencies should publish content online so the public can find what they need, understand what they find, and use what they find to meet their needs. Ideally, content should be designed and written so it is conversational, structured, and scannable by users.

- **Write content in plain language:** The Plain Writing Act of 2010 prescribes requirements for the writing style of a wide range of electronic and paper documents prepared by agencies.[20] Agencies must use plain language for any document that is necessary for obtaining any Federal Government service or benefit, provides information about a Federal Government service or benefit, or explains to the public how to comply with requirements the Federal Government administers or enforces.[21] In addition to meeting the Act's requirements, each agency should, to the extent practicable, write content for websites and digital services in accordance with Federal Plain Language Guidelines.[22]
- **Write and test content for the intended audience:** Agencies should write online content for the intended target audience and should routinely review online content to make sure it is easy for the audience to read and understand. Agencies should test online content with the intended target audience before and after publishing. When writing online content for the general public, agencies should produce material that is fully comprehensible to the average reader, who reads at an eighth-grade level [23] and generally prefers to read online content at levels lower than that. If the target audience is composed of experts (e.g., scientists), a higher reading level may be appropriate. If the target audience is people who may have trouble reading (e.g., low reading literacy, people with cognitive disabilities), then a lower reading level may be more ideal.
- **Write content in conversational language:** Agencies should write online content with an active voice; use clear and concise sentences; avoid slang, jargon, and acronyms; and use logical organization and informational headings. Agencies should write conversationally, like regular people talk to each other.

[20] Plain Writing Act of 2010, Pub. L. No. 111-274.
[21] *See* OMB Memorandum M-11-15, *Final Guidance on Implementing the Plain Writing Act of 2010.*
[22] *See* Federal plain language guidelines (https://www.plainlanguage.gov/guidelines/).
[23] "Readability of Patient Education Materials on the American Association for Surgery of Trauma Website" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4139691/#:~:text=The%20average%20reading%20skill%20of,at%20the%20eighth%2Dgrade%20level).

- **Avoid unnecessary "legalese":** Unnecessary legal jargon may inhibit public comprehension. When publishing content for websites and digital services, agencies should consider possible ways to balance competing needs for readability and legal precision. For example, an agency might publish a highly technical webpage on a legal issue for an expert audience, but also publish a complementary page that addresses the same issue in more easily understandable terms for a general audience.

c. Translation and Localization

Many members of the public who interact with Federal agencies have limited-English proficiency (LEP) or use a language other than English. Agencies may in some circumstances be required by statute or Executive order to provide information and services in multiple languages. Even in the absence of such an obligation, agencies should ensure that websites and digital services are offered in languages that meet the needs of their customers.

- **Consider limited English proficiency:** Agencies should examine websites and digital services to ensure content is written and implemented so that LEP users can meaningfully access those services consistent with, and without unduly burdening, the fundamental mission of the agency.[24]
- **Translate or localize content:** Agencies must translate content when required by law and should translate or adapt content based on user needs to more effectively communicate with people served by the website or digital service.[25] If a significant portion of the target audience speaks a language other than English, translation or localization and developing multilingual content for a website or digital service should be a priority. Agencies should develop an internal strategy for developing and managing multilingual content in conjunction with the information architecture of their websites and digital services.
- **Do not rely on auto-translation alone:** Agencies should utilize human-based multilingual content creation and test with native language speakers to verify accuracy and to understand cultural context instead of relying solely upon machine translation services (e.g., services where a computer algorithm translates text automatically into another language without human assistance or review).

d. Content Governance

The public should not be overly burdened with the responsibility to determine which online content published by the Federal Government is most current or most appropriate for their needs when published content differs or conflicts. While the members of the public are always

[24] *See* Executive Order 13166, *Improving Access to Services for Persons with Limited English Proficiency* (August 11, 2000).

[25] Translation is the process of adapting content from one language into another language. Localization is the process of adapting content for a more specific linguistic or cultural audience. Localization may go beyond translation of text and might involve changing images, color palettes, symbols and systems, etc. For example, English content can be translated into French, but there are many regional dialects and cultural differences to consider if the target audience is a French speaker in France, Canada, or the Caribbean. In this situation, localization may be more appropriate.

free to draw their own conclusions, agencies should take steps to reduce the cognitive burden or potential uncertainty that users might experience while also ensuring the quality and accuracy of the information they publish online. Accomplishing this at an enterprise level means establishing internal controls and management practices for the publishing of high-quality, authoritative information the public can rely on.

- **Establish an enterprise content strategy:** Agencies should develop internal content design and editorial guidance, including content creation guidelines, information architecture standards, and standardized language for common terms and phrases, to reduce the effort required by individual agency components, website managers, or digital delivery teams to develop or update web content on a regular basis.
- **Establish a content management system strategy:** Agencies should utilize content management systems (CMS) with automated editorial workflows to support ongoing review and quality control of content published on websites and digital services. Agencies should develop an enterprise-wide approach to content management systems and should consolidate and reduce existing content management systems, where appropriate, to reduce cost and complexity.
- **Establish content review controls:** Agencies should establish internal control processes to regularly review websites and digital services to ensure that content is current, accurate, useful, and authoritative and not outdated, inaccurate, useless, or duplicative. At a minimum, any web content that is not actively maintained should be reviewed no less than once every three years from initial publication or date of the last review to determine if there are opportunities to consolidate or remove outdated content. Agencies are encouraged to publish the following on each agency web page: last updated date, next review date, author or program owner, reviewer author or office, or other markers that provide transparency and build trust with users.
- **Involve subject matter experts:** Agency control processes should ensure that decisions regarding content, especially the removal or modification of existing content, are informed by persons knowledgeable of the content (such as subject matter experts)[26] and, to the extent practicable, the target audience of the content.
- **Clearly label non-governmental content:** Agencies should establish processes to label or distinguish non-governmental content (e.g., third-party information or research, user-generated content) that is disseminated on an agency website or digital service, including links to third-party websites,[27] in a manner that minimizes the impact of such labeling on the usability of their websites and digital services.[28]

e. Public Awareness Campaigns

[26] For example, statistical agencies and units should conduct the review of their own content.
[27] *See* OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications.*
[28] For example, popups, overlays, and interstitials are not recommended for this purpose due to their disruptive nature and negative impact to the user experience. Agencies should consult USWDS for best practices for labeling content that includes external links.

To better inform the public of government information and services, agencies may need to use websites and digital services to promote awareness of government services, benefits, and programs.

- **Ensure campaigns are strategic and time-bound:** Consistent with applicable law, agencies may establish campaigns (e.g., informational, public awareness, public affairs) to communicate with the public about an issue, service, benefit, or opportunity. However, online campaigns should be time-bound, strategic, and measured for performance. Agencies should monitor timeliness and duration of public awareness and advertising campaigns to ensure that expired online content does not persist.
- **Utilize campaign landing pages:** Agencies should avoid creating standalone websites ("micro sites") for marketing, advertising, and public awareness campaigns that unnecessarily duplicate information or functionality found on the agency's principal website. Instead, agencies should use the URL for the authoritative web page or tool on the agency's principal website in their awareness campaigns (e.g., [agency].gov/find-services); use vanity URLs that automatically redirect users to an authoritative web page or tool (e.g., get[agency]services.gov); or design and publish a single campaign landing page (e.g., [agency].gov/services) that directs users to authoritative web pages or tools. These strategies help prevent an agency's websites from competing with each other for visibility in third-party search results and reduce user confusion over which source is authoritative.

