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

November 8, 2016

M-17-06

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director, Office of Management and Budget

Howard Shelanski H.S.
Administrator, Office of Information and Regulatory Affairs

Tony Scott
Federal Chief Information Officer

SUBJECT: Policies for Federal Agency Public Websites and Digital Services

Federal Agency public websites and digital services are the primary means by which the public receives information from and interacts with the Federal Government. These websites and services help the public apply for benefits, search for jobs, comply with Federal rules, obtain authoritative information, and much more. Federal websites and digital services should always meet and maintain high standards of effectiveness and usability and provide quality information that is readily accessible to all.

The May 23, 2012 *Digital Government Strategy* set forth a roadmap to help agencies improve digital services and use emerging technologies to serve the public as effectively as possible.[1] Building on that strategy, on August 11, 2014, the White House released the *U.S. Digital Service Playbook* containing 13 key "plays" drawn from successful practices from the private sector and government.[2] The requirements in this Memorandum support building effective and user-centric digital services as outlined in those two documents. The goals of this Memorandum also align with the principles of OMB Memorandum M-11-24, *Streamlining*

[1] https://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf
[2] https://playbook.cio.gov/

Service Delivery and Improving Customer Service, and OMB Memorandum M-10-06, *Open Government Directive*. [3]

This Memorandum rescinds and replaces OMB Memorandum M-05-04, *Policies for Federal Agency Public Websites.*

For questions on this memorandum, please contact: infopolicy-oira@omb.eop.gov.

[3] https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-24.pdf; http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf

Policies for Federal Agency Public Websites and Digital Services

Federal Agency public websites and digital services are defined here as online information resources or services maintained in whole or in part by the departments and agencies in the Executive Branch of the U.S. Federal Government that are operated by an agency, contractor, or other organization on behalf of the agency. [4] They provide government information or services to the public or a specific user group across a variety of delivery platforms and devices, and support the proper performance of an agency function.

Unless already required by existing law or policy, or noted below, agencies are expected to comply with the requirements of this Memorandum within 180 days of its publication date.

The *Digital Services Playbook* and http://www.digitalgov.gov/resources/checklist-of-requirements-for-federal-digital-services/ may be helpful additional sources of information for agencies.

GSA will regularly report on their DotGov Dashboard how agencies are implementing the policies in this Memorandum. To facilitate this reporting and compliance, GSA's Office of Government-wide Policy will stand up a new Council of agency Web/Digital Directors within 30 days of the publication of this memo.

Agencies' management of their public websites and digital services must continue to comply with all relevant Federal laws and policies.

1. Establish Integral Digital Governance

A strong governance structure will help agencies develop coherent priorities, set up lines of accountability, and satisfy the public's expectation of the best possible level of service. Agencies must manage their websites and digital services not as discrete individual IT projects, but as part of a comprehensive strategy covering all their digital information and services.

A. As required in the *Digital Government Strategy*, every agency must establish a plan for governing its digital services, including websites and data. [5]

---

[4] Digital services include the delivery of digital information (i.e., data or content) and transactional services (e.g., online forms, benefits applications) across a variety of platforms, devices, and delivery mechanisms (e.g., websites, mobile applications, and social media).

[5] http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf; requirement 4.2.

B. Each agency must publicly post its governance plan on its Digital Strategy page at www.[agency].gov/digitalstrategy/ and update this page to reflect the current status of the agency's digital governance structure.[6]

2. Use Analytics and User Feedback to Manage Websites and Digital Services

All public facing websites and digital services should be designed around user needs with data-driven analysis influencing management and development decisions. Agencies should use qualitative and quantitative data to determine user goals, needs, and behaviors, and continually test websites and digital services to ensure that user needs are addressed.

A. All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program (DAP) and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs.

B. GSA will maintain a public listing of the domains participating in the DAP and track agency compliance on the DotGov Dashboard.

C. Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*.[7]

D. Agencies can often use the Fast Track clearance process under the Paperwork Reduction Act (PRA) for the collection of service delivery feedback.[8] In particular, the Fast Track process allows agencies to gather timely feedback from users through the following types of voluntary information collections:

- Focus groups;
- One-time or panel discussion groups;
- Customer satisfaction qualitative surveys;
- Post-transaction customer surveys;
- Online surveys;
- Comment cards or complaint forms;
- Moderated, unmoderated, in-person, and remote usability studies; and

---

[6] For standardized webpage locations cited in this memo such as www.[agency].gov/digitalstrategy and others, a similar format should be used if the agency resides on a .mil domain (e.g., www.[agency].mil/digitalstrategy).
[7] https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf
[8] https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-26.pdf

- Testing of a survey or other collection to refine questions.

E. OMB has issued additional guidance, *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act*, and *Flexibilities under the Paperwork Reduction Act for Compliance with Information Collection Requirements*, to clarify the PRA with respect to its existing flexibilities and various types of social media and collaborative technologies that can further help agencies get feedback from users.[9]

3. Make Information Searchable and Discoverable

Search functions are now a universal and expected website feature the public commonly uses to find information. Furthermore, search engine optimization is critical to reaching users who primarily rely on commercial search engines to find information.

A. Agencies' public websites must contain a search function that allows users to easily search content intended for public use. GSA maintains a search solution that meets this requirement and that is available to all agencies at http://search.digitalgov.gov.

B. Agencies must ensure that all content intended for public use on their website can be indexed and searched by commonly used commercial search engines.

4. Provide Open Data Public Engagement

Consistent with OMB Memorandum M-13-13, *Open Data Policy—Managing Information as an Asset*, agencies must disseminate information to the public, structured in a way that enables the data to be fully discoverable and usable.[10] Open and publicly accessible data can increase public participation in government, promote transparency and accountability, and increase government operations' efficiency and effectiveness.

A. Agencies must provide a machine-readable Public Data Listing at www.[agency].gov/data.json in accordance with the Project Open Data metadata schema and a human-readable Public Data Listing at www.[agency].gov/data.[11]

B. Agencies must provide a continually updated Data Publication Process at www.[agency].gov/digitalstrategy.[12]

---

[9] https://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/SocialMediaGuidance_04072010.pdf; https://www.whitehouse.gov/sites/default/files/omb/inforeg/pra_flexibilities_memo_7_22_16_finalI.pdf

[10] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf

[11] https://project-open-data.cio.gov/

[12] This refers to section 3(d) of OMB Memorandum M-13-13, *Open Data Policy*.

C. Agencies must provide a public two-way feedback mechanism available via www.[agency].gov/data.

D. Agencies must provide their existing and new web APIs and relevant open source documentation at www.[agency].gov/developer.

5. Provide Access to Government Information on Multiple Devices

Government information and services should be readily available to the public regardless of device. Agencies must, to the extent practicable, ensure that their public websites and digital services perform equally well on non-desktop devices such as mobile devices and tablets.

A. For new websites and major website redesigns, agencies must ensure responsive design that allows users on non-desktop devices equivalent access to Government information.[13]

B. When determining how to optimize legacy websites and digital services for mobile and other devices, agencies must use customer feedback and analytics to prioritize modernization of the sites and services that are most frequently accessed by users.

6. Protect Privacy

The Federal Government necessarily creates, collects, uses, processes, stores, maintains, disseminates, discloses, and disposes of personally identifiable information (PII) to carry out missions mandated by Federal statute. The review of privacy risks should begin at the earliest planning and development stages of agency actions and policies that involve PII, and should continue throughout the life cycle of the information.

Agencies must be transparent about policies and practices with respect to PII, and must provide clear and accessible notice regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII. This includes maintaining an up-to-date Privacy Program Page on an agency's principal website, posting plain language privacy policies on an agency's websites, mobile applications, and other digital services, providing Privacy Act statements where required by the Privacy Act of 1974, and providing privacy notices for online collections of information where feasible.

