



U.S. Department of State

Information Technology Strategic Plan
Fiscal Years 2019 – 2022

Table of Contents

Introduction	1
Department IT Vision and Mission	2
Goal 1: Data as a Strategic Asset	2
Objective 1.1: Data Architecture	2
Objective 1.2: Enterprise Identity Management System	2
Objective 1.3: Integrated, Secure, and Authoritative Repositories	3
Objective 1.4: Tailored Tools for Diplomacy	3
Goal 2: Enhanced User and Mission Effectiveness	4
Objective 2.1: Collaboration	4
Objective 2.2: Mobility	5
Objective 2.3: Streamlined Access, Catalog Services, and Rapid Delivery	5
Objective 2.4: Effective Security that Enables the Mission	5
Goal 3: IT Modernization	7
Objective 3.1: Interoperable Multi-Platform Cloud Ecosystem	8
Objective 3.2: Cybersecurity	9
Objective 3.3: Legacy Modernization	10
Goal 4: Strengthened IT Management	13
Objective 4.1: Streamlined IT Acquisition	13
Objective 4.2: IT Services Organization	14
Objective 4.3: Agile IT Governance	15
Goal 5: IT Workforce of the Future	17
Objective 5.1: IT Workforce Planning	18
Objective 5.2: IT Competencies	18
Objective 5.3: IT Workforce Recruitment and Retention	19
Acronyms	20

MESSAGE FROM THE CHIEF INFORMATION OFFICER

Perhaps nowhere in the federal agency arena has the impact of emerging technologies, business process re-engineering, and human capital requirements been felt greater than in the Information Technology (IT) community.

The extensive effect of digitization and the rapid evolution of IT capabilities creates many opportunities and challenges for how we deliver our global diplomatic mission. To capitalize on these opportunities requires that we improve and secure our data and make it, and our systems, more usable. We must re-engineer and modernize our systems and, to ensure that we use our IT resources well, we must institute more effective oversight.

These changes, while challenging, necessitate an ongoing assessment of our foreign and civil service IT workforce to ensure that we are recruiting, training, and retaining the IT talent of the future.

Within this framework, I am pleased to introduce our *IT Strategic Plan (ITSP) Fiscal Years (FY) 2019 – 2022*. Through this plan, we have identified goals and objectives the Department must address over the next four years.

Over the past year, the Department has developed many cross agency teams and forums to rethink and improve how IT is done. This plan strives to incorporate those ideas along with those provided through recent executive and legislative guidance regarding IT investment planning and management.

In particular, this ITSP directly aligns with the *Joint Strategic Plan (JSP) FY 2018 – 2022 Department of State and U.S. Agency for International Development*. More specifically, this plan further articulates how the Department will achieve Goal 4 in the JSP, “ensuring effectiveness and accountability to the American taxpayer,” by optimizing IT management and IT service delivery.

This plan lays out a bold vision for data management practices by leveraging cloud and shared solutions and improved IT acquisition and management processes. Our diplomats rely on modern, secure, and reliable technology for mission success, and the aggressive timelines we have set in this plan will ensure the Department meets our digital diplomacy requirements.

I am committed to the successful implementation of this ITSP. We will communicate our progress against goals on a quarterly basis and will engage in regular monitoring and reporting against our objectives.

As always, thank you for your service and your commitment to our mission. I look forward to working with you to make the vision in this plan a reality.



Karen Mummaw
Chief Information Officer, Acting

Introduction

As the global technology landscape evolves, our diplomats expect integration of the latest IT tools into their working lives. The influx of new technology must enable the conduct of diplomacy and must connect people to the information they need when they need it.

This strategic plan establishes five critical goals that align with the *President's Management Agenda* (PMA), are informed by the *President's IT Modernization Report*, and are influenced by the Department-wide IT modernization efforts that were conducted in FY 2017 and FY 2018.

The ITSP outlines how the Department will achieve Goal 4 of the JSP, and more specifically, how we will achieve Strategic Objectives 4.2 and 4.3 by modernizing and optimizing IT delivery across the Department. This plan serves as an authoritative document that will guide bureaus with mission-focused IT investments through FY 2022.

As the Department achieves the goals for data, user effectiveness, modernization, governance, and staffing as outlined in this plan, we will transform the way IT is done across the Department.

Over the next four years, the Department will strive to empower the workforce through a number of centrally-optimized shared services and through the expansion of cloud-based capabilities. These services and cloud capabilities will replace costly, in-house IT infrastructure and on-premises contracting services.

The plan calls for significant investment in IT modernization across the Department, requiring us to re-engineer many of our traditional practices to gain efficiencies and better leverage new and emerging technology capabilities. This will necessitate identifying and leveraging the right platforms to effectively deliver capacities at the right price. This, in turn, will require rethinking how we manage and oversee IT and how we improve the IT acquisition process, to include the types of vehicles available to the Department for enterprise-wide use.

Bureaus with IT investments are encouraged to integrate their investments into the management objectives of their functional and regional bureau strategies. All IT investments are required to be aligned to this ITSP, and coordinated with the Office of the Chief Information Officer (CIO) to ensure effective delivery and use of IT across the Department.

FY 2019 – 2022 ITSP Guiding Principles

Acquire services rather than build systems

Avoid vendor lock-in

Centralize and **standardize** in the cloud to maximize enterprise value

Re-engineer business processes as systems are modernized

Provide security that reflects real risk management and enables access

Rely on commercial and shared government services

Reduce internal data centers and legacy systems

Department IT Vision and Mission

Vision: Drive necessary and effective operations and collaboration across the Department, its partners, and foreign audiences.

