GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2160.1G
June 7, 2024

GSA ORDER

SUBJECT: General Services Administration (GSA) Information Technology (IT) Standards Profile

1. Purpose. The IT Standards Profile is the official GSA repository of all approved software applications. It is managed by GSA IT and can be found internally at GSA at ea.gsa.gov.

a. To ensure that acquisition and use of information technology (as defined in paragraph 3. below) adhere to the IT Standards Profile.

b. To ensure the correctness, completeness, and currency of the IT Standards Profile through the definition of roles, responsibilities, and processes for IT Standards Profile governance and maintenance.

c. In order to be listed as approved software at GSA, it must undergo review through the IT Standards process. To learn more about, or start this process, applicable GSA employees should start the process as explained on this internally available IT Standards website.

2. Background. OMB M-16-12, Category Management Policy, Improving the Acquisition and Management of Common Information Technology: Software Licensing, dated June 2, 2016, directed agencies to develop processes and guidelines to manage software consistent with OMB policies and guidance, including OMB circular A-130 and the Federal Acquisition Regulation, considering such factors as performance, security, privacy, accessibility, interoperability, and the ability to share or re-use software.

3. Applicability.

a. This Order is applicable to GSA Service and Staff Offices (SSOs) and Regions acquiring or using information technologies in the conduct of GSA business.

b. This order is applicable to the Office of Inspector General (OIG) only to the extent that the OIG determines it is consistent with the OIG's independent authority under the Inspector General Act and it does not conflict with other OIG policies or the OIG mission.

c. This Order applies to the Civilian Board of Contract Appeals (CBCA) only to the

extent that it is consistent with the CBCA's requisite independence as defined by the Contract Disputes Act (CDA) and its legislative history

d. Information technologies within the scope of this policy are: applicable software and applicable cloud services as defined below.

(1) Applicable software means:

a) software installed on GSA-furnished equipment such as laptops, mobile devices, or servers that are managed or packaged software requiring privileged access to install onto Government furnished laptops and servers.

b) Software libraries, application program interfaces, binaries, protocols, and related standards that can be installed without administrator-level access or are included as part of higher level packaged software (e.g. Operating systems, Open Source Software and Commercial off-the shelf programs, etc.) are excepted and determined to be approved as part of the higher level software package itself.

(c) Applicable software includes mobile applications available through the GSA application catalog or developed by, for, or on behalf of GSA.

(2) Applicable cloud services include: Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Low Impact Software as a Service (LiSaaS), Moderate Impact Software as a Service (MiSaaS) and Fedramp Authorized software.

e. This Order is applicable to the Internet of Things (IoT) Devices which are defined as devices that have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world. (references: NIST IR 8425 and the Internet of Things Cybersecurity Improvement Act of 2020 (IoT Act) (Public Law 116-207).

f. Collaboration with another agency through software or cloud services which they use for managing non-GSA data (either data owned by that agency or public data) does not require security or Section 508 compliance review, as that responsibility is assumed by the providing agency. Other policies which may restrict the use of GSA Enterprise Accounts or the release of GSA-owned data may still apply.

3. Cancellation. This Order cancels CIO 2160.1F CHGE 3 GSA Information Technology (IT) Standards Profile dated November 27, 2023.

4. Explanation of changes.

a. Added additional software approval requirements based on M-22-18, M-23-16, and GSA Acquisition Letter MV-23-02 Supplement 2.

5. Responsibilities.

a. Office of GSA IT. GSA IT is responsible for the IT Standards Profile.

b. Chief Technology Officer (CTO). The CTO's office within GSA IT has approval authority for changes to the IT Standards Profile. The CTO has primary responsibility of the management of the process and ensuring IT Standards are reviewed for use within GSA. The CTO also has responsibility for maintaining the authoritative list of IT Standards and its associated metadata, currently maintained at the GSA Enterprise Architecture Analytics and Reporting (GEAR) website (ea.gsa.gov). The IT Standards Team is within the CTO's office.

c. Security. The Office of the Chief Information Security Officer (OCISO) within GSA IT is responsible for reviewing the information technology for security vulnerabilities as well as other risks to the GSA network.

d. Enterprise Data & Privacy Management Office. The Section 508 Division within this office in GSA IT is responsible for reviewing the Accessibility Conformance Reports (ACR) that are required for new software requests. The ACR is a representation of how the product meets the applicable Section 508 Technical Standards for accessibility. In addition, the Records Management Division within this office in GSA IT is responsible for reviewing whether software being requested may create or store records, and if so, notifies requesters so that implementers and users can take any necessary recordkeeping actions.

e. Acquisition.