A. Privacy Program Page

Each agency must maintain a central resource page dedicated to its privacy program on the agency's principal website. The agency's Privacy Program Page must serve as a central source for information about the agency's practices with respect to PII. The agency's

[13] Responsive design usually refers to website design that automatically adjusts navigation and content presentation to best fit the device (e.g., mobile phone or desktop monitor) on which the content is viewed.

Privacy Program Page must be located at www.[agency].gov/privacy and must be accessible through the agency's "About" page.

1. At a minimum, agencies must include the following on their Privacy Program Page:

   a. System of records notices (SORNs). An agency must list and provide links to complete, up-to-date versions of all agency SORNs. This requires agencies to provide the following:

   - A list of all of the agency's systems of records;
   - Citations and links to all *Federal Register* notices that comprise the SORN for each system of records; and
   - For any SORNs that are comprised of multiple *Federal Register* notices, an unofficial consolidated version of the SORN that describes the current system of records and allows members of the public to view the SORN in its entirety in a single location.

   Agencies must come into full compliance with this requirement as soon as practicable, but no later than 18 months from the issuance of this Memorandum. 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*.

   b. 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.

   c. Matching notices and agreements. Agencies must list and provide links to up-to-date matching notices and agreements for all active matching programs in which the agency participates.

   d. Exemptions to the Privacy Act. Agencies must provide citations and links to the final rules published in the *Federal Register* that promulgate each Privacy Act exemption claimed for their systems of records.

e. **Privacy Act implementation rules**. Agencies must list and provide links to all Privacy Act implementation rules promulgated pursuant to 5 U.S.C. § 552a(f).

f. **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.

g. **Publicly available agency reports on privacy**. Agencies must list and provide links to all publicly available agency reports on privacy.[14] 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).

h. **Instructions for submitting a Privacy Act request**. Agencies must provide instructions in clear and plain language for individuals who wish to request access to or amendment of their records pursuant to 5 U.S.C. § 552a(d).

i. **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.

j. **Contact information for the SAOP**. Agencies must identify their Senior Agency Official for Privacy (SAOP) and provide contact information for his or her office. Agencies may also identify and provide contact information for any component privacy officials.

2. At the discretion of the SAOP, sub-agencies, components, and programs may maintain a sub-agency-, component-, or program-specific privacy program page. If an agency sub-agency, component, or program uses a domain that is different from the agency's domain, the sub-agency-, component-, or program-specific privacy program page must be accessible through www.[sub-agency, component, or program domain].gov/privacy.

   In circumstances where the sub-agency, component, or program uses a domain that is the same as the agency's domain, the sub-agency-, component-, or program-specific privacy program page must be accessible from the sub-agency's, component's, or program's primary webpage. Agencies may include on a sub-agency-, component-, or program-specific privacy program page any of the same resources posted on the agency's central Privacy Program Page. However, doing so does not relieve the agency of the requirement to provide the required resources on the agency's central Privacy Program Page.

[14] Examples of privacy reports include, but are not limited to, annual matching activity reports submitted pursuant to the Privacy Act and reports submitted pursuant to Section 552 of the Consolidated Appropriations Act of 2005, Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, and the Federal Agency Data Mining Reporting Act of 2007.

B. Privacy Policies on Agency Websites

Agencies must post Privacy Policies on their principal, sub-agency, component, and program websites, mobile applications, and other 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. This requirement does not apply to internal agency activities (such as on intranets or online interactions that do not involve the public).

1. A Privacy Policy must:

   a. be written in plain language and organized in a way that is easy to understand and navigate;

   b. provide useful information that the public would need to make an informed decision about whether and how to interact with the agency;[15]

   c. be updated whenever the agency makes a substantive change to the practices it describes;

   d. include a time/date stamp to inform users of the last time the agency made a substantive change to the practices the privacy policy describes;

   e. adhere to all other applicable OMB requirements; and

   f. include a link to the agency's Privacy Program Page.