4. Information and Services That Are Discoverable and Optimized for Search

Search is a basic and universal part of using the internet, and search functionality is an expected feature for websites and digital services. Moreover, the public currently gets to Federal Government information and services online primarily through external search engines, which are critical to discoverability. Agencies' websites must be structured well; contain rich, descriptive metadata; feature machine-readable content to the extent practicable; and follow search engine optimization (SEO) practices to ensure that members of the public can access government information and services from third-party websites and applications. In addition to SEO and public discoverability, a well-structured website also can be friendlier to assistive technology, archival software or services, and for other uses.

The Federal Government's public web presence is an open book that may be crawled, archived, or "scraped" by anyone in the general public, at any time. Enabling short- and long-term preservation of government content is critical to public understanding of the government and its history, when appropriate. Web scraping plays an important role in making government information and data available and useful for a variety of public uses, including potentially for the training of large language models that enable artificial intelligence chatbots and services to accurately represent information about the government.

- **Use on-site search functionality:** Agencies' public-facing websites must contain a search function that allows users to easily search content intended for public use. This search function should be a site-wide global search and, when appropriate, could be a feature-specific search for a subset of the website content that is of significant public

interest (e.g., find-a-form tool). Agencies should participate in the Search.gov program by utilizing Search.gov for on-site search solutions or by integrating search solutions with Search.gov.

- **Design search-engine optimized content:** Agencies should ensure that publicly available content (i.e., content that does not require user authentication or sign in) is designed and structured so it can be effectively crawled and indexed by search engines. Agencies must not limit which search engines or crawlers can access or archive their public content. Agencies should employ best practices to improve crawling or indexing of web content, including using sitemaps, robots.txt files,[29] and descriptive metadata in commonly parsed fields (e.g., meta element tags).
- **Promote the "right" content:** Agencies should be strategic with SEO efforts and should think about SEO in the context of the intended audience. Agencies generate a lot of content and not all of this content is of equal importance. Unoptimized or poorly optimized content will result in negative user experiences and poor customer satisfaction. Agencies should perform keyword research and actively look at third-party search results to better understand how the public is trying to find information and should optimize content accordingly so that search terms generate results that are most likely to address the user's query.
- **Optimize content for discoverability and utility**: Agencies should optimize and organize online content to help the public find what they are looking for as efficiently as possible, with the fewest number of steps or clicks, and without forcing the user to understand bureaucratic jargon, internal government concepts and structures, or any other superfluous information that would unnecessarily impede the public's understanding.
- **Indicate timeliness of content:** Agencies should indicate when content on static,[30] public-facing websites was created or last updated by including temporal information in line with content or by using "Last Modified" in the HTTP header, in metadata tags, or in XML sitemaps. Time-and-date stamps provide transparency to the user and help the public better understand the freshness of content. When developing a timestamp strategy, agencies should prioritize adding timestamps to content that is time-sensitive, frequently changed, or top-trafficked.
- **Permit automated web scraping:** Generally, agencies shall permit web scraping and archival services to operate unimpeded without challenge-response restrictions (e.g., without presenting CAPTCHAs). Blocking or throttling of even potentially abusive crawlers is only appropriate in exceptional circumstances, such as an active denial-of-service attack, and, even then, is appropriate only on a temporary basis. If an agency detects significant public interest in scraping information from web pages, the agency should strongly consider making that information available as machine-readable data that can be accessed in bulk and optimized for automated access (such as through an API).

[29] Robots.txt standard (or robots exclusion standard) is used by websites to indicate to web crawlers or other automated web robots (or bots) which part of a website they are allowed to visit. This is used to optimize crawling and to prevent overloading a site with requests. It is not designed to prevent indexing or to prevent bots from accessing a website.

[30] Timestamps may not be appropriate for dynamic websites and web applications with server-generated content.

5. Secure by Design, Secure by Default

Federal agencies must ensure that every phase of the design and development lifecycle for their websites and digital services accounts for application security and its impact on users. Accordingly, OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, establishes requirements for agencies to meet specific cybersecurity standards as part of the Federal Government's zero trust architecture strategy.

- **Encrypt in transit**: Agencies shall encrypt all web traffic across their websites and digital services as HTTPS, including both public-facing (internet-facing) and internal-facing traffic.[31] Agencies shall "preload" all their registered .gov or .mil domains as HTTPS-only in modern web browsers.
- **Provide secure and usable authentication:** Federal websites and digital services that require authentication should be both secure and easy to log into.
    - OMB M-22-09 establishes requirements for agencies' use of multi-factor and phishing-resistant authentication. Public-facing agency systems that support multi-factor authentication (MFA) must give users the option to use phishing-resistant authentication.[32] Agencies must require certain categories of users to employ phishing-resistant MFA to access agency-hosted accounts.[33] These baseline requirements empower users that need high levels of security and ensure that the Federal Government is keeping pace with innovations in usability and security. However, to ensure a diversity of options for public access, agencies should permit a variety of authentication methods.
    - Agencies shall not require users to periodically rotate their passwords.
    - Following on from M-22-09, this memorandum requires additionally that:
        - Agencies shall not automatically deactivate user accounts, or otherwise penalize inactivity, within an expected schedule of use.[34]
        - Agencies shall ensure websites that require the public to authenticate are compatible with commonly-used password managers, and shall not prevent the "pasting" of passwords or other automated, client-side assistive mechanisms.

In addition to M-22-09, a variety of other authorities and this memorandum require or recommend additional security practices for agencies.

---

[31] These requirements concerning HTTPS are established in OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, which extends the requirements of OMB Memorandum M-15-13, *Policy to Require Secure Connections Across Federal Websites and Web Services*, from internet-accessible websites to all Federally operated websites.

[32] *See* OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles.*

[33] *See id.*

[34] For example, if the users of a given website are expected to log in only rarely (e.g., once a year for tax purposes), then the agency administering the website must not deactivate accounts simply because they have been inactive for almost a year.

- **Design secure digital services and experiences:** When developing software, agencies should follow and automate security best practices to ensure security is considered throughout all stages of the design and development lifecycle, to the greatest extent possible.[35]
- **Conduct regular security assessments and testing:** Agencies should regularly assess the risk to websites and provide commensurate security testing of those sites based on that assessment. The assessment should consider the potential impact of a security incident on vital transactions or core services provided to the public, access to timely information, government and vital external operations, and public trust. Agencies should perform manual penetration testing, where appropriate, based on threat analysis and the criticality of the underlying system.
- **Allow users to safely report security issues:** As required by Binding Operational Directive (BOD) 20-01, issued by the Cybersecurity and Infrastructure Security Agency (CISA), each agency must have a vulnerability disclosure policy that applies to all its internet-accessible websites and digital services, even those that are not intentionally made available to the public. This policy must allow the public to report potential security vulnerabilities and provide that the agency will not pursue legal action based on activities that represent a good faith attempt to comply with the policy. While agencies may list their registered domains as a reference, they must not limit the scope of the policy to specific websites or use an allow list to restrict the range of users who may submit reports.[36]
- **Avoid unnecessary third-party resources:** Agencies must not embed static, unchanging web assets, such as a specific version of a common and widely used code library (e.g., JavaScript, CSS, fonts) that are hosted on third-party services not under the control of the agency. Embedding static third-party assets is an outdated practice that no longer confers significant performance benefits, and it creates unnecessary security risks. This restriction only applies to static (unchanging) third-party assets[37] and does not bar the practice of embedding dynamic third-party resources that are necessary for digital service delivery (e.g., analytics services).