Mission: Create an interconnected, secure, and informed Department through the prioritized, secure, and innovative application of IT resources.

Goal 1: Data as a Strategic Asset

Managing and leveraging data is integral to the Department’s mission and operation. We will invest in data over the coming years as a strategic asset. Our data, not the systems that store and process it, represents a true, long-term asset of value, and in most cases, our data will outlive the useful life of our technologies. This is especially true as the pace of technology innovation increases.

To leverage data as a strategic asset, we must first know what data we have. We must know that it is accurate for use in decision-making, and we must have appropriate access to it across the Department.

Under this goal, the Department will address the full lifecycle of data as it is transformed into information, intelligence, and knowledge for use by our diplomatic missions.

The modernization and re-engineering of systems and the transition of many of our systems to the cloud provides an opportune time to better manage our data and to appropriately share information in ways that improve its use across the Department at all levels. This will require advancing data management efforts, implementing and adhering to data standards, and increasing the accessibility to systems of record. These efforts, combined with the expansion and use of data analytic tools and related disciplines, will result in new insights and actionable intelligence. The Department will accomplish this by aggregating, layering, linking, and visualizing data and information in new ways.

The Department will also identify ways to leverage and integrate the power of familiar modern technologies, such as voice-to-computer interfaces similar to Siri, Alexa, or Google Assistant. We will also explore other emerging technologies, such as the use of artificial intelligence (AI), the expanded use of Global Positioning Systems (GPS) and digital mapping, and the use of foreign language translation services.

Objective 1.1: Data Architecture

The key to the success of Goal 1 is a data architecture that specifies how all of the Department’s data and information will be organized, stored, secured, integrated, and appropriately accessed from anywhere and with any device. The intent of the data architecture is to provide a rigorous structure that accommodates different types of internal and external data and information that the Department collects and generates. This effort requires a set of policies, standards, and methods for ensuring interoperability, appropriate security controls, data normalization, and tools that enable credentialed access, analysis, and use.

Objective 1.2: Enterprise Identity Management System

Over the course of this plan, the Department will employ an Enterprise Identity Management System (EIMS) that will enable users to access business data and services across the enterprise more efficiently. In addition to strengthening data security, the EIMS will enable credentialed single sign-on to enterprise systems and data, resulting in fewer passwords and streamlined

access. An enterprise EIMS also represents a more consistent way to secure data and control access across the enterprise and the cloud by integrating with all authoritative systems and users.

Objective 1.3: Integrated, Secure, and Authoritative Repositories

The Department will create authoritative and enterprise-wide data repositories that interoperate data across cloud and on-premises systems. This will include structured, semi-structured, and unstructured data of all types and media. These repositories will adhere to strict data management and architectural standards and will support enterprise-wide access to authorized and credentialed users. The migration of applications to the cloud and the integrated on-premises and cloud-based data repositories will enable the Department to shut down the majority of physical and on-premises data centers. We will drive data hosting decisions through the data categorization and classification process, which will define the controls required to protect the data at rest and in transfer. Cost continues to be a driver, requiring the Department to assess and deploy the most efficient platforms that meet the performance and security requirements of our customers.

The effort to integrate and secure authoritative repositories of data, information, and intelligence covers the full spectrum of data including Unclassified, Sensitive but Unclassified (SBU), Secret, and Top Secret classifications. For classified hosting, the Department will collaborate with the intelligence community's capabilities and expertise. Cloud services will provide global access, redundancy, disaster recovery, and security services that comply with federal regulations and the Department's standards and architectures.

Data repositories will comply with the National Archives and Records Administration (NARA) mandate to have all classified and unclassified records data in electronic form and searchable by December 31, 2019. For some datasets, this may require a two-phase migration: an initial phase to migrate data in its current form by the 2019 deadline, and a final phase as each legacy system is re-engineered following the systems modernization plan addressed in Objective 3.3.

Objective 1.4: Tailored Tools for Diplomacy

The CIO will convene a task force of subject matter and technology experts to develop a data strategy and a tactical plan that outlines specifications that bureaus can use as they modernize their systems and data repositories. We will standardize a suite of advanced information management tools for the Department's mission. The result will be an evolving and innovative suite of commercial and customized tools and applications to enable Department personnel to maximize the value of cloud-based data repositories.

We will keep current with technology and will ensure that all IT staff and end users are trained accordingly. Access to data will no longer be dependent on specific applications. Mash-ups of data through the use of advanced data analytic tools, as well as the layering of internal and external information, will be enabled. Users will have access to a suite of tools that access data needed from appropriate sources that result in tailored reports and presentations.

Table 1

Goal 1 – Data as a Strategic Asset	
<ul style="list-style-type: none"> • Build a framework for organizing the Department’s entire information collection on-premises and in the cloud via a global data strategy, inventory, and architecture 	<p>Outputs:</p> <ul style="list-style-type: none"> • Inventory all data repositories in the Department – Q3 FY 2019 • Implement an architecture for storing and accessing enterprise data in the cloud and practices to ensure data is current, accurate, and useful – Q1 FY 2020 • Curate data as systems are modernized and migrated to the cloud – FY 2020 - FY 2022 <p>Impacts:</p> <ul style="list-style-type: none"> • Universal access to enterprise data by all authorized users • Improved efficiency in mission-related tasks • Improved data security through universal tagging, encrypting, and access control and personnel safety through the elimination of critical data housed at posts abroad
<ul style="list-style-type: none"> • Universal inquiry and analysis capability 	<p>Outputs:</p> <ul style="list-style-type: none"> • Efficiently implement tools for advanced data analysis, pattern recognition, AI, and knowledge management – FY 2019 - FY 2022 <p>Impacts:</p> <ul style="list-style-type: none"> • Better informed for mission-oriented analysis and decision-making • Increased access to expertise throughout the Department and partner agencies and organizations
<ul style="list-style-type: none"> • Effective information production process 	<p>Outputs:</p> <ul style="list-style-type: none"> • Implement a process, templates, samples, and tools to create and distribute advanced and highly tailored information products – FY 2019 - FY 2022 <p>Impacts:</p> <ul style="list-style-type: none"> • Measurable improvement in the effectiveness of information as indicated by the level of understanding and support among target audiences • Compliance with NARA, Freedom of Information Act, Section 508 data regulations