2. If agencies provide content to children under the age of 13 and collect, maintain, or disclose children's PII, they may be required to comply with the requirements in the Children's Online Privacy Protection Act. Among other things, these requirements include adding a section in the agency's Privacy Policy that pertains to these activities.[16]

C. Privacy Act Statements for Online Collections of Information

A Privacy Act statement is required by law whenever an agency asks individuals to supply information that will become part of a system of records under the Privacy Act.[17] The requirements for a Privacy Act statement are described in the Privacy Act and in OMB guidance.[18] When agencies collect information using an online interface, the agency may need to provide a Privacy Act statement.

---

[15] https://www.whitehouse.gov/omb/memoranda_m99-18/
[16] http://www.business.ftc.gov/privacy-and-security/childrens-privacy
[17] *See* 5 U.S.C. 552a(e)(3)
[18] https://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf

A privacy notice must be provided, whenever feasible, where a Privacy Act statement is not required but members of the public could nonetheless provide PII to the agency using an online interface. 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.

7. Implement Information Security and Privacy Controls

Information technology changes rapidly and agencies must have the flexibility to address known and emerging threats while making continuous improvements.

FISMA and OMB Circular A-130 require each Federal Agency to develop, document, and implement an agency-wide information security program for the information and information systems that support the agency's operations and assets, including those provided or managed by another agency, contractor, or other source.[19] FISMA also provides for the development and maintenance of minimum controls to protect Federal information and information systems. Moreover, OMB Circular A-130 requires agencies to develop, implement, document, maintain, and oversee an agency-wide privacy program including people, processes, and technologies. Each agency-wide privacy program must implement privacy controls and verify that those controls are operating as intended and continuously monitored and assessed.

A. Agencies must follow the policies, principles, standards, and guidelines on information security and privacy, in accordance with FISMA and other laws. Each agency is already required to implement security and privacy policies as set forth in OMB Circular A-130 and National Institute of Standards and Technology (NIST) Special Publication 800-44, *Guidelines on Securing Public Web Servers*; and other associated standards and 800 series guidelines from NIST.[20]

B. All agency domains must be in compliance with OMB Memorandum M-08-23, *Securing the Federal Government's Domain Name System Infrastructure*, and any future updates to identity, credentialing, and access management policy.[21]

8. Use Secure Connections (HTTPS)

The public expects Federal Government websites to be secure and their interactions with those websites to be private. OMB Memorandum M-15-13, *Policy to Require Secure Connections across Federal Websites and Web Services*, requires that all publicly accessible Federal websites

---

[19] 44 U.S.C. § 3554(b)

[20] https://www.whitehouse.gov/omb/circulars_default/ https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf, http://csrc.nist.gov/publications

[21] https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf

and web services only provide service through a secure connection (HTTPS). [22] Unencrypted HTTP connections create a privacy vulnerability and can expose potentially sensitive information that is susceptible to interception, manipulation, and impersonation. This data can include browser identity, website content, search terms, and other user-submitted information.

Federal agencies are already required to deploy HTTPS on their domains following the guidelines in OMB Memorandum M-15-13 and must make all existing websites and services accessible through a secure connection by December 31, 2016. Newly developed websites and services at all Federal agency domains or subdomains must adhere to this policy upon launch. The use of HTTPS is encouraged on Federal intranets.

9. Use Only Approved Domains

Currently, the primary way users quickly determine if they are on an official U.S. Government website is to look for the .gov or .mil designation as part of the domain name.[23] The .gov and .mil domains are widely viewed as zones of increased trust, where the public can confidently access government information and services in a secure environment knowing that the site is legitimate and authoritative. Requiring Federal websites to be part of the .gov or .mil domain instills greater confidence in Federal Agency public websites and digital services.

The requirements laid out in this section serve as the minimum criteria for continued operation on official government domains. Non-compliance with these criteria may jeopardize the integrity and reputation of the agency and the ability to perform its mission.

A. Requests by Executive Branch agencies for new Federal .gov domain names must be approved by the General Services Administration's Office of Government-wide Policy (OGP). OGP will exercise its discretion and authority in considering approvals for new .gov domains and renewals for existing .gov domains, including denying requests for agencies that cannot demonstrate reasonable compliance with the policies identified in this Memorandum.

