GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO IL-14-03

GSA INSTRUCTIONAL LETTER

SUBJECT: Information Technology (IT) Integration Policy

1. Purpose. To set forth policy for integrating key IT principles when planning and managing IT solutions developed for or operated by GSA. This policy has been developed to assure that solutions are compliant with GSA IT standards; these standards are addressed as early as possible during project and acquisition planning activities; and GSA IT is engaged throughout the project lifecycle.

2. Background. In accordance with the Clinger-Cohen Act of 1996, the GSA Chief Information Officer (CIO) provides IT policy, planning, programming, and budgeting guidelines for IT investments. This guidance is consistent with acquisition management guidance in the Federal Acquisition Regulation (FAR) and the GSA Acquisition Manual (GSAM).

3. Objectives. Objectives of the Key IT Principles Integration policy are to:

- Describe a set of key IT principles that require compliance when IT solutions are planned, developed, operated and retired.

- Mandate that these key IT principles apply to **all internal GSA IT projects** (new or existing), **regardless of budget source**, size, complexity or significance, in all of its life cycle phases. *(Note: This IL applies to all GSA internal IT engagements, not just those funded by GSA IT.)*

- Establish a requirement that ensures GSA staff initiating a new IT project or initiating a major enhancement to an existing IT project are responsible for compliance with the Key IT Principles defined by the GSA IT Vendor Management Office (VMO) and GSA IT Service Portfolios (i.e. Office of the Chief Technology Officer (ID), Infrastructure Enterprise Operations (IO), Information Security (IS), Enterprise Operations, Planning and Governance (IE), and Government-wide and Enterprise Solutions (IA)).

- Establish the expectation that GSA staff are working with the GSA IT Vendor Management Office (VMO), the GSA IT Service Portfolios and the GSA Business Capability Portfolios (i.e. Workspaces IT Services (IP), Financial and HR IT Services (IB), Acquisition IT Services (IQ)) as needed to ensure compliance.

- Foster a pro-active project planning culture to reduce risk and project failure and to identify and address IT compliance issues as early as possible.

- Support effective resource management, acquisition, and budget planning.

- Help position the agency to meet current and future business requirements while also complying with Federal mandates (e.g. Cloud First, Digital Strategy), GSA goals (i.e. Savings, Efficiency, Service), and GSA IT commitments.

4. Scope and applicability.

   - This policy applies to acquisition, planning, development, maintenance, enhancement, operation and disposal of IT systems and solutions of any size, complexity, or significance that should be considered part of the agency's IT portfolio as defined in GSA Policy CIO 2135.2B GSA IT Capital Planning and Investment Control.

   - This policy applies to all GSA IT project managers, system owners, and other staff responsible for defining, delivering, operating, supporting, and retiring IT systems and solutions.

   - This policy 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 IG Act and it does not conflict with other OIG policies or the OIG mission.

5. Policy.

   - General guidelines.

     - The policy applies to **any new, internal GSA IT solution**, regardless of budget source, size, complexity or significance, in all of its life cycle phases. *(Note: This IL applies to all GSA internal IT engagements, not just those funded by GSA IT.)*

     - This policy applies to **any major enhancement effort** related to an existing project that meets the following criteria:

       - All IT efforts valued over the simplified acquisition threshold (currently $150K), excluding license renewals, production support activities, and basic operational activities.

       - Any cloud acquisition, regardless of dollar value.

       - Any proposed Blanket Purchase Agreement (BPA) for IT products or services, regardless of dollar value.

       - Requests for Information (RFI) and other market research initiatives related to IT initiatives.

       - Strategic or high-priority IT acquisitions.

     - All solution development, modernization, and enhancement efforts are to ensure compliance with the Key IT Principles. Failure to follow this policy may result in unacceptable deviations from planned cost, schedule, and performance expectations, and could ultimately result in project termination.

     - The policy requires integration of compliance-based processes and controls specific to the Key IT Principles identified above, appropriately scoped to ensure effective management control and authority over IT projects.

- The proper integration of the Key IT Principles requires coordination with the GSA IT (i.e. Office of the Chief Technology Officer (ID), Infrastructure Enterprise Operations (IO), Information Security (IS), Enterprise Operations, Planning and Governance (IE), and Government-wide and Enterprise Solutions (IA)).

- The GSA IT VMO must approve all IT acquisition packages and will provide guidance to ensure the proper contracting language pertaining to the Key IT Principles is appropriately included.

- Although the GSA IT VMO will assist in providing coordination support between IT Project Teams and the various IT Service and Business Portfolios, as described above, it is ultimately the responsibility of the IT Project teams to own this collaboration and ensure compliance with the Key IT Principles. A supplemental guide providing guidance on the implementation of the Key IT Principles will follow to outline how this process will work.