6. User-Centered and Data-Driven Design

---

[35] *See* OMB Memorandum M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices;* NIST's *Secure Software Development Framework (SSDF)*, https://csrc.nist.gov/Projects/ssdf; and the Cybersecurity and Infrastructure Security Agency (CISA)'s *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default*, https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf.

[36] These requirements for vulnerability disclosure policies are stated in OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation*, and CISA BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy*. Agencies were permitted upon the initial issuance of those policies to incrementally expand the scope of their vulnerability disclosure policies (VDP) over time. However, all relevant deadlines have passed, and agencies are no longer permitted to exclude an internet-accessible system or service from the scope of their VDP.

[37] In this context, static assets refer to files, such as images or code, that are not expected to be changed by the server before they are delivered to the user.

Federal websites and digital services should be designed and delivered with users at the center of the experience while also achieving an agency's business or organizational goals. Every website and digital service should have a defined core customer, segmented group, or user. By identifying the core audience for each, and clarifying each audience's specific needs through user research and design, agencies can best optimize the digital experience to help that audience meet their needs. Only after agencies have researched and validated the specific wants and needs of users should they create a new website or digital service. Agencies should have a continuous, user-centered design process for gathering and responding to user wants and needs, with both qualitative and quantitative research and data-driven analysis influencing design, technology, and related business decisions.

- **Start with users' wants and needs:** Agencies should conduct generative user research and business or market analysis, employing common user-centered research and design practices,[38] before developing a new website or digital service. Agencies should proactively identify customer or user pain points and opportunities to make improvements to existing experiences or to design new digital solutions, and use research and data to validate their assumptions about how customers or users want to interact with their agency or service.
- **Engage users throughout design and development:** Agencies should evaluate the user experience created by their websites and digital services from beginning to end to proactively reduce burden on the public. Agencies should seek actionable feedback from diverse user groups throughout the development process, including while researching an initial design concept, iterating on content and user interface design, conducting usability testing, and monitoring the performance of the website or digital service. Agencies should establish processes to get qualitative feedback from actual users and not rely solely on web analytics data or the perspectives of frontline agency staff. User research should be conducted directly with members of the real-life user base.[39]
- **Test with a representative cross-section of users:** Agencies should conduct ongoing usability testing to validate websites and digital services, including iterations on existing designs or new features and functionality, for ease of use and overall user satisfaction. As new pain points and challenges are identified, agencies should make incremental, iterative changes to respond to real-time user needs and improve usability or functionality. Agencies should proactively engage users from underserved communities to ensure their perspectives are incorporated. Usability testing should incorporate persona[40] groups that have been developed to capture the spectrum of user types for the website or digital service.

[38] User research focuses on understanding user behaviors, needs, and motivations through observation, interviews, collaborative design methods, and other feedback methodologies (such as focus groups or usability testing). See Digital.gov for more information.

[39] For example, agencies may designate subject matter experts to help ensure that websites and web applications meet mission outcomes and legal, policy, and other requirements. However, these activities are complementary to user research and should not be considered as user research or a substitute for user research.

[40] Personas (or user personas) are semi-fictional character profiles, which are created based on user research for products and services. They serve as an archetypal representation of your current (or ideal) customer for design and development.

- **Incentivize participation:** Agencies should compensate participants for their time and expertise when conducting user research, where appropriate. Compensation improves recruiting and ensures that agencies are gathering input from a diverse group of users, including those from underserved communities. Agencies should establish policies and processes to compensate research participants.[41]
- **Make data-driven design and development decisions:** Agencies should enhance the functionality of their websites and digital services through data-driven decision-making. This should include, but is not limited to, measuring task completion, using web analytics to understand user flows and behavior, assessing user satisfaction through feedback surveys, optimizing web pages and content for performance, and conducting research on user burden.
- **Utilize web analytics:** Agencies should use web analytics to better understand user behavior for the purpose of improving public-facing websites and digital services. The use of web measurement technologies (such as cookies, tracking pixels, tags, and other tracking technologies) is subject to limitations.[42] Agencies are required to participate in GSA's government-wide Digital Analytics Program (DAP).[43] Participation in DAP does not preclude agencies from using other web analytics services.

7. Customized and Dynamic User Experiences

The public increasingly expects digital experiences to be customizable, which makes for a dynamic experience and reduces burden when completing tasks. Customization[44] is controlled by users, who can make changes manually to a digital service or experience to meet their needs. Customization relies on user choice. Customization is different from personalization, which relies on data about the user and is not controlled by the user.

- **Design customizable experiences:** Agencies should design websites and digital services with user-controlled options to customize users' experience or to activate or deactivate certain features within an experience. For example, agencies could provide users with an option to configure the view they prefer, such as tiles or lists, while using a digital service or could develop a decision support tool with filtering and sorting options to help users make the most informed decision about an offered service. Agencies should prioritize customization that helps users complete more relevant tasks, and do so more quickly.
- **Respect user privacy:** Agencies should consider privacy risks when utilizing customization or personalization technologies and should ensure that the design of the digital service incorporates appropriate privacy safeguards.[45]
- **Pre-populate with user data:** Agencies should leverage data previously provided by users, where appropriate, to reduce the burden of future interactions. For example, when

[41] There may be legal limitations on compensating participants. Agencies should consult their counsel and Chief Financial Officer appropriately when establishing policies and processes for compensation.
[42] *See* OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*.
[43] *See* Digital Analytics Program (DAP), https://digital.gov/guides/dap/.
[44] *See id.*
[45] *See id.*

providing an authenticated experience, agencies should consider using existing information about the person to populate or pre-fill known form data about the person, as appropriate. Pre-population can help improve the user experience and save time. Agencies should consider privacy risks when assessing whether to pre-populate user data, particularly if users provided that data for a different purpose, and ensure that its deployment incorporates appropriate privacy safeguards.

- **Communicate to users through their preferred channels:** Where appropriate, agencies are encouraged to develop multi-channel messaging (such as sending email and text/SMS notifications in addition to physical letters) to communicate timely, important, and personalized information to customers or users in the channel(s) they prefer. Agencies should also allow users to adjust online settings to establish their preferred channels and frequency for receiving notifications and communications.