B. Each agency must use only an approved .gov or .mil domain for its official public-facing websites.

C. The requirement to use only approved government domains does not apply in circumstances where the agency is a user or a customer of a third-party website or service that resides on a non-governmental domain.

---

[22] https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf

[23] This includes Fed.us sites which have already been grandfathered in. There will be no new registrations to Fed.us as it is transitioning to .gov.

D. Within 60 days of this Memorandum's publication agencies must update their list of non-governmental URLs that they operate at http://search.digitalgov.gov/developer/govt-urls.html, and maintain the list up-to-date thereafter.

E. Agencies must migrate all official public facing websites not currently residing on a .gov or .mil domain (excluding agency third-party services), to a .gov or .mil domain within 180 days after the publication of this Memorandum, unless the agency head explicitly determines a non-governmental domain is necessary for the proper performance of an agency function. Agency head determinations for this exception must be sent to: registrar@dotgov.gov.

All requests for new domains and renewals must be submitted by the Federal Agency CIO or equivalent using the process found on http://www.dotgov.gov.

10. Comply with Third-Party Website and Application Requirements

Using third-party services such as social media and collaboration platforms is now a common business practice and helps to create a more robust, user-friendly, and interactive online experience. Agencies may use a third-party website or application at their discretion so long as the agencies comply with all relevant Federal laws and policies.

A. Agency use of third-party websites and applications must have an intended purpose directly related to an agency function that supports its mission.

B. To help confirm the validity of official U.S. Government digital platforms, within 60 days of the publication date of this Memorandum, agencies must register their public-facing digital services such as social media, collaboration accounts, mobile apps and mobile websites, with the U.S. Digital Registry at: http://www.digitalgov.gov/services/u-s-digital-registry/.

C. Agency use of third-party websites and applications must comply with all relevant privacy protection requirements and a careful analysis of privacy implications as specified in OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites*.[24]

D. When choosing which third-party websites and applications to adopt, agencies must review the set of terms and conditions that governs access to and use of such products and services and be aware of terms of service that are incompatible with Federal law or regulations. A list of tools with federal-compatible Terms of Service agreements can be found at: http://www.digitalgov.gov/resources/negotiated-terms-of-service-agreements/.

[24] https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf

E. Federal Acquisition Regulation Clause 48 CFR 52.212-4(u) and OMB Memorandum M-13-10, *Antideficiency Act Implications of Certain Online Terms of Service Agreements*, provides additional guidance for addressing terms of service and user agreements.[25]

11. Ensure Information Quality and Accuracy

The Internet enables agencies to communicate information quickly and easily to a wide audience, which, while of great benefit to society, also increases the potential harm that can result from disseminating incorrect information. Taking this into account, information disseminated from Federal Government websites and digital services, or from third-party services on behalf of the Government, is expected to be authoritative and reliable.

The Information Quality Act applies to all information disseminated from Federal websites, and in certain cases, to information published to third-party sites on behalf of the Government. OMB has published Information Quality Guidelines to help agencies meet this requirement.[26]

A. Information published by an agency must convey a sense of utility, objectivity, and integrity which are defined in OMB's Information Quality Guidelines as:

    1. Utility - The usefulness of the information to its intended users.
    2. Objectivity - Whether the information is presented in an accurate, clear, complete, and unbiased manner.
    3. Integrity - The security of the information from being altered, corrupted or falsified by unauthorized sources.

B. Agencies must be transparent about the quality of the information that they disseminate and must take reasonable steps where practicable to inform users about the information quality of disseminated content, such as:

    1. Clearly identifying the inherent limitations in the information so users are fully aware of its quality and integrity;
    2. Taking steps, when and where practicable, to remove these limitations; and
    3. If necessary, reconsidering whether to disseminate the information if its information quality is not sufficient.