- Key IT Principles. The following information identifies the eight Key IT Principles that must be addressed **for all new and existing,** (per the criteria defined above), IT projects.

  - Single Sign On Shared Service Team engagement. The Single Sign On Shared Service team is the authority responsible for managing the Single Sign On strategy and associated solution options available within GSA. One of the largest challenges for GSA IT, however, is early and consistent engagement with the Single Sign On Shared Service team throughout the project to understand their solution options, which needs to be engaged to implement the solution, and how this impacts the project schedule. It is the responsibility of the Single Sign On Shared Service team to determine, in conjunction with the project team, which Single Sign On solution is most appropriate for an IT application.

  - Cloud First. The Cloud First policy mandates that agencies take full advantage of cloud computing benefits to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize cost. Any new GSA IT solution being proposed should implement a cloud-based solution whenever a secure, reliable, cost-effective cloud option exists. There are many considerations and standards, however, which must be taken into account when implementing a cloud solution to include: hosting approaches, architecture standards, and security processes. Approaches and standards specific to cloud based solutions, therefore, have been developed by the GSA IT Service Portfolios. It is the responsibility of each of these service portfolios, therefore, to approve the approach being utilized for cloud based solutions as it pertains to their particular areas of expertise.

  - Open Source Software (OSS). GSA strongly encourages the development and procurement of open source software (OSS). OSS makes its source code publicly available, under licenses that allow use, copying, modification, and redistribution. All software developed internally within GSA, therefore, whether directly by GSA staff, or by contractor staff via a contract to acquire such services (with the exception of pre-existing Intellectual Property belonging to the contractor,) will be published as OSS to the extent practicable. As part of OSS development efforts, developers are required to use the latest, stable release of OSS. When mature, patched releases of OSS are made available, developers will incorporate the new secured/patched release into the code. Submission of OSS code will be in accordance with the product manager's code management practices.

When procuring new or modifying existing technology stacks, GSA shall give priority consideration to acquiring OSS tools to the extent practicable. In these cases, all future contracts for development of software must include language to ensure that all data rights to the software belong to GSA, and GSA has the ability, when appropriate, to publish resulting solutions as OSS. For more information about OSS, please see these best practices for developing OSS.

- Enterprise Information and Data Management Team (EIDM). The EIDM team is the authority for establishing GSA enterprise data management policies and standards at GSA to include: Metadata Management, Data Sourcing, Data Quality, Enterprise Data Warehouse (EDW), Data Mart/ETL, and Business Intelligence (BI) solutions/activities. They are also responsible for ensuring GSA compliance with federal agency data management related initiatives that include coordinating and facilitating the prioritization and clearance process for centralizing the release of data to the public (data.gov or other "open data" initiatives).

- Digital services. Digital services refer to the online delivery of U.S. government information and services. The GSA Office of Citizen Services and Innovative Technologies (OCSIT) provides government-wide support and solutions that help agencies deliver excellent customer service to the public via web, social media, mobile, phone, email, print, and newly evolving media. OCSIT also maintains digitalgov.gov, which facilitates the dissemination of this information, to include compliance requirements associated with digital services. Projects that have a digital services component must access digitalgov.gov and ensure compliance with the Checklist of Requirements for Federal Websites and Digital Services. This checklist lays out high-level requirements for federal public websites and digital services, and the current laws, policies, and regulations related to each requirement. Project teams should review their websites and digital products and services against this list on a quarterly basis, to make sure all digital products comply with the latest requirements.

- Records management. Federal law requires all Federal agencies to create and preserve records that adequately and properly document "the organization, functions, policies, decisions, procedures, and essential transactions of the agency" (44 U.S.C. 3101). In accordance with the Clinger-Cohen Act, codes and regulations such as 44 U.S.C chapters 21, 29, 31 and 33; Freedom of Information Act (5 U.S.C. 552); Privacy Act (5 U.S.C. 552a); and 36 CFR Part 1222 and Part 1228, the objectives of the internal GSA Records Management Branch are to:

  - Create and preserve records documenting the organization, functions, policies, decisions, procedures, and transactions of GSA; also, records necessary to protect the legal and financial rights of the Government and of persons affected by GSA's activities (44 U.S.C. 3101).

  - Implement the full lifecycle of information management from creation or acquisition through its final disposition. This includes organizing, categorizing, classifying, disseminating, and migrating information.

  - Apply standards, procedures, and techniques established by GSA and National Archives and Records Administration (NARA) to improve the management of records.

  - Provide control schedules for the cutoff, retirement, and destruction of records (44 U.S.C. 3303).

- Prevent the unauthorized removal or destruction of GSA records (44 U.S.C. 3105).