(1) The Contracting Officer (CO) or Purchase Card Holder responsible for acquiring the IT software or cloud services shall review, negotiate, and determine acceptability of any Commercial Supplier Agreement (CSA). FAQs for GSA acquisition personnel regarding CSAs are found here on GSA's Acquisition Portal. COs and Purchase Card Holders should seek guidance from their assigned legal counsel if they are unsure about the meaning and effect of terms in the agreement.

(2) Internet of Things (IoT) devices cannot be procured unless a review of the contract by the CIO identifies that it complies with NIST SP 800-213 or the CIO grants a waiver under one of the conditions of the IoT Act. Any waivers must include the elements identified in the IoT Act and be sent to the GSA Administrator. Questions regarding waivers should be directed to it-standards@gsa.gov.

6. Compliance. Information technologies may be used in the GSA IT environment if approved for use in the IT Standards Profile.

a. No software can be acquired until it has been through the IT Standards process and has been approved.

b. The criteria for considering an information technology to become a standard product include the following:

(1) Whether an existing information technology standard product can meet the requirements in an effective manner that is optimized for programmatic, business and technical needs;

(2) Whether the product is attached to an existing solution;

(3) The projected life cycle of the proposed product including all associated deployment, operations and maintenance requirements; and

(4) Related practical considerations.

c. In order for an information technology to become an approved IT standard, it must undergo GSA's security, Section 508, Records Management, and Secure Software Development Attestation reviews as well as CTO approval as determined by formal review.

Before it can be acquired, or as part of the acquisition process, all new software must have a Software Attestation, an M-22-18-specific Plan of Action and Milestones (POA&M), or waiver in place that complies with OMB M-22-18 and M-23-16 and GSA Acquisition Letter MV-2023-02 Supplement 2. Software previously acquired must obtain an attestation, POA&M or waiver by following the procedures outlined on the IT Standards website (https://sites.google.com/a/gsa.gov/it_standards/it-standards).

There are two mechanisms for initiating an information technology request:

(1) When an information technology is being introduced to a production environment or for a known value to the enterprise, a request for desktop software/ server software/cloud SaaS approval can be initiated through the IT Service Desk; and

(2) When the feasibility or applicability of an information technology is not known or not yet proven, a pilot project can be conducted, in close coordination with the CTO's office, to explore the usability of the new technology. A pilot request for desktop software/server software/cloud SaaS can be initiated through the IT Service Desk.

(a) In order for the requested information technology to be considered a pilot project, it must meet the following criteria:

1. The usage must not be on a GSA production environment or have technical integration with GSA production systems;

2. Piloted systems/environments shall not store or process Federal data and to the greatest extent possible focus on 'dummy' information to determine the operation/feasibility of the piloted solution. Data that is already in the public domain is permissible; the piloted system shall not be the authoritative source of this information;

3. The cost of the technology may not exceed $25K;

4. The number of people in the user pool must be limited to a number jointly agreed upon, in advance, by the CTO and the requesting group, as appropriate to the functionality being delivered; and

5. The duration of the pilot may not exceed 90 days.

(b) Security reviews for pilots are optional, at the discretion of the OCISO, and may be conducted concurrently with the pilot project. The purpose of the security review for pilot projects is to determine the steps necessary, if any, for the piloted technology to be able to become a fully approved technology.

(c) At the conclusion of the pilot, the requester will provide to the CTO the following key outcomes:

1. Determination of whether or not the requester believes that the piloted technology is acceptable and should be a candidate for full approval;

2. Path to attain full security and Section 508 approval; and

3. Evidence that all costs have been identified and budgeted within the requesting office and as required by other affected offices, to include out-year operations and maintenance.

d. Exceptions to this policy may be granted by the CTO on a case by case basis. Requests for exceptions shall be sent to it-standards@gsa.gov.

7. Signature.

/S/_____
DAVID SHIVE
Chief Information Officer
Office of GSA IT