

M-16-NN

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director, Office of Management and Budget

Tony Scott
Federal Chief Information Officer

SUBJECT: Information Technology Modernization Initiative

Purpose

This memorandum provides guidance to agencies on planning for the modernization of at-risk information technology (IT) systems. It establishes a series of actions for agencies to implement to support the modernization of inefficient and insecure IT systems.

Background

Of the \$52 billion in Federal civilian IT spending planned for fiscal year (FY) 2017, approximately 71 percent (\$37 billion) is classified as “legacy” IT spending – that is, spending dedicated to maintaining the existing IT portfolio, excluding provisioned services such as cloud.¹ These systems may pose serious security risks, such as the inability to utilize current security best practices, including data encryption and multi-factor authentication. Further, unsupported commercial software may be impossible to update. Operational risks arise when these systems cannot adapt to current or expected mission requirements, user needs, operating environments, or are no longer cost justifiable. In these cases, modernization would improve the ability of these systems to deliver the necessary levels of functionality, security, and efficiency to satisfy the needs of agency users, stakeholders, and the American public.

Agency efforts to modernize existing IT systems have faced substantial challenges. The high costs and risks associated with modernization efforts, combined with the increasing cost to maintain existing systems, is harming agencies’ ability to manage their portfolio of IT systems strategically and deliver the functionality needed to achieve their missions. In addition, given the presence of significant interdependencies between agency IT systems, challenges in modernizing one system often have ripple effects across the agency’s IT portfolio, and in some instances, across the Federal Government.

¹ Source: Agency FY 2017 IT Portfolio budget submissions to the Federal IT Dashboard, <https://itdashboard.gov>.

Approach for Information Technology Modernization

The President's FY 2017 Budget² identified retiring or upgrading legacy IT systems as a key component to improving the cybersecurity and efficiency of the Federal Government. The President's Budget proposed increased resources for identifying and securing high-value information assets, and also proposes the creation of an IT Modernization Fund (ITMF) as a resource to retire, replace, and modernize the Federal Government's highest-risk IT legacy systems.

In order to improve the cybersecurity and efficiency of Federal IT systems, agencies must ensure priority planning for the modernization of high-risk IT systems and develop an updated Enterprise Roadmap, with a focus on modernization of the agency's IT portfolio.³ In accordance with OMB's authority to ensure effective information resource management⁴ and with the strategic goals described in agencies' Enterprise Roadmaps, this guidance will require the development of targeted modernization plans for specific high-risk, high-priority systems, as further discussed below.

Moving the Federal Government to modern infrastructure and cloud-based solutions is a fundamental necessity to building a digital government that is responsive to citizen needs and secure by design. Doing so will enhance agencies' ability to protect sensitive data, reduce costs, and deliver world-class services to the public.

Policy Requirements

Consistent with the Federal Information Technology Acquisition Reform Act (FITARA)⁵ and OMB Memorandum M-15-14, "Management and Oversight of Information Technology,"⁶ agency Chief Information Officers (CIO) shall leverage the improved authorities, visibility, and role in contracting and budget processes provided to them under FITARA to implement the requirements of this memorandum. Other senior agency officials, including the Agency Head, Chief Financial Officers, Chief Acquisition Officers, and Chief Human Capital Officers shall support the CIO in the execution of this initiative.

The IT Modernization Initiative will be implemented in four phases:

1. Development of updated Enterprise Roadmaps
2. Identification and prioritization of systems

² The President's Budget for Fiscal Year 2017, Office of Management and Budget, <https://www.whitehouse.gov/omb/budget>.

³ 44 U.S.C. § 3506(b)(2) requires agencies to "develop and maintain a strategic information resources management plan" in accordance with OMB guidance. Annual Enterprise Roadmaps are required by OMB Memorandum, *Increasing Shared Approaches to Information Technology Services*, May 2, 2012, https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/sharedapproachmemo_0502.pdf.

⁴ Clinger Cohen Act, 40 U.S.C. § 1101, et. seq.

⁵ Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Pub. L. No. 113-291.