- Support the creation, use, and management of electronic records as directed by OMB and the President (OMB Memorandum M-12-18).

- Access and ensure compliance with those projects that have a records management component as per GSA OAS P 1820.1 Records Management Program and Policy.

- IT Security engagement. The IT Security team (IS) is the authority responsible for ensuring IT solutions are compliant with federal and GSA security standards. The number of and complexity associated with the implementation of security requirements and finalizing of related documentation, however, varies among IT projects. One of the largest challenges for GSA IT is early and consistent engagement with the IT Security team throughout the project to understand what security requirements apply, who needs to be engaged to assist in implementation, and how this impacts the project schedule. It is the responsibility of the IT Security team to determine, based upon input from the project team, the IT Security requirements that require compliance.

- IT Vendor Management Office (VMO) engagement. One of the functions of the IT VMO is to promote IT standardization and establish management controls for new IT procurements to enable stewardship of IT funds and ensure alignment of IT purchases to agency business and technology strategies. The IT VMO accomplishes this by providing compliance based resources, such as the IT Procurement Checklist and relevant contracting language to aid in the development of detailed requirements, as well as assisting project teams with the review of IT Procurement packages prior to submission to contracting teams. The IT VMO must be immediately engaged for all IT Procurements once these projects are approved by their respective IT Business Capability Portfolios and prior to submission through the Spend Request approval process. Once contacted, the IT VMO will review and approve any required acquisition packages that have been developed. The IT Procurement Checklist should be referenced in the development of acquisition packages prior to submission to the IT VMO. Contact with the IT VMO is accomplished by emailing the requirement, any required documentation, and a responsible point of contact for follow-up to vmo@gsa.gov.

6. Responsibilities.

- GSA IT. GSA IT is responsible for the development of compliance standards in relationship to the Key IT Principles.

- GSA staff. Although the GSA IT VMO will assist in providing coordination support between GSA staff and the various IT Service and Business Portfolios, it is ultimately the responsibility of GSA staff to own this collaboration and ensure compliance with the Key IT Principles for both new projects and major enhancements to existing projects. GSA staff that currently have oversight over an existing IT Project are responsible for assessing their compliance with the Key IT Principles described above and proactively reaching out to the GSA IT Service Portfolios when initiating a major enhancement to ensure proper compliance.

7. Contacts. The Points of Contact (POCs) relative to this IL are identified in the table below.

#	Category	Organization	Name	Email
1	IT Procurement Checklist/Vendor Management Review	IT Vendor Management Office (VMO)	Lydia Dawson / Teresa Curtis	vmo@gsa.gov

#	Category	Organization	Name	Email
2	Single Sign On	Infrastructure	Brian Muolo	Brian.Muolo@gsa.gov
3	Cloud First	Enterprise Architecture	Kevin Wince	Kevin.Wince@gsa.gov
4	Enterprise Information and Data Management Open Source Software (OSS)	Enterprise Information and Data Management Office of the Chief Technology Officer (ID)	Kris Rowley	Kris.Rowley@gsa.gov
5	Digital Services	Office of Citizen Services and Innovative Technologies (OCSIT)	Martha Dorris	Martha.Dorris@gsa.gov
6	Document Management Records Management	Office of the Chief Technology Officer (CTO) Office of Administrative Services (OAS)	Vanessa Ros Deborah Lague	Vanessa.Ros@gsa.gov Deborah.Lague@gsa.gov
7	IT Security Engagement	IT Security	Kurt Garbars / Bo Berlas	Kurt.Garbars@gsa.gov Bo.Berlas@gsa.gov
8	Enterprise IT Governance	Enterprise IT Governance	Brian Isbrandt	Brian.Isbrandt@gsa.gov
9	General Information	IT PMO	Janine Gray	Janine.Gray@gsa.gov

8. References. Additional information related to the Key IT Principles may be accessed through the links listed below.

- Definition of an IT Project
- GSA IT VMO Chatter Site
- IT Procurement Checklist
- GSA Acquisition Manual (GSAM)
- Center for Excellence in Digital Government
- www.digitalgov.gov
- Digital Services Checklist of Requirements for Federal Websites and Digital Services
- GSA Information Technology (IT) Security Policy
- CIO GSA Wireless Local Area Network (LAN) Security
- Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing
- CIO Mandatory Use of Personal Identity Verification (PIV) Credentials
- ATO Extensions/Limited ATO
- GSA Web Domain Names
- GSA Information and Data Quality Handbook
- GSA IT Standards Profile
- Presidential Memorandum- Managing Government Records
- GSA Records Management Program and Policy
- IT Standards Process
- Best Practices for Developing OSS

9. Signature.

_____

SONNY HASHMI
Chief Information Officer
Office of the Chief Information Officer

July 24, 2014
Date