U.S. General Services Administration (GSA)

GSA Order: General Services Administration (GSA) Information Technology (IT) Standards Policy

CIO 2160.1H
Office of the Chief Technology Officer
cto@gsa.gov

Purpose:

The IT Standards Policy 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.

The GSA EA Analytics & Reporting (GEAR) is the official GSA repository for all software applications (approved, denied, retired, etc.). It is managed by GSA IT and can be found internally at ea.gsa.gov.

1. To ensure that acquisition and use of information technology adhere to the IT Standards Policy.
2. To ensure the correctness, completeness, and currency of the IT Standards Policy through the definition of roles, responsibilities, and processes for IT Standards governance and maintenance.
3. In order to be listed as approved software at GSA, it must undergo review through the IT Standards approval 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.
4. To ensure pilots are safe, secure, and comply with applicable laws, regulations, and policies.

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.

Applicability:

This Order applies to all GSA employees as they perform their duties with the following exceptions:

1. This Order applies 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.
2. This Order applies to the Civilian Board of Contract Appeals (CBCA) only to the extent that the CBCA determines it is consistent with the CBCA's independent authority under the Contract Disputes Act, and it does not conflict with other CBCA policies or the CBCA mission.
3. 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.
4. Information technologies within the scope of this policy are: applicable software and applicable cloud services as defined below.
    - Applicable software means:
        a. Software installed on GSA-furnished equipment (GFE) 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.
    - 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.

5. 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).

6. 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.

Cancellation:

This Order cancels and supersedes CIO 2160.1G, General Services Administration (GSA) Information Technology (IT) Standards Profile and CIO IL-24-02, Software Pilots.

Summary of Changes:

1. Incorporated language from CIO IL-24-02 Software Pilots.
2. Made other minor editorial updates.
3. Updated document to conform with OAS 1832.1C.

Roles and Responsibilities:

1. **Office of GSA IT**. GSA IT is responsible for the IT Standards Policy.

2. **Chief Technology Officer (CTO)**. The CTO's office within GSA IT has approval authority for changes to the IT Standards Policy. The CTO has primary responsibility of the management of the process and ensuring IT Standards are reviewed before 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. The CTO shall be responsible for overseeing the pilot process.

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

4. **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.

5. **Acquisition**.

    a. 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.

    b. 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.

Signature

/S/_____ 8/27/2025_____

David Shive
Chief Information Officer
Office of GSA IT

Date

1. IT Standards Compliance

Information technologies may be used in the GSA IT environment if approved for use through the IT Standards Approval Process.

1.1. No software can be acquired until it has been through the IT Standards approval process and has been fully vetted.

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

- Whether an existing information technology standard product can meet the requirements in an effective manner that is optimized for programmatic, business and technical needs;
- Whether the product is attached to an existing solution;
- The projected life cycle of the proposed product including all associated deployment, operations and maintenance requirements; and
- Related practical considerations.

1.3. 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.

1.4. 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).

1.5. There are two mechanisms for initiating an information technology request:

- 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

- 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. See sections below for details on how to conduct a pilot.

2. Conducting Pilots

2.1. When the feasibility or applicability of new information technology is not known or not yet proven, a pilot project can be conducted to explore its use and build a case to become an approved IT Standard.

- If software is not already approved for use, a pilot must be conducted if it is intended to address new user or business requirements.
- A pilot need not be conducted for new software that addresses pre-existing requirements for which there is already a solution in place, or where existing software gains new features resulting from a change implemented by the vendor.
- Exploratory pilots may be conducted to evaluate emerging technology for which there is no current business requirement.

2.2. All new technology software pilots, including hardware with software/firmware components and those leveraging cloud services, must be conducted in close coordination with the Office of the Chief Technology Officer (OCTO) and the Technology Standards Pilot Committee (TSPC) established herein. Pilot requests should be initiated through the IT Service Desk, which will be reviewed by the TSPC. The process and requirements for pilots shall be as follows:

3. The Technology Standards Pilot Committee

3.1. Pilot proposals shall be reviewed by the TSPC, which shall be established and led by the Chief Technology Officer (CTO). The TSPC will evaluate all pilot proposals, set each pilot's limitations as appropriate to the specific technology being piloted, and determine what type of security review is required. The committee will determine whether or not, and with what restrictions, the pilot may proceed. If the pilot proposal is denied, the committee shall provide the reason(s) for the denial.