Goal 2: Enhanced User and Mission Effectiveness

The influx of new technology makes it possible for employees to communicate, collaborate, and work more efficiently. The Department will aggressively move to leverage innovative and emerging services to provide Department employees ready access to the tools and information resources that are crucial to their work. Our workforce will be empowered through rapid deployment of innovative technologies and remote capabilities.

Objective 2.1: Collaboration

Collaborative tools enable tech-savvy users to change the way we do business. In moving to the cloud, we will offer modern services that are more in line with how people are accustomed to using technology in their everyday lives.

Collaboration is supported by network, platform, and security services that enable secure video, audio teleconferencing, documents, and data sharing. Reliance on appropriately secured commercial (where appropriate) and Federal Risk and Authorization Management Program (FedRAMP) cloud infrastructure (Goal 3) will enable the Department to make these products available to personnel wherever they are and whenever they need them. The Department will implement a security architecture that enables secure collaboration within and outside the Department, including digital collaboration with civilian and military agencies, non-governmental organizations, contractors, and other nations.

To further support collaboration, the Department will implement a modern, enterprise-wide, real-time cloud-based customer relationship management (CRM) system that leverages modern platforms, tools, and capabilities to enable data analysis, reduce duplication, and standardize and enhance contact event management around the globe.

Objective 2.2: Mobility

To further user and mission effectiveness, the Department will offer more capabilities through wireless connectivity and a range of mobile devices and applications. We expect the demand for mobile functionality to continue to grow, and the Department is committed to developing IT services that allow employees to communicate across Departmental and physical boundaries. Diplomats need untethered communication tools and access to information when they need it as they carry out modern diplomacy in an increasingly mobile world.

To this end, the Department will create and maintain a diverse mobile environment with reliable, secure, and straightforward connectivity inside and outside Department facilities for both government and personally-owned devices. Extending the functionality and capabilities of systems and applications to mobile platforms with integrated security will be the standard. As a result, our mobile workforce will be equipped with the knowledge and resources needed to carry out modern diplomacy.

Objective 2.3: Streamlined Access, Catalog Services, and Rapid Delivery

In surveying our workforce, it was clear that digital-savvy employees are seeking self-service IT and automation. They expect IT is kept updated and current by providers, allowing users to capitalize on innovations as they become available in the marketplace.

To improve services, we will implement a self-service catalog that allows users quick access to approved business products and applications that meet their specific needs. The Department will maximize the use of centralized shared services to lower costs. The increase in savings will be used to fund modernization investments, such as curating data as systems are modernized and migrated to the cloud, reengineering of systems in ways that create operational effectiveness, and greater seamless integration of security at all levels in ways that lower risk and enable innovation.

We will build upon the Department's successful cloud-based platform, which replaces legacy administrative systems. The Department will continue to seek government-wide best-of-breed IT services and technologies wherever possible and will deploy a catalog of services and capabilities, ensuring visibility and transparency into the cost associated with available shared services.

Objective 2.4: Effective Security that Enables the Mission

The Department will offer Enterprise Security Services (ESS) that apply to all environments where the Department's data is hosted, including the Enterprise Server Operations Centers, Cloud@State ecosystems, and Dedicated Internet Networks (DIN). This service will



MyServices platform provides the shared services platform for over 95,000 interagency users at 275 embassies and consulates worldwide to request \$3.4 billion in services annually. This state-of-the-art enterprise service management system leverages the latest in cloud-based technology to streamline processes and support administrative functions around the globe while providing a platform for increased user accessibility and service.

include applications, platforms, and infrastructure components. The Department will also establish a Cloud Access Security Broker (CASB) who will provide end-to-end security services and architecture allowing system owners to focus on their unique security controls needed at the application level. The ESS will include enterprise security management, continuous monitoring, and identity and access management (including single sign-on). In addition, it will include incident and vulnerability management for all systems with data in a production environment, regardless of data categorization. The security services that can be leveraged by using this approach will be driven by security requirements based on data categorization, impact levels, appropriate controls, and environment specifications.

Leveraging centralized security capabilities will streamline the security assessment process and reduce deployment time while strengthening the overall security posture of systems and services. ESS will allow a range of services and cloud capabilities to inherit a majority of security controls based on data categorization from the platform and infrastructure as authorized by security profile. In all instances, security efforts will be based on risk management and focus on how best to achieve a mission requirement securely.