[25] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-10.pdf
[26] http://www.whitehouse.gov/omb/assets/omb/fedreg/reproducible2.pdf

C. The Information Quality Act also applies to third-party publications in cases where the agency is using the third-party service to disseminate information on its behalf or where the agency has the authority to review and approve the information before it's published.

   In cases where members of the public are allowed to post or contribute their own information to a third-party site operated on behalf of the agency (e.g., agency sponsored social media accounts), the agency must ensure that it is clear to the public to the extent practicable:

   1. The inherent limitations of such information and that it is not sponsored by the Federal Government; and

   2. That the same level of utility, objectivity, and integrity found in Federally-sponsored information may not be present.

D. Agencies must include reasonable management controls and establish a review process to ensure that information provided online, and links to any external information, provide a suitable level of information quality as implied by the agency linking to or referencing it from their official website.

E. Agencies must clearly identify external links from their websites, and to the extent practicable update or remove the links when the external information is no longer sufficiently accurate, relevant, timely, necessary or complete.

   1. Agency websites must clearly state that the content of external links to non-Federal Agency websites is not endorsed by the Federal Government and is not subject to Federal information quality, privacy, security, and related guidelines.

   2. Agencies should choose the best approach to identify external links to users in a way that minimizes the impact on the usability of their websites and digital services.

F. Agencies must post information quality guidelines, information quality correction requests, agency's formal response(s), and any communications regarding the appeals on their website. Agencies must also establish a process for updating their information quality web pages on a regular basis.[27]

[27] https://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/info_quality_posting_083004.pdf

12. Ensure Accessibility for Individuals with Disabilities

Section 508 of the Rehabilitation Act was enacted to eliminate barriers in information technology, open new opportunities for people with disabilities, and encourage development of technologies that will help achieve these goals.[28] The law applies to all Federal departments and agencies when they develop, procure, maintain, or use electronic and information technology[29]. Under Section 508, departments and agencies must ensure that employees and members of the public with disabilities have access to information and data that is comparable to access available to others unless an undue burden would be imposed on the department or agency.

A. Agencies must comply with Section 508 and with the Electronic and Information Technology (EIT) Accessibility Standards.[30] Additionally agencies must also adhere to their own Section 508 regulations and policies. Section 508 does not limit rights, remedies, or procedures otherwise available under other Federal laws, including Sections 501, 503, and 504 of the Rehabilitation Act and the Americans with Disabilities Act.[31]

B. Section 508 technical and EIT Accessibility requirements must be included in the requirements document for the procurement of EIT products and services and planned for and built into the development, operations and management lifecycle of a Federal website or digital service. Any new functionality must be regularly tested to ensure it meets the EIT Accessibility Standards and is accessible for persons with disabilities.

C. Agencies must develop accessibility statements for their website and appoint a Section 508 Coordinator as required by OMB Memorandum, *Strategic Plan for Improving Management of Section 508 of the Rehabilitation Act*.[32]

13. Comply with Records Management

All Federal records on agency websites and third-party sites and applications must be properly managed. At a minimum, agencies must be able to identify, retrieve, and preserve Federal Agency records created and maintained on agency websites or third-party sites. These requirements apply until their business use has ended and the records are transferred to NARA or destroyed according to their disposition schedule. Agencies must also manage administrative records that provide evidence of how of their web and third-party programs are managed and operated. Agencies using third-party websites or services are responsible for managing and capturing Federal records created or received on those sites.

---

[28] *See* 29 U.S.C. § 794d

[29] Section 508 does not apply to national security systems, as that term is defined in section 11103(a) of title 40. 29 U.S.C. § 794d(a)(5).

[30] 36 CFR Part 1194

[31] 29 U.S.C. § 794d(g)

[32] https://www.whitehouse.gov/sites/default/files/omb/procurement/memo/strategic-plan-508-compliance.pdf

Agencies are required to comply with all Federal records management laws, regulations, and policies. Additional guidance for agencies on meeting their records management responsibilities can be found at http://www.archives.gov/records-mgmt/ .