8. Mobile-First Design That Scales Across Varying Device Sizes

Federal websites and digital services targeted at the public should be available, accessible, and usable on a wide range of devices and platforms. A majority of the public accesses Federal information and services online, increasingly from mobile devices.[46]

- **Design mobile-friendly and device-agnostic websites and digital services:** To the greatest extent practicable, agencies must ensure that public-facing websites and digital services are mobile-friendly and developed in such a way that the website may be navigated, viewed, and accessed on a smartphone, tablet computer, or other mobile device.[47]
- **Design mobile-first experiences:** Agencies should draw on mobile-first design principles[48] when developing (or redeveloping) public-facing websites and digital services so that they are responsive on a variety of devices and window or screen sizes as well as popular mobile device browsers. For websites or digital services where the majority of users are on mobile devices or tablets, mobile-first design should be a priority.
- **Test on mobile and tablet devices:** Agencies should ensure that websites and digital services are functionally tested not only on desktop and laptop computers, but also on mobile and tablet devices, for both usability and performance. Modern browsers contain emulators and the ability to constrain both viewport size and internet speed. While it is recommended to test on actual mobile devices, these browser-based tools are acceptable substitutes during development if resources are limited.
- **Leverage device usage patterns:** Agencies should measure and analyze the device usage patterns of their users in the aggregate to optimize the design and experience based on the

[46] As measured via the Digital Analytics Program (https://analytics.usa.gov/), as of the publication of this memo.
[47] Connected Government Act, Pub. L. No. 115-406 (2018).
[48] Mobile-first design is an approach in which a website or digital service is designed for mobile devices first. This typically involves designing for the smallest screen first and gradually working up to larger screen sizes. Designing for small screens first encourages user experience designers to remove anything that is not essential for rendering and navigation, which optimizes the experience for the user.

most commonly used browsers and devices. Agencies should also ensure that websites and digital services are designed and tested proportionately based on device usage patterns.

- **Optimize for performance:** Agencies should routinely analyze websites and digital services for load speed and continually strive to optimize for performance (e.g., high page speeds, low page load times, small load page size). Agencies are encouraged to use techniques such as minification and image optimization, and eliminate any unnecessary plugins.[49] Agencies should give special consideration to low-bandwidth users whose mobile devices and cellular connectivity are often their only means to interact with the government online.
- **Use modern protocols:** Agencies must employ the latest stable versions of HTTP (i.e., HTTP/2, HTTP/3, and any successor versions), HTML, and other relevant standards. In recent years, the web platform and its associated technical protocols have prioritized making the mobile web more responsive and resilient to network disruption. Agencies must keep pace with these developments and optimize for real-world situations (such as intermittent connectivity or throttled bandwidth).
- **Avoid building or maintaining unnecessary mobile apps:** An agency should avoid building native mobile applications[50] unless it has validated a compelling user need through research, and has balanced the need against additional long-term cost implications. Agencies should evaluate their existing mobile apps and retire those that are not continuing to provide significant user or business value. Instead, agencies should prioritize the design, development, and management of web applications that can be used on mobile devices.

9. Other Digital Experience Requirements

a. Privacy

The Federal Government must consider and protect an individual's privacy throughout the information lifecycle.[51] Integrating privacy into agency websites and digital services takes two primary forms: (1) addressing privacy risks related to these products, and (2) providing clear and accessible notice through these products about how an agency creates, collects, uses, processes, stores, maintains, disseminates, discloses, and disposes of personally identifiable information (PII).[52] Clear communication and transparency with the public are critical to both activities—whether internal to the agency, when agency officials communicate early and often

[49] See tools recommended in the U.S. Web Design System's performance guidance, https://designsystem.digital.gov/performance/.
[50] Mobile applications are software applications designed to run natively on a mobile device's operating system and should not be confused with mobile web applications, which are applications that are optimized to be used on a browser on a mobile device.
[51] *See* OMB Circular No. A-130, *Managing Information as a Strategic Resource*. Agencies are responsible for ensuring their activities and policies comply with all applicable laws (e.g., the Children's Online Privacy Protection Act), which may have additional requirements.
[52] *See* OMB Circular No. A-130, *Managing Information as a Strategic Resource*, for the definition of PII.

about privacy considerations, or external to the agency, when its websites inform the public about how it handles PII.

- **Design with privacy in mind:** To ensure appropriate risk management and compliance with applicable law and policy, agencies should consult their privacy programs led by Senior Agency Officials for Privacy (SAOPs)[53] at the earliest planning and development stages for websites and digital services that involve PII, and they should continue the review of privacy risks throughout both the development and information lifecycles.[54]
- **Maintain a clear, up-to-date Privacy Policy:** Agencies must post Privacy Policies on all public-facing websites and digital services (including their principal, sub-agency, component, and program websites and digital services). For each website, agencies must post a link to that website's Privacy Policy on any known, major entry points to the website as well as any webpage that collects PII.[55] A Privacy Policy must:
    - Be written in plain language and organized in a way that is easy to understand and navigate;
    - Provide useful information that the public would need to make an informed decision about whether and how to interact with the agency;[56]
    - Be updated whenever the agency makes a substantive change to the practices it describes;
    - Include a time-and-date stamp to inform users of the last time the agency made a substantive change to the practices the Privacy Policy describes;
    - Adhere to all other applicable OMB requirements; and
    - Include a link to the agency's Privacy Program Page.
- **Provide appropriate notice for online collections of information:** A Privacy Act statement is required whenever an agency asks individuals to supply information that will become part of a system of records under the Privacy Act.[57] Agencies must provide a privacy notice, whenever feasible, where a Privacy Act statement is not required but members of the public nonetheless could provide PII to the agency using a website or digital service. The privacy notice should include a brief description of the agency's practices with respect to the PII that the agency is collecting, maintaining, using, or disseminating.
- **Maintain an up-to-date Privacy Program Page:** Each agency must maintain a central resource page dedicated to the privacy program on the agency's principal website,

[53] *See* OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy*.
[54] *See* OMB Circular No. A-130, *Managing Information as a Strategic Resource*.
[55] This requirement does not apply to internal agency activities (such as on intranets or online interactions that do not involve the public).
[56] *See* OMB Memorandum M-99-18, *Privacy Policies on Federal Web Sites*, and OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.
[57] *See* 5 U.S.C. § 552a(e)(3). *See also* Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,961, 28,962 (July 9, 1975); OMB Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act* (2016).

located at [agency].gov/privacy, [58] to serve as a central source for information about the agency's practices with respect to PII. At the discretion of the SAOP, sub-agencies, components, and programs may maintain a sub-agency-, component-, or program-specific privacy program page. At a minimum, agencies must include the following on the Privacy Program Page:

- *System of records notices (SORNs), matching notices and agreements, exemptions to the Privacy Act, Privacy Act implementation rules, and instructions for submitting a Privacy Act request*.[59]
- *Privacy impact assessments (PIAs)*. Agencies must list and provide links to PIAs. However, agencies may determine not to include a link to a PIA if doing so would raise security concerns or reveal classified or sensitive information (sensitive information may include information that is potentially damaging to a national interest, law enforcement effort, or competitive business interest). Agencies must have a specific, compelling justification in order to decline to post a link to a PIA. If deciding not to post a link to a PIA, agencies should produce a summary or a modified version of the PIA that is suitable for posting.
- *Publicly available agency policies on privacy*. Agencies must list and provide links to all publicly available agency policies on privacy, including any directives, instructions, handbooks, manuals, or other guidance.
- *Publicly available agency reports on privacy*. Agencies must list and provide links to all publicly available agency reports on privacy (e.g., annual matching reports submitted pursuant to the Privacy Act, Section 803 reports submitted pursuant to the Implementing Recommendations of the 9/11 Commission Act of 2007). These reports need not include agencies' Federal Information Security Modernization Act of 2014 (FISMA) reports or reports provided to OMB and Congress pursuant to 5 U.S.C. § 552a(r).
- *Contact information for submitting a privacy question or complaint*. Agencies must provide appropriate agency contact information for individuals who wish to submit a privacy-related question or complaint.
- *Contact information for the SAOP*. Agencies must identify their SAOP and provide contact information for the SAOP's office. Agencies may also identify and provide contact information for any component-level privacy officials.

b. Software Development Principles

Complex systems can make websites and digital services costly and difficult to manage and maintain over time. Building around principles of agility, reliability, scalability, maintainability, interoperability, and simplicity can reduce these burdens.