⁶ OMB Memorandum M-15-14, *Management and Oversight of Federal Information Technology*, Office of Management and Budget, June 10, 2015, <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf>.

3. Development of modernization profiles for high-priority systems
4. Execution

GSA is currently collaborating with selected agencies to refine relevant criteria and templates, and will share best practices and other resources to aid agencies in carrying out this initiative. These materials will be maintained at management.cio.gov.

The requirements of this memorandum shall apply to all CFO Act agencies.⁷ Other agencies are encouraged to submit prioritized systems information and modernization profiles to OMB as best practices that improve the composition and execution of their IT portfolios.

Phase 1: Development of Updated Enterprise Roadmap

Agencies are currently required to develop and maintain updated Information Resource Management (IRM) Strategic Plans and Enterprise Roadmaps on a recurring basis.⁸ For FY 2016, OMB streamlined and restructured its Enterprise Roadmap guidance to ensure an appropriate focus on the modernization of agency IT portfolios, including better utilization of shared services and reduction in the proportion of agency IT budgets dedicated to non-provisioned operations and maintenance (O&M) spending.

As part of their annual Enterprise Roadmap submission that were due September 30, 2016, agencies were required to identify opportunities to transfer IT functions to shared services or cloud services and reduce legacy IT spending, as well as provide a sequencing plan for these activities. These updated Enterprise Roadmaps will serve to assist the agency with the identification and prioritization activities described in Phase 2.

Phase 2: Identification and Prioritization

Refinement of Criteria and Templates

By **MM DD, YYYY**, based on pilot work GSA performed with selected agencies, OMB will provide (with GSA's assistance) agencies a full list of criteria to be utilized by agencies in order to uniformly evaluate and prioritize information systems for modernization and a template for the submission of information to OMB on such identified systems. The criteria and template will support the prioritization of the systems based on security risks, operational risks, modernization impact, and execution ability and facilitate uniform comparison of agency information resource management.

A sample minimum list of criteria to be used by agencies to evaluate and prioritize systems for modernization can be found in Appendix A. A sample system information template, to be used by agencies to submit information on priority systems, can be found in Appendix B. Agency CIOs

⁷ Agencies listed in 31 U.S.C. § 901(b).

⁸ OMB Memorandum M-13-09, *Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management*, Office of Management and Budget, March 27, 2013, <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-09.pdf>.

should immediately begin to engage other senior agency officials, including program managers and business process owners, in the evaluation and prioritization of systems for modernization based on the information contained in Appendices A and B.

By MM DD, YYYY, OMB (again, with GSA's assistance) will publish a template to be used to develop and submit system modernization profiles, as required under Phase 3. A sample modernization profile template can be found in Appendix C.

Prioritization of IT Systems for Modernization

By MM DD, YYYY, all CFO Act agencies will be required to submit to OMB information on each of the agency's highest priority systems for modernization, using the criteria and system information template described above. Given the unique mission, environment, and long-term modernization goals of each agency, the agency CIO should determine the appropriate weight given to each criterion in evaluating the modernization priority of an individual system within the context of the agency's updated Enterprise Roadmap. Detailed information must be provided for a minimum of three systems, although agencies are encouraged to include information on additional systems as warranted. As part of this submission, agencies shall include at least one system for which full modernization or retirement, including completion of the replacement system, if applicable, could occur over a 6-12 month timeframe.

Agencies should leverage existing system inventories required under the Federal Information Security Modernization Act (FISMA), systems associated with High Value Assets (HVA) identified through the Cybersecurity Strategy and Implementation Plan (CSIP) or other high-value data sets listed in agency Enterprise Data Inventories, as well as automated hardware and software continuous monitoring or other asset inventory tools (e.g., Continuous Diagnostics and Mitigation), to assist in identifying and prioritizing systems.⁹ Agencies should also utilize, to the extent permitted by contract, any pre-existing systems inventories, such as stewardship reports, maintained by the agency's private sector vendors, to help identify agency systems and their current support status.¹⁰

To fulfill this requirement, the agency CIO is responsible for submitting a completed system information template for each of the agency's priority systems through an encrypted MAX Collect exercise. Upon receipt of this information, OMB, with the assistance of GSA, will conduct an initial review of each agency's System Information Templates and determine what, if any, additional information is needed from the agency.