To carry out this objective, we will pursue the following initiatives:

- Reduce the cost and resources required to process independent application level Authorization to Operate (ATO) by leveraging an enterprise ATO for each platform and infrastructure per cloud service providers
- Identify ESS and develop Information Security Program Plans based on functional areas
- Implement a data-informed security management approach that protects enterprise data independently of applications, thus enabling broad and secure access
- Assess current security risk policy for alignment with acceptable security risk thresholds
- Devise cloud security requirements to determine the security services and level of protection required for client data and information in the cloud
- Establish and monitor security performance objectives and metrics

Table 2

Goal 2 – Enhance User and Mission Effectiveness
<ul style="list-style-type: none"> • Increase employee satisfaction, productivity, and usability by improving technical capabilities and access Outputs: <ul style="list-style-type: none"> • Raise the level of satisfaction with IT service delivery by 25% – FY 2019 - FY 2022 Impacts: <ul style="list-style-type: none"> • Increased user productivity and value from IT investments • Implement Single Sign-On Outputs: <ul style="list-style-type: none"> • Pilot advanced identity management to enable a single credential across multiple applications – Q1 FY 2019 • Expand legacy system integration with IDMS – Q3 FY 2019 Impacts: <ul style="list-style-type: none"> • Increased user productivity and heightened cybersecurity • Internal and external collaboration Outputs: <ul style="list-style-type: none"> • Implement a cloud security architecture and a collaboration suite to allow unclassified and classified internal and external collaboration – Q1 FY 2020 • Implement Contacts and Events Management application globally – Q4 FY 2020

Goal 2 – Enhance User and Mission Effectiveness (Continued)
<p>Impacts:</p> <ul style="list-style-type: none">• Expanded Chief of Mission and diplomatic communication capabilities• Enhanced partnering with external entities• Enhanced personnel safety <ul style="list-style-type: none">• Establish a set of Centralized Shared Services Department-wide <p>Outputs:</p> <ul style="list-style-type: none">• Establish a development and operations (DevOps) cloud delivery service for new cloud solutions available to the Department – Q3 FY 2019• Establish a business/requirement service available to the Department – Q4 FY 2019• Publish a Department-wide services catalog with quarterly updates – FY 2019 - FY 2022 <p>Impacts:</p> <ul style="list-style-type: none">• Improved productivity through the increased utility of applications and tools

Goal 3: IT Modernization

The IT Modernization goal outlines the Department’s migration to the cloud, cybersecurity efforts, and legacy IT systems modernization that will transform IT. The Department will work rapidly to achieve the President’s IT modernization vision and to comply with new and existing federal mandates.

Cloud computing is the Department’s target operating environment, whereby we will implement an interoperable, scalable, multi-platform cloud ecosystem that supports collaboration, mobility, and agility as articulated in the *FY 2018 – 2022 Department Cloud Strategy (DCS)*. Aggressive steps toward moving legacy systems to the cloud will reduce reliance on owning and operating a costly IT infrastructure. This will require updating business processes, enterprise standards, and architectures in ways that equip the Department with innovative, user-friendly, and easily accessible data, services, and technologies.

There are risks in transitioning the Department to a cloud-based service provider environment, particularly as uniform cloud interoperability standards are still in early development. There also remains a significant gap between cloud services and the risk associated with cloud computing. The most significant of these include vendor lock-in, cost of data extraction, securing data at rest and in-transit, and elastic usage that may not align with annual funding levels and structures.

The Department will address these risks through a robust risk management framework within a Security Assessment Report on a per cloud-service basis. The Department will provide a centralized and optimized Cloud@State ecosystem by implementing an authoritative cloud technical architecture and platform roadmaps to ensure that solutions and capabilities built on our multi-platform cloud environment maintain a level of standardization and uniformity. We will also develop a set of policies that will be optimized and managed centrally.

Centralized, integrated, and optimized Platforms as a Service (PaaS) and Infrastructures as a Service (IaaS) with well-defined standards will be shared across the Department. This will enable bureaus to focus their resources on developing mission-centric, end-user software capabilities rather than duplicating infrastructure and platform investments and will ensure that related systems and services are secure and interoperable across organizations. To achieve targeted efficiencies, our modernization efforts will require business processes within and between organizations to be re-engineered to eliminate duplication, improve security, drive cost down, and provide operational efficiency.

This will be accomplished, in part, by leveraging out-of-the-box capability to the greatest extent possible. A critical element of the Department's shared services model is the Department's Working Capital Fund (WCF). The Department intends to leverage and expand the use of its WCF as products and services are matured and costs are adequately controlled.

The WCF allows the Department to offer fee-based shared IT services in line with the intent of the *Modernizing Government Technology Act* (MGT Act). Fee structures will be based on unitized cost models developed by and approved by IRM, the Bureau of Budget and Planning (BP), and the Bureau of Administration in partnership with the user community across the Department.

Objective 3.1: Interoperable Multi-Platform Cloud Ecosystem

Over the course of this ITSP, the Department will transition from a legacy brick and mortar ecosystem to an ecosystem that leverages a secure cloud architecture. The migration to this environment will follow a set of technical, security, and data standards. Improvements to the Department's Enterprise Architecture (EA) will encompass the integration of Business, Technical, Security, and Data Architectures. The technical architecture will contain sub-architectural artifacts including a cloud architecture and associated platform roadmaps. This architecture aligns with the goals outlined in the DCS, the *President's IT Modernization Report*, the MGT Act, and the Administration's *Cloud Smart* policy.

To facilitate a smooth transition to the cloud, the Department plans to employ an enterprise shared services model for delivering cloud services that will be structured, agile, and cost-effective. This will enable the broad sharing of technology, information, subject matter expertise, and resources while securely maintaining reliability as a result of strictly enforced service level agreements.

This will also require investments in a common cloud infrastructure and technologies that support the capability to provision and deploy IT resources and service elastically. The desired outcome will be accelerated cloud adoption through enterprise security and cloud brokerage services – resulting in cost savings, increased agility, enhanced security, improved productivity, and greater access to mission and administrative data. The Department's transition to an optimized enterprise cloud ecosystem is consistent with all existing laws and regulations.