[58] *See* OMB Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

[59] See the requirements for each of these items in OMB Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*. The requirement to provide links to complete, up-to-date versions of SORNs on the agency's Privacy Program Page does not replace the Privacy Act's statutory requirement to publish SORNs in the *Federal Register*.

- **Prefer loose coupling:** When building websites and digital services, agencies should prefer loose coupling[60] as a design pattern over monolithic architecture patterns, where appropriate. Monolithic architecture typically involves tight coupling between components, especially in large, complex systems. Tightly coupled systems can be more difficult to scale and maintain, and may introduce unnecessary business risk.
- **Decouple front-end and back-end systems:** When developing websites and digital services, especially around large, complex systems, agencies should consider decoupling front-end (e.g., presentation, client-side layer) user interfaces from back-end (e.g., server-side, data access layer) systems.
- **Default to static websites:** Where a website or digital service does not require a dynamic back-end service to provide necessary functionality, agencies should prefer "static" website architectures. Static website architectures are designed to serve static files at specified URLs, rather than dynamically executing code to assemble content on a web request. Since static sites do not execute server-side code, their attack surface is dramatically smaller than dynamic applications. In addition, static websites are generally much more cost-effective to operate than dynamic applications and load faster for users, especially those with low-bandwidth internet.
- **Promote interoperability by leveraging standard interfaces:** Agencies should build and share standardized interfaces (e.g., web APIs with industry-standard exchange formats), to the greatest extent possible, where appropriate. Standard interfaces enable easy data exchange functionality without additional work to integrate and promote interoperability between different systems and components.
- **Follow open standards and be browser neutral:** The internet is built on a robust ecosystem of open standards. To ensure websites and web applications work well in this ecosystem, agencies should follow appropriate web standards[61] to the greatest extent practicable. Agencies should avoid building or maintaining websites or web applications that only work in a specific browser by design. Agencies should ensure that websites and web applications are generally compatible and functional across a wide range of common browsers.[62]
- **Default to HTML:** HyperText Markup Language (HTML) is the standard for publishing documents designed to be displayed in a web browser. HTML provides numerous advantages (e.g., easier to make accessible, friendlier to assistive technology, more dynamic and responsive, easier to maintain). When developing information for the web, agencies should default to creating and publishing content in an HTML format in lieu of publishing content in other electronic document formats that are designed for printing or

[60] In this context, loosely coupling is an approach in which components in a system are weakly associated with each other, and depend on each other to the least extent practicable. This means changes in one component least affect existence or performance of another component.

[61] Web standards, such as those developed by the World Wide Web Consortium (W3C), are non-proprietary standards, technical specifications, or guidelines that define and describe aspects of the World Wide Web (e.g., development and design practices for websites).

[62] Due to the wide ranges of browsers and browser-related standards, universal browser access is impractical, but, nevertheless, agencies should strive for browser compatibility rather than designing for a singular browser as a means to save development time and reduce costs.

preserving and protecting the content and layout of the document (e.g., PDF and DOCX formats). An agency should develop online content in a non-HTML format only if necessitated by a specific user need.

- **Promote resources to developers:** Agencies should maintain a developer page (e.g., [agency].gov/developer or developer.[agency].gov) to centralize information about relevant technical materials for external developers. This should include information on how to access and use public web APIs, public source code or code repositories, and any other appropriate developer tools or technical documentation that could help developers build integrated digital experiences.

c. Required Links

Agencies may need to convey information about legal compliance, points of contact, or other topics of interest to the public on their websites.[63] In the footer of each agency's principal website or principal sub-agency websites,[64] the agency must include links to:

- The agency's "about" page, which contains descriptions of the mission and statutory authority of the agency, information about the organizational structure of the agency, and the agency's strategic plan.[65]
- The agency's Freedom of Information Act page. [66]
- The agency's accessibility statement.[67]
- The agency's vulnerability disclosure policy, which must include a security contact for the public to report observed or suspected information security issues.
- The equal employment opportunity data required to be posted by each agency under Title III of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act).[68]
- The agency's Privacy Program Page.

In the footer of each agency's website, or the entry point for a digital service, the agency must include links to the website's privacy policy.

[63] Agencies have flexibility in how to present or organize this information unless explicitly stated by law or OMB guidance. For other required links, Federal agencies should determine the best location on their website to place those links based on user needs and the underlying requirement from law or policy.
[64] Each department or agency, as well as its significant components, offices, or programs, as determined by law or the agency, should provide the required links on its primary homepage. Components, offices, or programs may utilize the same required links as their parent agency, if appropriate.
[65] *See* E-Government Act of 2002, Pub. L. No. 107-347, § 207(f)(1)(A).
[66] *See* 5 U.S.C. § 552(g).
[67] *See* OMB's "Strategic Plan for Improving Management of Section 508 of the Rehabilitation Act" (Jan. 24, 2013), https://obamawhitehouse.archives.gov/sites/default/files/omb/procurement/memo/strategic-plan-508-compliance.pdf.
[68] Pub. L. No. 107-174, § 301; 29 C.F.R. § 1614.704.

Agencies should consult USWDS and Digital.gov for more specific recommendations on how to best display required links and other relevant information on websites and digital services.[69]

B. Digitization of Forms and Services

Reliance on paper-based processes, forms, and services precludes a digital experience, which is what the majority of the public now expects. Forms, services, and associated processes should be designed and modernized with digital service delivery in mind for the public and agencies to fully reap the transformational benefits and promises of a digital government, including increased convenience of online transactions, greater cost savings, and higher levels of public satisfaction with and trust in government.

1. Forms

Forms are an essential component of government and often a prerequisite to obtaining Federal Government services or benefits. Web-based forms, also called digital forms, provide numerous advantages when compared to paper-based forms. As a web application, a digital form has the capability to capture, validate, submit, and process structured information digitally and in an automated manner.[70] Digital forms, when designed correctly, can help improve information collection accuracy and usability, reduce business inefficiency, enhance security, and reduce costs and labor associated with managing and reviewing paper-based documents.