Phase 3: Modernization Profiling

⁹ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Improving Federal Information Security and Privacy Management Requirements*, October 30, 2015, <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf>.

¹⁰ OMB outreach to private sector vendors indicates that many of the vendors maintain comprehensive inventories of all systems that have been provided to, or are currently maintained by, the vendor. These inventories may include information on whether the systems are currently supported.

By MM DD, YYYY, using the modernization profile template refined in Phase 2, all CFO Act agencies are required to submit to OMB a minimum of three modernization profiles (one each for an individual system for which a system information template was previously submitted); however, submission of additional modernization profiles is encouraged. In addition, agencies are permitted to submit joint modernization proposals, provided that a single agency be designed as the lead; joint proposals will count only toward the three-system minimum of the lead agency.

Modernization profiles should demonstrate and explain why the selected system should be prioritized for modernization, retirement, or replacement. Consistent with OMB's Cloud Computing Strategy, CIOs should consider the use of provisioned services, such as cloud, where possible, in developing agency modernization profiles.¹¹

To fulfill this requirement, the agency CIO will be responsible for submitting a completed modernization profile template for each of the agency's priority systems through a MAX Collect exercise. A sample modernization profile template can be found in Appendix C. Modernization profiles are not to exceed 10 pages each.

Phase 4: Execution

Agencies must plan for continuous modernization. To accomplish such plans, agencies must leverage their Enterprise Roadmaps and system-level modernization profiles to inform their annual budget submissions.

Contingent upon Congressional enactment of the ITMF, funding provided by the ITMF could be used to supplement and accelerate modernization efforts proposed in agency budget submissions and subsequently appropriated by Congress, and would not duplicate funding provided through agencies' existing budgets.

Agency Point of Contact

By MM DD, YYYY, the agency CIO shall designate an IT Modernization Initiative point of contact (POC) who will serve as the principal representative of the agency CIO for the execution of the IT Modernization Initiative described in this memorandum. This leader must have sufficient capacity to implement the initiative and must be provided with the authority and responsibility to assign tasks and work elements, as well as make business, product, and technical decisions to ensure the success of the overall initiative. The agency POC shall also identify one POC for each system for which a modernization profile is submitted to OMB. The system POC should have technical expertise and knowledge of the system.

¹¹ Federal Cloud Computing Strategy, February 8, 2011, https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf.

Cross-Agency Support

Executive branch employees are encouraged to join the IT Modernization Initiative listserv by emailing listserv@listserv.gsa.gov with no subject and “subscribe it modernization” in the body (from a .gov or .mil email address only.) The listserv will help support cross-agency communication, collaboration, and sharing of best practices and lessons learned. Questions regarding implementation of this memorandum may be referred to this listserv.

In addition, GSA will collaborate with agencies to refine relevant criteria and templates and share best practices and other resources at management.cio.gov.

Questions regarding this memorandum that cannot be asked on the listserv may be referred to Sean Casey, OMB Office of the Federal Chief Information Officer (OFCIO), at scasey@omb.eop.gov and the OFCIO inbox at ofcio@omb.eop.gov.