IRM has established a Cloud Program Office to build and manage the consolidated cloud ecosystem and will leverage approved platforms to provide service delivery to Department customers. The office will leverage a multi-cloud approach with scalable solutions, robust security, and change management policies, in addition to a cost recovery model. The solutions and policies will evolve incrementally as business lines mature.

There are two principal challenges to moving to the open cloud architecture. First, the transition of legacy applications to the cloud, especially high value assets (HVA), will be time-consuming and costly. Some of these legacy systems may require a hybrid-cloud that will support components and/or services on a private Department cloud, while other forward facing components may leverage the open commercial cloud architecture. Second, the business process transformation of existing applications and services transitioning to the cloud will be hampered by the lack of documentation and resources that undergird those processes. Ultimately, by implementing business process transformation, applications will be streamlined so that they can effectively use the cloud; thus, the overall performance and operation is more optimal.

To expedite implementation, the Department’s cloud ecosystem will use enterprise licenses and products that are FedRAMP-approved or have earned other agency ATOs. Figure 1 shows the interoperable cloud ecosystem, which simplifies our IT architecture and leverages commercial services and expertise to maximize performance, mission capabilities, and security. We expect to engage multiple cloud providers to encourage competition and continuous performance improvement and to avoid vendor lock-in as mandated by the MGT Act.

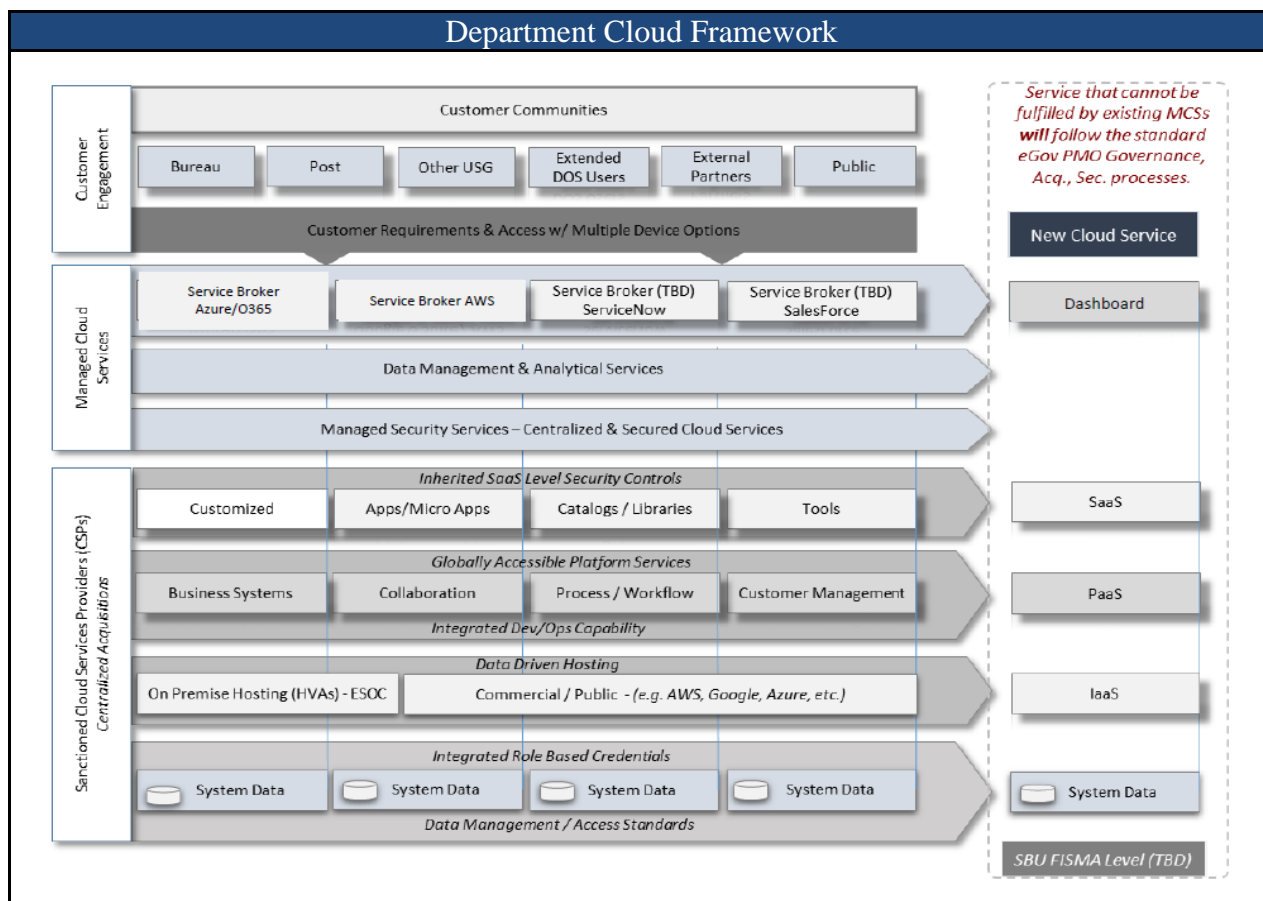


Figure 1

The cloud ecosystem will enable the Department to transition from buying and maintaining IT hardware and software and transition to acquiring services instead. Commercial cloud vendors will be the primary choice for cloud services and operations for the Department’s unclassified environment. For classified processing, we will leverage the cloud capabilities of other agencies in the defense or intelligence community, merging security architectures to accommodate the Department’s identity management system.