- **Provide a digital option for forms:** Agencies should make forms available to the public in a digital format to the greatest extent practicable. The design and development of digital forms should be prioritized over the creation of paper forms or electronic forms, whenever feasible. With limited resources, agencies should prioritize providing digital options for those forms that directly support the delivery of those services or benefits that have the greatest impact on the public.
- **Design digital forms first:** When agencies need to revise forms that have both digital and paper versions, agencies should design the digital form first and then use the digital form as a baseline for the redesign of the paper form.
- **Digitize paper forms:** Agencies should establish internal review processes to routinely identify non-digital forms and expedite the digitization of forms related to serving the public. Agencies should prioritize the digitization of those forms that have the greatest impact on the public. Consistent with section 4(d) of the 21st Century IDEA and as described in OMB Memorandum M-22-10, *Improving Access to Public Benefits Program Through the Paperwork Reduction Act*, if a particular form cannot be made available in a digital format, an agency is expected to document through its Paperwork Reduction Act approval process: (1) the office responsible for receiving the form, (2) the reasons the form cannot be made available in a digital format, and (3) any potential solutions, such as

[69] See Digital.gov: Required Web Content and Links, https://digital.gov/resources/required-web-content-and-links/?=checklist.

[70] Since a digital form is a web application itself, then all the aforementioned website requirements would apply in addition to the specific form requirements listed in this section.

implementing existing technologies or making procedural, regulatory, or legislative changes, that could allow the form to be made available to the public in a digital format.

- **Build adaptable and resilient digital forms:** In building new or upgraded digital forms, agencies should prioritize designing platforms that allow for efficient future alterations to question sets or response options. Similarly, agencies should prioritize building digital forms that can be scaled or replicated for use in similar information collections or transactions that an agency administers.
- **Keep digital forms digital, end-to-end:** Agencies should ensure that information collected via a digital form remains digital throughout the information lifecycle. For example, if information is collected from a digital form, it should not be converted or transformed into a paper or electronic format and then back into a digital format, unless strictly necessary.

2. Services

While websites, digital services, and other digital interactions should make up the majority of the public's interactions with the Federal Government, services can and should be provided over different channels to best meet the needs of the public. The public increasingly expects to complete tasks and transactions using omni-channel and multi-channel offerings. Omni-channel means customers can start a task or transaction in one channel (e.g., online) and seamlessly continue or finish the same task or transaction in another channel (e.g., in person). Multi-channel means customers have the option to complete a task or transaction, from start to finish, in the channel that works best for them (e.g., online, in person, over the phone, through the mail).

- **Increase digital channels and self-service:** Agencies should, to the greatest extent practicable, make services provided to the public available in a digital channel and in a manner that maximizes self-service task or transaction completion.
- **Meet people where they are:** For each service, agencies should determine the channels that are most appropriate for the intended customer or user group(s), considering the accessibility, language, and technology needs of that audience. Multi-channel services may include in-person offices, phone and contact centers, websites and web applications, mobile applications, postal mail, email, text/SMS, chat, and social media.
- **Design a seamless, unified customer experience:** Agencies are strongly encouraged, where appropriate, to take an omni-channel approach to service design and delivery. With that approach, customers have a consistent, high-quality experience regardless of channel and are allowed to advance toward task or transaction completion using the channel that is most convenient to them.
- **Maintain non-digital interaction options:** Agencies must always maintain an accessible method (i.e., physical availability) for completing a digital service through in-person, paper-based, or other means, so customers without the ability to use a digital service are not deprived of or impeded in their ability to access it. This means that agencies should afford the public the ability to complete a transaction over at least one traditional service channel (e.g., in person, postal mail, or phone).

3. Signatures

Signature requirements are common for Federal Government forms and services. Signatures are typically the means by which a person indicates an intent to associate themselves with a document in a manner that has legal significance. This often constitutes legally-binding evidence of the signer's intention with regard to a document. The reasons for signing a document will vary with the transaction.

There are many different types of signatures (e.g., handwritten or wet signatures, electronic signatures, and digital signatures). As used in this memorandum, an "electronic signature" is a method of signing an electronic message that identifies and authenticates a particular person as the source of the message, and indicates the person's approval of the information in the message.[71] Electronic signatures are typically used for the signing of electronic documents and are common in online transactions. Electronic signatures are a generic, technology neutral concept. This means that there is not a particular prescribed technology, process, or user interaction that must be used to generate an electronic signature. There are various methods by which a user can indicate the intent to "sign" electronically (e.g., typing their name, checking a check box, drawing a signature, scanning a wet signature). A digital signature is a specific type of electronic signature that uses a cryptographic mechanism to verify the authenticity of the message or document. Digital signatures, when implemented properly and used in conjunction with identity proofing processes, can provide assurance of an individual's identity and authenticity.

The use of signatures may not be appropriate for every scenario involving a public-facing form or service. Unnecessary signature requirements and poorly implemented signature requirements can prevent adoption of digital services and add unnecessary customer friction, cost, and burden on the public. Agencies should strive to find a balance between the convenience and usability of the service and any signature requirement and associated processes.

- **Accept electronic signatures:** Agencies are required, when practicable, to provide for the use and acceptance of electronic signatures. [72] Agencies have flexibility in implementing electronic signature processes, but must ensure that the use of electronic signatures and the associated signing process satisfy all applicable legal and security requirements. When used in accordance with the procedures established by OMB under the Government Paperwork Elimination Act,[73] electronic signatures cannot be denied legal effect, validity, or enforceability merely because they are in electronic form.[74]
- **Avoid unnecessary signature requirements for forms and services:** Agencies should avoid establishing unnecessary signature or identity proofing requirements that create user friction and prevent or impede an individual from successfully utilizing a form or

[71] Government Paperwork Elimination Act (GPEA), Pub. L. No. 105-277, § 1710(1).
[72] *Id.*
[73] Those procedures are set out in OMB Memorandum M-00-10, *OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act* (Apr. 25, 2000).
[74] *Id.* § 1707.

service.[75] When signatures or identity verification are required for a transaction, agencies should not collect more information from the user than is required to securely complete the transaction.[76]

- **Maintain a digital equivalent method:** To the greatest extent practicable, agencies should not require a handwritten signature (i.e., wet signature) or other in-person identity proofing requirements as a requirement for completing a public-facing form or service without providing the public with a comparable digital equivalent method for submitting information or transacting with an agency. To the greatest extent practicable, agencies should ensure that any public-facing form or service can be provided and completed by the user over different channels, preferably over at least one traditional service channel (e.g., in person) and one digital service channel (e.g., web application) and ideally in the channel that is most convenient to the user.
- **Use identity verification when greater assurance of identity is needed:** Agencies should use appropriate identity verification processes for online transactions, commensurate with the agency's risk assessment, when there is a need for assurance of the identity of the user or the authenticity and integrity of the transaction. Signatures alone do not provide identity assurance and should not be used by themselves for identity verification, identity proofing, or non-repudiation purposes when identity assurance is required.

C. Customer Experience and Digital Service Delivery

Customer experience is the public's perceptions of and overall satisfaction with interactions with an agency, product, or service.[77] Digital experience refers to the interactions between an individual and an organization that are enabled by digital technologies. Digital experience is inclusive of both the technology required to deliver services over digital channels as well as the information technology that supports or enables the delivery of services over traditional channels.

