GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2160.1F CHGE 2
March 31, 2017

GSA ORDER

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

1. Purpose. To ensure acquisition and use of standard information technologies and proper maintenance of the IT Standards Profile. The IT Standards Profile is the official GSA repository of all approved software applications. It is managed by GSA IT and can be found at ea.gsa.gov.

a. To ensure that acquisition and use of information technology (as defined in paragraph 2. 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.

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

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

d. Applicable cloud services include: Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS).

e. 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 CHGE1 GSA Information Technology (IT) Standards Profile dated January 23, 2017.

4. Explanation of change paragraph. Responsibility for the IT Standards Profile is hereby transferred from the Enterprise Architecture team to the Chief Technology Officer. The policy is being updated to reflect this change.

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's office will coordinate with the Technology Standards Committee (TSC) as appropriate. 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. Technology Standards Committee (TSC). The TSC will continue to be the body that reviews and provides recommendations on proposed IT Standards to the CTO.

d. 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.

e. Section 508. The Section 508 team within GSA IT is responsible for reviewing the compliance of the information technology by way of the voluntary product accessibility template.

f. GSA staff. A GSA employee may initiate requests for changes to the IT Standards Profile. The process for requests can be found on the IT Standards Webpage on InSite.

g. Acquisition. 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), to include Terms of Service (TOS) and End User License Agreements (EULAs). Acquisition Letter MV-15-03 and Supplement #1 provide guidance for negotiating CSAs. As part of the IT Standards Process, requesters will be directed to send the CSA to his or her servicing CO or Purchase Card Holder. The CO or Purchase Card Holder shall review, negotiate, and

approve the CSA prior to acquiring the requested IT software or service. CO 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. For free IT software or services, the CTO's office will coordinate with the requester, the Office of General Counsel, and the vendor to ensure CSAs are reviewed, negotiated, and approved.

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

a. GSA program managers are responsible for ensuring that their programs are compliant with the IT Standards Profile and policy, in accordance with CIO 2160.1 Information Technology (IT) Integration Policy. 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. The IT Standards Team conducts an initial analysis and provides results to the TSC. The TSC incorporates recommendations from across GSA IT and proposes actions to the CTO.

d. In order for an information technology to become an approved IT standard, it must undergo GSA's security and Section 508 reviews as well as CTO approval as determined by formal review. 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 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;

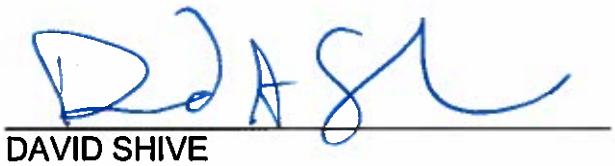
2. Path to attain full security and Section 508 approval; and

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.

f. More details about the formal IT Standards approval process can be found on the IT Standards webpage on InSite.

g. Exceptions to this policy may be granted by the CTO on a case by case basis. Requests for exceptions shall be sent to cto@gsa.gov.

7. Signature.



DAVID SHIVE
Chief Information Officer
Office of GSA IT