Objective 3.2: Cybersecurity

Cybersecurity is an enduring priority and a key consideration in every Department IT decision. The Department’s Cybersecurity Strategy Framework approach evaluates and addresses risk, vulnerabilities, and mitigation options. This is informed by strategic, operational, mission, and budgetary considerations and developed in close coordination with the Bureau of Diplomatic Security (DS). This approach is based on the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*. As the various

legislative and federal mandates evolve and change, the Department will continue to review and revise its Cybersecurity Strategy Framework.

Migrating to the cloud through a centrally-managed, optimized, shared services delivery model will enhance the Department's IT security posture, while also increasing efficiency and accessibility. As noted in the *President's IT Modernization Report*, it is becoming increasingly difficult for any single agency to stay current with security demands and to protect against threats.

In addition to the joint digital security services provided by DS and IRM, this plan calls for a broader government-wide partnership that utilizes specific security services provided by the Department of Homeland Security (DHS), the intelligence community, and commercial cloud providers. We will capitalize on the best cybersecurity expertise available, and ensure that our IT infrastructure and the security of our data in the cloud is kept current in response to constantly evolving threats.

To strengthen the Department's cybersecurity posture, we will expand on the capabilities of the Cybersecurity Integrity Center (CIC), and we will fully integrate these capabilities with the Joint Security Operations Center (JSOC) to create a joint digital security service delivered by IRM and DS in partnership with DS Foreign Affairs Cybersecurity Center (FACC). We will also expand our cyber risk management program, fully integrating it into the Department's enterprise risk program. In addition, the Department will deploy a Continuous Diagnostics and Mitigation program.

These programs will close gaps identified by the annual Federal Information Security Modernization Act (FISMA) audits and will put in place the controls necessary to ensure that all IT systems across the Department adequately integrate security into their systems. Those systems that fail to address weaknesses in a timely manner will be identified as an "at risk investment" by the E-Gov Program Management Office review process. The Department will make a concerted effort, as a part of this objective, to change the culture of the Department with regard to cybersecurity by raising awareness about cybersecurity and the importance of individual cybersecurity practices at all levels of the organization both when working on-site or remotely.

Objective 3.3: Legacy Modernization

Currently, more than three-quarters of the Department's IT resources are dedicated to supporting the operations and maintenance (O&M) of existing systems, many of which depend on outdated legacy technologies. As Figure 2 illustrates, the Department's O&M costs have quadrupled over the past 20 years, while the funds invested in new development, modernization, and enhancements (DME) have been nearly flat. This trend must be reversed; it represents an inefficient use of IT resources that do not result in increased value to the mission nor the American taxpayer.

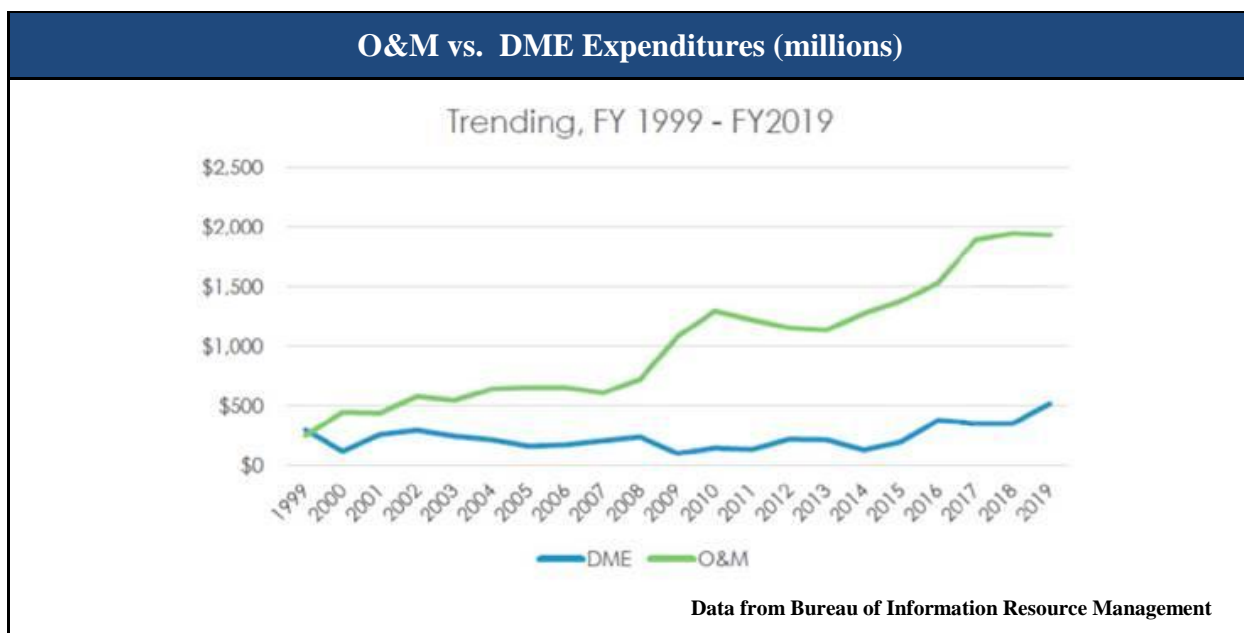


Figure 2

Modernization of legacy IT will increase operational efficiency and security, minimize the need for on-premises data centers, and simplify our IT and security architectures. Legacy system modernization addresses data that needs to be integrated, interoperable, normalized, and structured for use in decision-making using modern data analytics tools. Legacy modernization directly aligns with the PMA, the *President’s IT Modernization Report*, and will support the achievement of the ITSP’s data resource management and strategic data initiatives.

