

Social Security Administration's Digital Governance Plan

August 2017



Background

On November 8, 2016, the Office of Management and Budget (OMB) released memorandum [M-17-06, Policies for Federal Agency Public Websites and Digital Services](#). The memorandum makes clear that “federal agency public websites and digital services are the primary means by which the public receives information from and interacts with the Federal Government...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.”

One specific provision of M-17-06 requires that each federal agency “must establish a plan for governing its digital services, including websites and data.”

The Social Security Administration (SSA) has a strong history of effective governance of our digital services. This plan explains our process for how we govern our digital services in these areas:

- Information Technology Investment Process
- Website Governance – Internet Policies
- Social Media Platforms
- Open Data
- Privacy

Information Technology Investment Process

SSA’s Information Technology Investment Process, or ITIP, provides governance that ensures responsible, efficient use of public resources to make IT investments to support digital services, and provides oversight throughout the investment lifecycle. To support investment decisions, ITIP ensures strategic alignment of IT investment proposals to core missions and priorities, and improvement to public and enterprise business processes. Throughout the life of a digital service IT investment, ITIP subject matter experts review progress to monitor performance, and ensure priorities are met through the appropriate use of modern technologies and agency data, that support our changing business processes.

Website Governance – Internet Policies

Throughout SSA, Web Managers are the front line in SSA’s web management. Web Managers are responsible for implementing the agency’s web strategies, policies, standards, and procedures within their organizations, with the guidance and direction of the Web Steering Committee (WESCO). WESCO was established in the 1990s and is co-chaired by representatives from the Office of the Deputy Commissioner for Communications and the Office of the Deputy Commissioner for Operations. WESCO operates under the authority provided by SSA’s eServices Governance Steering Committee (eGSC).

The eGSC is led by an Associate Commissioner-level representative from the Office of the Deputy Commissioner for Communications, the Office of the Deputy Commissioner for Operations, and the Office of the Deputy Commissioner for Systems. Membership of eGSC is comprised of Associate Commissioner-level representatives from numerous SSA offices.

Each Deputy Commissioner's office and other agency-level offices name a Web Manager to manage content development and carry out other web management functions in that organization. Likewise, each Regional Component names a Web Manager for the Region.

These Headquarters and Regional Web Managers work with their respective office heads to develop and use procedures within the organization to create and approve content, and carry out other web management responsibilities.

SSA's internet policies for web governance are available online at www.ssa.gov/instructions/governance/policies.html. These policies address many important governance areas, including, but not limited to, web page certification, linking, privacy, web browser testing, and much more. All SSA Web Managers are required to follow these internet policies.

Social Media Platforms

We use social media to share information with the public about our programs and services, and we use a variety of social media platforms to expand our reach. Engaging with the public is also important us; we use social media to listen and respond to our customers' questions and comments where appropriate. The Office of Communications (OCOMM) develops and manages content of and responds to comments on the agency's primary social media accounts. OCOMM collaborates with several other agency components on social media governance issues, including the Office of the General Counsel and the Office of Systems, including its records management staff.

Our [Social Media Hub](#) details our significant social media presence with names and descriptions for each of our 18 channels on our blog, Facebook, Twitter, Google Plus, YouTube, and LinkedIn.

We developed our [Social Media Policy](#) in September 2014. That policy document is available at our [Social Media Hub](#). We are currently updating the policy and will post the revised policy document when completed. The current policy document covers several important topic areas, including:

- Roles and Process
- Monitoring and responding to comments
- Rules for employee use of our social media sites as it relates to official use and personal use
- Prohibited content
- Authorities and References

Also available on our [Social Media Hub](#) is our [Negotiated Terms of Service for Social Media Tools](#). A federal-compatible Terms of Service (TOS) agreement is required for official government use of social media tools. This web page details:

- Services for which SSA has signed an addendum to the standard terms of service; or
- Services for which the General Services Administration (GSA) has negotiated federal-compatible TOS agreements that do not require SSA to execute a signed addendum prior to use.

Open Data

SSA collects a variety of data about people to help us carry out our mission, including workers' earnings, their employers, identifying information, addresses, data about the programs we administer, and more. For more than 80 years, we remain committed to protecting the data entrusted to us through policy, training, and technology. We follow strict rules that determine what we can and cannot share, whether protected by the Privacy Act, Internal Revenue code, HIPAA, statutes, or Executive Order.

On May 9, 2013, the Office of Management and Budget issued [Memorandum M-13-13. M-13-13](#) directed agencies to create and maintain an enterprise data inventory and to identify in a public data listing those data resources that have or can be released to the public. SSA published its [Data Page](#), at which the public can browse and download more than 1,700 different data sets. All of our open data activities are carefully performed to ensure that privacy and confidentiality are fully protected and that data are properly secured. The data we make available through the Open Data initiative does not contain personally identifiable information.

Privacy

One of our most important responsibilities is protecting your personal information and your financial contributions. We use state-of-the-art systems for this. We are committed to safeguarding the information and resources entrusted to us. Our [Privacy Program page](#) documents our privacy compliance program. Below is a list of privacy topics related to digital governance, accompanied with a brief summary. Please refer to the [Privacy Program page](#) for details.

- The Privacy Act of 1974 – The Act is the federal law that governs our collection and use of records we maintain about a person in a system of records. A system of records is any grouping of information about an individual under the control of a Federal agency from which information is retrievable by personal identifiers, such as name, social security number, or other identifying number or symbol.
- System of Records Notices - The Privacy Act of 1974 (5 U.S.C. 552a) requires each federal agency to publish a notice in the Federal Register of each system of records that it maintains.

A system of records is any grouping of information about an individual under the control of a Federal agency from which it retrieves information by the name, Social Security number, or some other personal identifier.

- Privacy Act Exemptions - The Privacy Act of 1974 (5 U.S.C. § 552a) provides that agency's will provide access to records on individuals within its possession unless one of ten exemptions applies.
- Privacy Act Implementation Rules - In accordance with the Privacy Act (5 U.S.C. § 552a), federal agencies are required to implement various agency rules pursuant to 5 U.S.C. § 552a(f).
- Submit a Privacy Act Request - Under the Privacy Act of 1974 (5 U.S.C. § 552a(d)), you have the right to request access to, or amendment of records about yourself that are in our systems of records.
- Privacy Impact Assessments (PIAs)- Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36) requires that the Office of Management and Budget issue guidance to agencies on implementing the privacy provisions of the E-Government Act. The E-Government Act requires agencies to conduct PIAs for their electronic information systems and collections. Agencies must make these PIAs publicly available. The list of PIAs SSA has conducted is available online.
- Computer Matching Programs - Pursuant to the Privacy Act of 1974 (5 U.S.C. § 552a), a computer matching program is required for any computerized comparison of two or more automated systems of records, or a system of records with non-Federal records, for the purpose of establishing or verifying eligibility of, or compliance with, statutory and regulatory requirements by applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to cash or in-kind assistance or payments under Federal benefit programs.
- Privacy Policies and Reports – A list of privacy reports and privacy policies is available.