Digital experience plays a significant role in customer experience. For example, a seamless digital experience is often expected and necessary for overall customer trust, confidence, and satisfaction. Customer experience cannot be successfully achieved without considerations of digital experience since much of modern service delivery is through digital channels or is supported by technology. Agency success in digital experience means developing and actualizing a long-term organizational strategy around digital service delivery, investing in digital transformation and necessary information technology modernization efforts, and, most importantly, building a digital workforce capable of delivering information and services to the public.

[75] For example, requiring additional documentation from an individual who has already been properly identity-proofed and authenticated or requiring identity proofing or other documentation for service delivery without a specific legal requirement or risk assessment.
[76] *See* OMB*, Implementation of the Government Paperwork Elimination Act*, 65 Fed. Reg. 25,508-21 (May 2, 2000).
[77] *See* Executive Order 14058, *Transforming Federal Customer Experience and Service Delivery To Rebuild Trust in Government* (Dec. 13, 2021).

- **Apply customer experience principles:** Agencies are reminded of their obligation to comply with OMB guidance for customer experience and service delivery and are encouraged to apply leading customer experience and service delivery practices to all services, not just those services associated with High-Impact Service Providers, where appropriate.[78]
- **Leverage customer feedback data:** Agencies are encouraged to collect common customer metrics, measures, and outcomes for websites and digital services (or about the underlying service provided) as well as for non-digital experiences (e.g., an office visit, a phone call to a contact center). Agencies should regularly measure customer perceptions of trust, confidence, and satisfaction and use customer experience data and customer feedback information to inform business decision-making and operations.
- **Provide transparency to users:** Agencies should design transparency into the information and services they provide so the public has a greater understanding of how agencies operate. For example, agencies could design a case status tool that includes estimated processing times per phase, assigned adjudication staff, and completed and uncompleted steps. Agencies should prioritize designing and adding topic-based transparency details into their websites and digital services based on feedback they receive from customers from various sources, such as frequently asked questions they receive from customers or users for a specific service.
- **Build effective digital services:** Agencies should utilize the Digital Services Playbook from the United States Digital Service when developing services that are provided over a digital channel.[79]
- **Use cross-functional teams:** Agencies should build cross-functional teams that have expertise in human-centered design and agile development practices. Critical roles may include product managers,[80] user experience researchers and designers, content designers and copywriters, front-end developers, software engineers, and data analysts and may include accessibility specialists, privacy and security specialists, information architects, service designers, behavioral scientists, data scientists, or other specialized roles. Agencies are strongly encouraged to establish a dedicated team to be responsible for each digital service (a "Scrum" team), where appropriate and feasible.

D. Standardization

The 21st Century IDEA instructs agencies to maintain as much standardization and commonality with other agencies as practicable in implementing the requirements of the Act, so as to best ensure an integrated digital experience across the Federal Government and enable future transitions to centralized shared services, both within and across agencies. Increased standardization and cross-government collaboration reduce government-wide implementation costs and ensure a more consistent digital experience for the public.

[78] *See* OMB Circular No. A-11, § 280, "Managing Customer Experience and Improving Service Delivery."
[79] See the United States Digital Service's Digital Services Playbook, https://playbook.cio.gov/.
[80] Product managers serve in a particularly critical role in government since they translate business goals into development priorities, scope product backlogs and roadmaps, and manage value creation for users and the business.

- **Leverage government-wide programs:** Agencies should utilize government-wide programs provided by GSA, the Department of Homeland Security (DHS), and other Federal shared-service providers, where practicable, when developing websites and digital services.
- **Streamline and consolidate systems:** Agencies should develop an enterprise-wide strategy for adopting centralized systems and services that can be shared across departments, components, offices, and programs, to the greatest extent practicable. Agencies should work to consolidate outdated and duplicative systems and services within their agencies.
- **Enable data sharing:** Agencies should improve the efficiency and effectiveness of data sharing and support processes among agencies and with State and local governments to improve customer experience and service delivery.[81] Where feasible and appropriate, agencies should collaborate to find and actualize data-sharing opportunities with other agencies or with State and local governments. Data sharing should be pursued only when there is a demonstrated user need or potential benefits for individuals, when the benefits outweigh the costs,[82] and with appropriate privacy and security safeguards.

IV. ENSURING AGENCIES DELIVER INTEGRATED DIGITAL EXPERIENCES

Meeting the public's expectations for high-quality digital experiences requires Federal agencies to design and develop government websites and digital services that are simple to use, seamless across journeys, and secure by design. Digital channels are now the primary way the public interacts with the government in the 21st Century. Technology shapes the public's experiences with government and agencies' service delivery to the public, whether interactions occur online, in person, over the phone, through the mail, on paper, or through other channels. OMB acknowledges the challenges that agencies will encounter in their efforts to bring all websites and digital services into alignment with the requirements and recommendations of this memorandum to fully realize a digital government for the 21st Century.

All agencies must immediately take steps to achieve alignment, to the greatest extent practicable. Within 180 days of the date of this memorandum, unless an alternative deadline is specified elsewhere for specific requirements, executive agencies should address the requirements outlined in this memorandum to the fullest extent practicable when designing new or redesigning existing websites and digital services.

OMB recommends that agencies prioritize remediation of websites and digital services based on the following criteria:

1) Public-facing websites and digital services that directly support the delivery of information or a service or benefit to the public, prioritizing those with the highest volume (e.g., transactions, customers served) or those with an outsized impact in the lives

[81] *See* Executive Order 14058, *Transforming Federal Customer Experience and Service Delivery To Rebuild Trust in Government* (December 13, 2021).
[82] *See* OMB Memorandum M-01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy*.

of the population served (e.g., services designed for Tribal members to access and manage trust assets).

2) Public-facing websites and digital services with the highest volume (e.g., average monthly unique users, average daily visits).
3) Severity of website or digital service issue (e.g., security or privacy risk, complaints or litigation due to non-accessible design).

OMB recommends that agencies prioritize developing digital options for existing paper forms and non-digital services based on the following criteria:

1) Forms directly supporting the delivery of a service or benefit to the public, starting with those forms associated with the highest volume of annual transactions or highest average adjudication times.
2) Forms directly supporting the delivery of a service or benefit to the public that, if provided digitally, would address user needs, reduce public burden, or improve public impact, as determined based on user research or business analysis.
3) Assistance provided through customer call center support that could be designed as self-service digital tasks for customers to reach resolution on their own.

Finally, agencies should also consider the digital experience of Federal employees by striving to also remediate those internal-facing websites and digital services that serve Federal employees. Improvements to internal-facing websites and digital services can increase the efficiency of government operations. Such gains in efficiencies enable employees to better deliver information and services to the public and fulfill their agencies' respective missions.

With regards to internal-facing websites and digital services, OMB recommends prioritizing websites and digital services that, if remediated, would enable agency employees to better deliver information and services to the public, websites and digital services that have been identified for improvements through employee feedback, and websites and digital services with the highest severity of issue (e.g., security or privacy risks, complaints or litigation due to non-accessible design).