The FY 2019 – 2022 ITSP supports increased operational planning by system owners, with the potential for each major system owner to develop a legacy systems modernization plan and an associated timeline for its modernization. The Department will identify one of the major systems to be modernized and migrated to the cloud on a pilot basis by the end of FY 2019. For the remaining major systems, the E-Gov Program Board (E-Gov PB) will approve a plan for modernizing and migrating each system to the cloud ecosystem by the end of FY 2019. The plan should address legacy modernization, linking to the strategic data goal so that cloud-based data will be fully accessible beyond the individual application in which it was created.

The scope of the Department’s legacy modernization includes updating the software lifecycle processes we use to plan for and provision IT by instituting a standard, agile, and modern approach. This effort will empower the Department to refocus talent and resources on technology that supports and improves mission delivery rather than the costly legacy IT. The shift to a service-based delivery represents a significant departure from today’s model. The changes to technology, business processes, and enterprise standards will prevent the Department from falling into a similar legacy IT cycle in the future.

Modernization of legacy IT will be a collaborative process and involve functional and regional bureaus and posts. The process to identify, evaluate, and prioritize legacy modernization will require a number of considerations. These considerations include technology defined by DHS as an HVA, FISMA-related risk (high, moderate, or low), availability of alternative products, total lifecycle cost, and interoperability.

Consolidation and optimization of networks, duplicative systems, and platforms (including applications) will be coordinated in conjunction with the implementation of the Federal Information Technology Acquisition Reform Act (FITARA) and Data Center Optimization Initiative (DCOI). This process will reveal shared service opportunities, transition the Department to an incremental development standard, and provide the necessary analyses to find products that maximize the return on investment for the Department and American taxpayers.

The Department will allocate all available resources to legacy systems modernization. As appropriate, this may include the use of the newly created Technology Modernization Fund established by the MGT Act. However, our objective remains to consolidate and optimize systems with similar capabilities, to replace systems whose cost are unsustainable, and to modernize those systems whose security posture continue to put the Department’s data and mission at risk. In addition, the Department will explore appropriate ways to redirect savings from the consolidation, optimization, and reduction of legacy IT. These activities will involve working closely with the Office of Management and Budget (OMB) and federal partners to identify best practices across the federal sector IT community.

Table 3

Goal 3 – IT Modernization
<ul style="list-style-type: none"> • Implement a central secure, modern, global, interoperable, and optimized cloud ecosystem that supports multiple platforms Outputs: <ul style="list-style-type: none"> • Establish a process for selecting and approving new cloud service providers – Q3 FY 2019 • Develop a cloud architecture that will serve as a roadmap for migrating legacy systems to the cloud – Q4 FY 2019 • Establish enterprise license agreements for approved cloud service providers – FY 2019 - FY 2022 • Centralize and optimize cloud services in accordance with the Department’s Cloud Strategy – FY 2019 - FY 2022 • Begin consolidating duplicative production cloud environments – FY 2019 - FY 2022 Impacts: <ul style="list-style-type: none"> • Enhanced reliability, security, collaboration, and mission support • Implement a data-driven risk management security approach that protects enterprise data independently of applications, enabling broad and secure access Outputs: <ul style="list-style-type: none"> • Expand the capabilities of our continuous monitoring, diagnostics, and mitigation program – Q1 FY 2019 • Develop comprehensive security strategy and architecture – Q2 FY 2019 • Establish an Enterprise Security Service (ESS) Program with a particular focus on Cloud security services – Q4 FY 2019 • Implement a comprehensive enterprise IT risk management program – Q1 FY 2020 • Expand the Department’s IT security focus to include greater emphasis on data layer protection – FY 2019 - FY 2020 Impacts: <ul style="list-style-type: none"> • Enhanced mission support through improved access to data anywhere; reduced vulnerability to hacking and other threats • Modernize legacy IT and underlying business processes Outputs: <ul style="list-style-type: none"> • Develop criteria for identifying legacy system practices that require system modernization – Q2 FY 2019 • Develop an IT modernization plan and timeline – Q4 FY 2019 • Migrate one of the large management systems to the cloud – Q4 FY 2019

Goal 3 – IT Modernization (Continued)

Impacts:

- Improved cost-effectiveness for IT
- Enhanced management efficiency and effectiveness due to improved system access, cross-system integration, and improved disaster recovery

- **Ongoing innovation and modernization**

Outputs:

- Establish a process for ongoing user input and rapid response – Q2 FY 2019
- Implement a DevOps approach through a centralized shared services to provide rapid deployment to the cloud – Q3 FY 2019
- Streamline and strategically align all governing boards under the CIO and E-Gov governing process – FY 2019 - FY 2021
- Reduce average deployment time for new IT capabilities by 10% annually – FY 2019 - FY 2021

Impacts:

- Enhanced tools for diplomacy
- Timeliness in implementing tools when they are current – increased security and functionality; more supportable

Goal 4: Strengthened IT Management

This goal focuses on the best practices in IT leadership, governance, personnel, and organization needed to transform the way IT is managed and delivered at the Department in support of our diplomatic and development mission. New legislation, directives, and plans have created a bold challenge for federal agencies to rapidly modernize and secure IT assets and programs while improving service delivery. Meeting these challenges will require the Department to embrace shared services across bureaus and to draw on expertise and solutions from across the federal government.

To aid in this effort, we will restructure and streamline our existing governance processes to enable more cost-effective, agile IT operation and decision-making. The Department will aggressively seek opportunities to expand the use of centralized shared services and solutions across the Department and from other agencies and the private sector, rather than developing new custom or duplicative solutions.