14. Use Plain Writing

Web content is most effective when it is easy to understand, find, and use. The Plain Writing Act of 2010 requires agencies to draft all public-facing web and print documents in plain writing, calling for agency writing to be clear, concise, and well-organized.[33] On April 13, 2011, OMB issued Memorandum, M-11-15, *Final Guidance on Implementing the Plain Writing Act of 2010*.

As required by law and OMB guidance, agencies must ensure that web content is written in a manner suitable for the intended audience. The Federal Plain Language Guidelines and other resources maintained by the interagency Plain Language Action and Information Network (PLAIN) at www.plainlanguage.gov can assist agencies in meeting the goals of the Plain Writing Act.

15. Provide Multilingual Content

Agencies must already provide appropriate access for people with limited English proficiency by implementing Department of Justice guidance for Executive Order 13166, *Improving Access to Services for People with Limited English Proficiency*.[34] Agencies must use this guidance to determine which website content must be provided in other languages, based on their agency's mission, analytics, and user feedback.

16. Ensure Access to Mandatory Content

Laws, regulations, or other policies will occasionally mandate that agencies place certain links on their website. Agencies must respect and adhere to these statutory or executive-level mandates and incorporate these requirements in a manner that does not reduce the usability or performance of the agency's website and digital services.

At a minimum, agencies must post links to the following information on the agency's principal website and on any known sub-agency or other major entry points to their site:

A. USA.gov;
B. the website's privacy policy;
C. the agency's Freedom of Information Act webpage;

---

[33] 5 U.S.C. § 301 note

[34] Exec. Order No. 13,166, 65 FR 50121, *available at* http://www.gpo.gov/fdsys/pkg/FR-2000-08-16/pdf/00-20938.pdf

D. a page about the agency with descriptions of the agency organization structure, mission, and statutory authority, and links to the following information:[35]

1. the agency's strategic plan and annual performance plans;
2. the agency's Privacy Program Page;
3. the agency point of contact as required by the Small Business Paperwork Relief Act of 2002;[36]
4. the agency's Open Government Page;
5. the agency's Plain Writing Page;[37]
6. information as required under the No Fear Act of 2002;[38] and
7. information associated with the agency's implementation of the Information Quality Act.[39]

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.

17. Transition to Internet Protocol Version 6 (IPv6)

Agencies must remain up to date with major technical changes in internet protocol.

A. Agencies are already required to upgrade public/external facing servers and services to use native IPv6.[40]

B. Agencies must also ensure that their procurements of networked information technology comply with Federal Acquisition Regulation (FAR) requirements[41] for use of the U.S. Government IPv6 Profile and Test Program for the completeness and quality of their IPv6 capabilities.[42]

---

[35] This refers to the webpage about the agency which is usually referred to as "About", "About Us", "About Agency," or a similar variant.

[36] 44 U.S.C. § 3506(i)

[37] The agency's Plain Writing Page should also continue to be accessible from their Open Government Page per OMB Memorandum, M-11-15, *Final Guidance on Implementing the Plain Writing Act of 2010*.

[38] 5 U.S.C. § 2301 note

[39] This refers to OMB's *Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies* at http://www.whitehouse.gov/omb/assets/omb/fedreg/reproducible2.pdf, and OMB's *Information Quality Guidelines for Peer Review* at https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-03.pdf.

[40] http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf; https://cio.gov/wp-content/uploads/downloads/2012/09/2012_IPv6_Roadmap_FINAL_20120712.pdf; http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf

[41] 48 CFR 11.002(g); *see* 48 CFR 7.105(b)(4)(iii), 12.202(e), and 39.101(e)

[42] *See* NIST SP 500-267, "A Profile for IPv6 in the US Government:" http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf

18. Ensure a Consistent Look and Feel Across Websites

Common user interface components and visual styles help create a seamless transition across an agency's websites and improve the ease with which the public can find information.

Federal Agencies should ensure a consistent look and feel of their public facing websites and digital services.

The U.S. Website Design Standards, found at https://playbook.cio.gov/designstandards/getting-started/, is available to all agencies to assist with this process.