Appendix A – Minimum Criteria for Legacy IT System Prioritization

Minimum Criteria for Legacy IT System Prioritization	
Security Risks	<ul style="list-style-type: none"> • Security categorization: Moderate or high potential impact rating based on an agency's Federal Information Processing Standards Publication (FIPS) 199 security categorization assessment. • Sensitivity: Relationship of the system to the priority high value asset (HVA) list identified as part of the Cybersecurity Strategy and Implementation Plan (CSIP). • Past incidents: Incidents involving the system that have been reported to the United States Computer Emergency Readiness Team (US-CERT). • Compliance: Inability of the system to meet relevant guidelines issued by the National Institute of Standards and Technology (NIST) – examples include the inability, because of cost or technical incompatibility, to implement multi-factor authentication or storage encryption where recommended or required. • Support: Use of hardware, software, or firmware components no longer supported by developers, vendors, or manufacturers through the availability of software patches, firmware updates, replacement parts, and maintenance contracts. • Documented deficiencies: Security risks within the system documented in reports (including the FISMA report to Congress), by an agency's office of inspector general, the Government Accountability Office (GAO), or other organizations.
Operational Risks	<ul style="list-style-type: none"> • Mission criticality: Degree to which core mission functions of the agency or other agencies are dependent upon the system¹² • Impact: Relationship of the system to the OMB High Impact List • Cost: Rising costs associated with maintaining the system due to age or technical obsolescence • Human capital: Difficulty in maintaining necessary staff with skill sets relevant to the system • Documented deficiencies: Operational risks within the system documented in reports by an agency's office of inspector general, the GAO, or other organizations • Operational stability: Inability of the system to routinely achieve service-level requirements for uptime, availability, or response time • Technical friction: Operational or budgetary limitations on modifying the system due to technical complexity, complex dependencies, or obsolescence • Data integrity: Inability of the system to maintain valid, consistent, or projected data requirements

¹² As defined by NIST, SP 800-60, <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>.

	<ul style="list-style-type: none"> • System integration: Inability of the system to interface cleanly with other components in the agency's Enterprise Roadmap or IRM Strategic Plan
Modernization Impact	<ul style="list-style-type: none"> • Savings potential: Anticipated reductions in operations and maintenance (O&M) cost due to efficiencies gained by moving to modern architectures • Reuse potential: Anticipated agency-wide reuse of new technologies, including replacing multiple legacy systems with a single common platform • Business process simplification: Anticipated simplification, consolidation, or streamlining of underlying business processes, including complex, duplicative, or fragmented processes • Functionality improvement: Anticipated improvements to the quality of interactions and engagement with the public, businesses, other levels of government, and Federal employees
Execution Ability	<ul style="list-style-type: none"> • Program management maturity: Degree to which the agency has a sustained track record of successful delivery of IT systems and the means to ensure the proper methods are used to effectively plan and manage modernization initiatives • Governance maturity: Maturity level of agency governance framework to ensure proper continued oversight and adjustments to a modernization initiative • Modernization strategy maturity: Degree to which modernization of the system aligns with priorities described in the agency's Modernization Strategy and Sequencing Plan • Execution readiness: Degree to which personnel, hardware, and software infrastructure and processes are in place to carry out this modernization

Appendix B – Sample System Information Template

System Vitals

- Agency name
- System name
- Who will be the Point of Contact for this modernization?
- Please provide a short description of the system and its primary purpose.
- What is the Unique Investment Identifier (UII) associated with system, if any?
- What type of system is this (platform, application, database, web-based service, etc.)?
- For a software system or application, what are the primary base languages or programming platforms, and their current revision levels?
- On what date was the system placed in service?
- What is the date of last major system upgrade (hardware or software)?
- What vendors actively maintain or support the system?
- What is the name of the current operating system (OS)?
- What is the version level of the current operating system?
- Is the OS currently supported by the developer, vendor, or manufacturer through the availability of software patches?

Security Risks

- What is the impact rating based on an agency's Federal Information Processing Standards Publication (FIPS) 199 security categorization assessment?
- Is the system, or any data or service hosted on this system, identified on the priority high-value asset (HVA) list per the Cybersecurity Strategy and Implementation Plan (CSIP)?
- What incidents involving the system that have been reported to the United States Computer Emergency Readiness Team (US-CERT)?
- Are there known inabilities of the system to meet relevant guidelines issued by the National Institute of Standards and Technology (NIST)?
- Does any portion of the mission-critical functionality of this system require the use of unsupported and/or unpatchable hardware or software?
- Are there security deficiencies within the system documented in reports by the agency's office of inspector general, the Government Accountability Office (GAO), other organizations, or known to the agency IT staff or vendor?

Operational Risks

- What mission critical needs will not be met if this system is unavailable?
- What core mission functions of other components or other agencies depend upon this system?
- Are any aspects of the system or the services that it provides identified on the OMB High Value Asset list?