3.2. In evaluating a pilot proposal, the TSPC shall consider the following factors and apply limitations as necessary:

- Total amount of money that can be spent on the technology during the pilot, including expected labor costs.
- Duration of the pilot.
- Redundancy with other existing technology.
- Likelihood the technology will adequately address the business problem.
- Risks posed by piloting the technology.
- Whether, if successful, the technology's procurement for long-term use would be permitted under procurement rules, regulations, and laws.
- Appropriate security requirements as determined by the TSCP.
- If use of any federal data is authorized for use during the pilot and the risk

acceptance/mitigation is sufficient.
- Any additional restrictions required to ensure the safe, secure, compliant, equitable, and appropriate piloting of the technology.
- For cloud services, if not FedRAMP authorized, ability to fund FedRAMP sponsorship for the requested technology.
- Identify key GSA IT teams or individuals with whom the piloting team must coordinate.
- Any additional reporting required of the proposing team beyond those outlined below in Section 4.3 below.

4. Piloting Teams' Responsibilities

4.1. Teams seeking to pilot software must submit a written pilot proposal.

4.2. To initiate a Pilot Proposal, complete and submit the Technology Standards Pilot Committee (TSPC) Pilot Project Request Form. With their proposal, teams must where applicable:

- Identify the specific hardware and/or software that will be evaluated.
- Propose a budget and timeline, including any associated cloud or infrastructure support costs.
- Identify all key business objective(s) sought through the use of the technology, and show that if successful, the technology will sufficiently meet all intended requirements at implementation.
- Identify which individuals/users will use the pilot technology, and limit them to the minimum number required to evaluate it. These users must be identified in advance of the pilot; however, through mutual agreement between the TSCP and proposing team, the user group can be modified during evaluation as needed.
- Create success metrics by which the pilot will be evaluated.
- Address all additional applicable TSPC consideration factors identified in Section 3.2 above.
- Identify any software (e.g. cloud sandboxes), hardware, or other technical resources required to conduct the pilot. Complete a thorough market research and competitive analysis driven by clearly defined and documented requirements that explains the research procedures undertaken and stands up to expert scrutiny. Depending on pilot execution strategy, the analysis must identify which vendor or vendors are among those being considered for, or have been selected for, the pilot, and the justification for their inclusion or potential inclusion in the pilot. All applicable acquisition regulations and other legal requirements must be followed.
- Consult with OCISO C-SCRM team to ensure the piloted technology complies within the secure cyber supply chain risk management framework.
- Include a risk management plan approved by the TSPC to mitigate or

accept any risks stemming from their use of Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), any other federal data, and any integration with GSA production systems if applicable.
- Anything else required by the TSPC in order to evaluate the proposal.

4.3. Pilots cannot proceed without a Decision Memo issued by the TSPC. While conducting the pilot, piloting teams must:

- Keep the CTO team apprised of key milestones, as mutually agreed upon at the project's outset.
- Alert the CTO team, Office of Digital Infrastructure Technologies POC, and appropriate Information System Security Manager (ISSM) of any potential security risks, either theoretical or realized, once identified. Incidents shall be immediately reported to the GSA Incident Response Team through the GSA IT Service Desk.
- Propose any changes to the TSCP to the pilot's scope before deviating from the approved scope.

4.4. At the conclusion of the pilot, piloting teams must provide the TSPC with a pilot close-out document detailing the following:

- A determination of whether or not the requester believes that a piloted technology is an acceptable solution to the stated business problem, including the timeframe for which the technology is expected to remain suitable.
- Where applicable, a report of the pilot's findings/outcomes that includes a comprehensive analysis of alternatives comparing the piloted technologies, existing solutions, and the consequences of implementing none of the evaluated solutions.
- 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.
- A proposed path to attain full security, Section 508, and records management approval, if sought.
- A statement, developed with the IT security team, identifying any security risks or blockers the piloted technology would present in the event full approval is sought.
- For SaaS pilots, where the proposed software would require FedRAMP authorization, the piloting team is encouraged to engage with the vendor to determine if they intend to pursue FedRAMP; however, the piloting team may not commit to sponsoring the technology without the explicit approval of the CIO and CISO.

5. Exploratory Pilots

5.1. Where neither a new business requirement exists nor an existing

solution is in place, an Exploratory Pilot may be proposed. Exploratory pilots:

- Are appropriate for conducting research into emerging technologies for which there is not a current stated need, but a need is expected in the future.
- Must follow the same approval process.
- Need not produce the same close-out documentation (although the nature of the required close-out must be defined in the proposal phase).
- Because they are not being measured against a requirement, by definition they do not provide sufficient analysis of alternatives documentation for full approval as an IT Standard.

6. AI Pilots

6.1. If the piloted technology uses AI, it must also be approved by the AI Safety Team via the process defined in the Use of Artificial Intelligence at GSA, Section 2.2 “New or Proposed AI Use Cases.”

7. Additional Policies

7.1. All pilots must comply with GSA IT Security Policy, IT Rules of Behavior, the Order for the Use of Artificial Intelligence at GSA, Section 508 requirements, and Records Management requirements.

8. Exceptions

8.1. Exceptions to this policy, in whole or in part, may be granted by the CTO on a case by case basis. Requests for exceptions shall be sent to cto@gsa.gov.