A. Immediate Agency Actions

1. **Identify digital experience delivery lead:** Within 30 days of the date of this memorandum, agencies shall identify a primary point-of-contact within their organization responsible for communicating information to the relevant stakeholders across the agency, providing requested information to OMB, engaging with other agencies to share best practices for implementation, and overseeing efforts to align with the requirements and recommendations of this memorandum.[83]

[83] See Digital.gov for additional information on role responsibilities and reporting instructions.

2. **Identify public-facing websites:** Within 90 days, agencies shall review data maintained by GSA's Site Scanning Program[84] and identify public-facing websites to OMB.[85]
3. **Identify and assess top websites:** Within 180 days, agencies shall analyze available web metrics (e.g., through GSA's Digital Analytics Program) to identify the public-facing websites that generate the top 80 percent of traffic (based on average monthly users) and provide this list to OMB. Agencies should review available automated scanning data (e.g., through GSA's Site Scanning Program) for these sites to assess conformance and prioritize actions related to the requirements and recommendations of this memorandum.
4. **Assess common questions and top web content for deduplication and SEO:** Within 180 days, agencies shall identify the most common questions received across all channels (e.g., online search, social media, message boards, chat, email, phone, in person); review available web metrics to identify top pages for common searches; and conduct a high-level review of potentially duplicative or substantively similar content across websites within the agency or across agencies. Agencies shall provide to OMB a list, in aggregate across channels, of the 25 to 50 most commonly asked questions and a list of no less than 10 opportunities to retire, consolidate, or explain duplicative web content; redesign or rewrite underperforming web content; or further optimize web content to improve search engine results.
5. **Assess top tasks for self-service optimization:** Within 180 days, agencies that provide services to the public shall review the highest volume public-facing services and identify the tasks required to access each service as well as the channels available to complete each task (e.g., online, phone, mail, in person). Agencies shall provide to OMB a list of opportunities for no less than 5 top tasks that can be newly designed or further optimized as self-service digital options.
6. **Inventory public-facing services:** Within 180 days of the release of the Federal Services Index, each agency shall develop and submit a preliminary inventory to the Federal Services Index[86] of all public-facing services. For each service that cannot be made available in a digital format, the agency must provide the information specified by section 4(d) of the 21st Century IDEA.[87] Within one year of the release of the Federal Services Index, agencies shall finalize the inventory and make it publicly available online.

B. Immediate Government-Wide Actions

1. **Expand resources on Digital.gov:** Within 60 days, GSA, in coordination with OMB and with other relevant interagency bodies and stakeholders, will update Digital.gov to continue to serve as the primary, centralized home for communities, best practices, and resources to help agencies and their respective digital delivery teams with implementation of the 21st Century IDEA.
2. **Facilitate interagency coordination:** Within 90 days, the CIO Council will establish a "Digital Experience Council" as a subcommittee of the CIO Council. This will serve as

[84] See Site Scanner, https://digital.gov/guides/site-scanning/.
[85] See Digital.gov for additional information on reporting instructions.
[86] See Digital.gov for additional information about reporting instructions.
[87] Pub. L. No. 115-336, § 4.

the primary interagency advisory body for assisting in the government-wide implementation of the 21st Century IDEA and related digital experience activities.

3. **Update website standards:** Within 180 days, GSA, in coordination with OMB and relevant interagency bodies and stakeholders, will review and update, as necessary, the existing Federal website standards[88] to align with this guidance. These updates will include guidelines for branding, content, and search.
4. **Update plain language guidelines:** With 180 days, the Plain Language Action and Information Network (PLAIN), in coordination with OMB and with support from GSA, will review and update, as necessary, the Federal Plain Language Guidelines.
5. **Facilitate industry collaboration:** Within 180 days, GSA will host an "industry day" to bring together agency and industry representatives so that industry can better understand the needs of the Federal Government and highlight or present solutions that can address those needs to support the full implementation of the 21st Century IDEA. GSA should explore establishing an interagency industry working group to maintain an ongoing dialogue between agencies and industry on emergent implementation needs.
6. **Make it easier to buy:** Within 180 days, GSA will identify strategic sourcing opportunities, such as potential category management solutions, to assist agencies in buying services that help meet digital experience requirements and report those recommendations to OMB. GSA is also encouraged to explore opportunities to further assist agencies in buying services that help meet digital experience requirements by providing complementary market research support to help identify capable vendors or by providing sample acquisition documents, templates, and buying guides.
7. **Identify opportunities to enhance shared digital offerings:** Within 180 days, GSA will review existing platforms, products, tools, standards, practices, and other service offerings, as well as government-wide technology initiatives and, in consultation with OMB, identify opportunities and priorities for supporting agencies with the full implementation of the 21st Century IDEA and related polices.
8. **Develop and maintain a Federal Services Index:** Within 180 days, GSA, in coordination with OMB, will develop and maintain a process or tool for agencies to use to submit and manage an inventory of services offered to the public, which should, to the greatest extent practicable, contain descriptive information about each service, usage data for each service (e.g., volume, aggregated user demographics), and a list of the tasks to get or manage each service and the channels available to complete each task (e.g., online, phone, mail, in person). GSA, in coordination with OMB, should review and identify opportunities to use existing data sources or data collection to reduce agency burden. Within one year of the completion of the inventory of public services, GSA, in coordination with OMB, will make the inventory publicly available online.

C. Ongoing Agency Assessment and Reporting Requirements

1. **Keep public-facing website information up-to-date**: Agencies should regularly review and identify their public-facing websites.

[88] See U.S. Web Design System: Federal Website Standards (https://designsystem.digital.gov/website-standards/).

2. **Keep service information up-to-date:** Agencies should periodically review service information in the Federal Services Index and update this information as needed.
3. **Keep form information up-to-date:** When seeking to obtain approval to collect information or extend or revise an existing collection, agencies must continue to document in their Information Collection Request submission materials to OMB's Office of Information and Regulatory Affairs (OIRA) how forms and associated websites and services are consistent with digitization requirements.[89]
4. **Update internal controls and policies:** Agency Chief Information Officers (or designees) should periodically review policies and internal control processes in coordination with other appropriate agency officials and update them as necessary to ensure that websites and digital services meet applicable legal and policy requirements, including those established or reiterated by this memorandum.
5. **Perform evidence-based accountability reviews:** The Chief Information Officer at any agency listed in 31 U.S.C. § 901(b)(1) or (b)(2) should regularly review and evaluate IT investments to identify struggling or underperforming IT projects (i.e., public-facing websites and digital services that are in significant misalignment with the requirements and recommendations of this memorandum). Agencies should use evidence-based accountability review processes, such as TechStat sessions,[90] to identify performance issues, conduct a root-cause analysis of those issues, identify challenges or barriers (including any resource and budget constraints), develop corrective action plans that may potentially address these causes, and develop a timeline for implementing corrective actions.

D. Policy Assistance

Questions or inquiries about this memorandum should be addressed to OMB through the Office of the Federal Chief Information Officer (OFCIO) via email: ofcio@omb.eop.gov

[89] *See* OMB Memorandum M-22-10, *Improving Access to Public Benefits Programs Through the Paperwork Reduction Act*.
[90] *See* OMB Memorandum M-15-14, *Management and Oversight of Federal Information Technology.*