- What are the Operations and Maintenance (O&M) costs for:
 - Prior year (PY)
 - This year (CY)
 - Budget year (BY) (projected)
- What are the Development, Modernization, and Enhancement (DME) costs for:
 - PY
 - CY
 - BY (projected)
- What difficulties in recruiting and retaining necessary staff with skill sets relevant to the system have been identified?
- What operational risks within the system are documented in reports by the agency's office of inspector general, the GAO, or other organizations?
- Describe any known inability of system to routinely achieve service-level requirements for uptime, availability, or response time.
- Describe any operational or budgetary limitations on modifying the system due to technical complexity, complex dependencies, or obsolescence
- Describe any known issues in maintaining and managing current or projected data sets.

Modernization Impact

- What are the anticipated cost savings and impact on the agency, mission, and personnel that accrue from the collective efforts to modernize this system?
- Please describe the potential for agency-wide reuse of new technologies, including the ability to replace multiple legacy systems with a single common platform (or a more flexible set of services).
- List each user community (and the size of the community) that may significantly benefit from this modernization. For each of the user communities listed, what benefits have been identified?

Execution Ability

- What methods and personnel are in place to effectively plan and manage this modernization?
- Please describe your agency's or components' recent successes, especially using human centered design, lean, or agile methods to modernize or develop new IT systems.
- What is the maturity level of the agency's governance framework that will ensure proper continued oversight and adjustments to a modernization initiative?

Appendix C – Sample Modernization Profile Template

Planning Summary

- Of all the systems you have considered modernizing, why does modernizing this system provide the highest value?
- Please describe the goals of the modernization effort, including plans to utilize or deploy existing cloud services, shared services, or Application Programming Interfaces (APIs), as applicable.
- Please provide a short narrative description of the implications of maintaining the status-quo, including potential impact on the mission, personnel, and business processes of the system and on the agency.
- What is the schedule for the modernization? Please include intermediate milestones when new services become available, or older components are retired.
- What risks have been identified, including cost, schedule, scope, data complexity, software development, and project management risks, as well as a risk mitigation strategy?

Operational Risks

- What are the estimated post-modernization operations and maintenance costs for the first year of operations?
- Please provide anticipated cost savings and impact on the agency, mission, and personnel that the collective efforts to modernize will have.
- What are the projected yearly and total modernization costs? Please describe the methodology used to calculate estimated costs, such as cost benefit analysis.
- What are the costs associated with early contract termination in the event that the system is replaced or retired?
- If the modernized system presents new user interfaces or business processes to its existing user base, what retraining costs will be incurred?
- What types of data does this system store or process, beyond that identified in the HVA list?
- What is the aggregate size of data stored in the existing system? What growth is expected?
- What are the data retention requirements for data stored on the system being modernized?
- Is a data migration plan in place?
- What other systems will be affected by the modernization of this system? To what degree will the other systems be affected (e.g. upstream or downstream systems that will require replacement or modernization to support the modernization of this system)?
- Which other mission-critical systems can be more easily modernized following the modernization of this system?

- Will this modernization operate in a supported Cloud environment? If so, which environment?
- Will this modernization split out functionality consistent with a service-oriented enterprise architecture?
- If new services are split out, what other systems are candidates to share those services?

Modernization Impact

- What other systems can be retired as a result of this effort?
- What opportunities have been identified that will create strategic technological changes to the agency at large through reuse or re-application of techniques derived from modernization?
- What opportunities to re-engineer underlying business processes, including streamlining or consolidating complex, duplicative, or fragmented processes, have been identified?
- When you replace this system, what other upgrades (possibly non-mission critical) become feasible, or are simplified?
- How will Human Centered Design techniques be employed to ensure that the modernized system is more usable than its predecessor?
- What goals have been set for improving the usability of the systems?

Execution Ability

- What alternatives for system modernization have been explored?
- How does this modernization fit into the agency's Enterprise Roadmap?
- Will this modernization adopt lean/agile system development techniques?
- Who are the expert staff involved in the project (names and areas of expertise)?
- How many agency technologists will be required for this work?
- How many agency technologists are or will be available for this work?
- How many other staff members need to be hired or otherwise obtained?