Objective 4.1: Streamlined IT Acquisition

IT acquisition represents a critical service influencing the way IT is delivered to customers across the Department. It also functions as one of the most significant cost and risk drivers of IT service delivery. The desired outcome of the IT acquisitions modernization objective is to:

- Create efficiency in the acquisition process resulting in lowering IT acquisitions cost;
- Remove unnecessary friction in the acquisition process resulting in improved time to market;
- Eliminate redundant contracts improving IT acquisitions transparency; and
- Implement IT contract standards resulting in meeting business and regulatory requirements for modern IT systems.

Achieving these outcomes will result in data driven decision-making, more efficient delivery of IT solutions, increased transparency in IT spending, and fulfillment of the overarching goals in the FITARA legislation. The Department is committed to managing IT more effectively, which requires accurate reporting of IT investments and acquisitions and consistently measuring IT investment performance.

A key part of this effort will be to strengthen and expand IT acquisition services with the understanding that this service is critical to the efficient and effective delivery of IT across the Department. Another important element of these efforts is to refine, provide transparency, and automate the IT acquisitions review process. This will include introducing “acquisitions review” earlier into the acquisition process. The optimized IT acquisition review process is intended to:

- Enable greater economies of scale and purchasing power by increasing the use of Enterprise License Agreements (ELAs) and Blanket Purchase Agreements (BPAs) across the Department;
- Eliminate acquisition duplication for hardware, software and services by expanding the ELA program to include EA for hardware and services; and
- Enhance service delivery by simplifying time and effort required for Department personnel to acquire IT services.

The Department will establish standard and flexible acquisition vehicles, largely relying on Government-wide Acquisition Contracts (GWAC) to support the entire enterprise. These vehicles offer easy and rapid ordering and delivery of standard services and products, to include self-service ordering as well as streamlined procurement of custom solutions as needed. Over the course of this plan, the Department will consolidate its disparate licensing models to gain savings in recurring operational costs. GWACs, Department-wide ELAs, BPAs, and indefinite delivery/indefinite quantity contracts will become the standard.

As a part of this effort, the Department will implement the Technology Business Management (TBM) framework to increase transparency, accountability, accuracy, and oversight of the agency’s IT spending. It will also develop an IT acquisitions cadre through recruiting and training to ensure that the Department is adequately equipped to execute inherently governmental functions. The Department will implement all aspects of the FITARA legislation, and the initiatives outlined in this objective will help the Department achieve its IT management and acquisition goals.

Objective 4.2: IT Services Organization

Successful IT organizations of the future must adapt to tomorrow's mobile-centric and cloud-enabled environment to deliver a high-quality user experience. To this end, the Department will establish a centralized IT service delivery model equipped to leverage the appropriate cloud platform that delivers automated capabilities in the most cost effective, secure, and agile way.

With the move to an optimized and shared cloud ecosystem, the IT services delivery organization will facilitate the use of a DevOps methodology designed to leverage approved cloud environments. Department personnel and on-site contractors will have less day-to-day responsibility for managing the infrastructure and will shift to delivering more IT services support.

The Department will also significantly reduce its domestic data center infrastructure and the system data required to be on-premises overseas. This will drive a shift in our IT workforce’s role from “build and maintain” to services that enable personnel to access and utilize the multiple platform cloud services. IT products that operate within the approved Cloud@State ecosystem and align with the enterprise architecture will not need to be reviewed or approved by control boards, thus simplifying the governance process.

Service catalogs with pre-approved technologies will permit employees to leverage existing services through appropriate contract vehicles. A centralized business process re-engineering and requirement service will be established to help bureaus define their business requirements and best leverage the Department's cloud investment and platforms. Bureaus with demonstrated experience will be able to leverage and configure centralized cloud services directly through the DevOps methodology.

Objective 4.3: Agile IT Governance

Improvements and innovations in IT are being introduced at an ever-increasing pace. To leverage the latest innovations, organizations must act swiftly and smartly. Although FITARA provides the CIO with extensive authority, oversight, and control over IT operations, moving to an agile delivery framework will require an IT management framework in which decision-making to ensure agile performance and operations will need to take place at the least common denominator level – e.g., portfolio, area product, and program manager level.

Traditional governance models based on complex structures of processes, documentation, and governance boards are not compatible with the modern IT environment. Agile governance is a 21st century methodology for ensuring effective enterprise oversight of IT projects, portfolios, and investments. It parallels agile software development methodologies and is well-suited to the current IT environment, which is based heavily on shared and acquired services rather than the development of complex and risky one-off solutions.

Capitalizing on shared services will enable the Department to eliminate many of today's control boards and oversight processes. Instead, the Department will rely on prior approvals that apply to all implementers and users. Under this objective, the Department will implement agile governance based on the following fundamental tenets:

- **Fast pace of change** – Impeding change is not viable in today's environment in which new technologies and innovations are introduced at a record pace. Accordingly, the Department will make change easy and will encourage managers to take risks and to move rapidly to acquire and implement new solutions.
- **Accountability and transparency** – Managers will have the authority to implement solutions rapidly with minimal advance approval, as long as their efforts are consistent with the ITSP, Cloud@State ecosystems, security protocols, architectural roadmaps, and budget authority. Dashboards will ensure visibility and insight into progress and results, enabling the CIO and E-Gov PB to oversee projects effectively with minimal documentation.
- **Commitment to enterprise strategic, architectural, resource, and acquisition plans** – The ITSP will be updated at least annually through an agile update process and through tactical plans for major projects such as legacy systems modernization that have received approval from the E-Gov PB. Dashboards will indicate progress against plans. Project and portfolio managers will be expected to present the key objectives they intend to satisfy and to indicate how the accomplishment of these objectives will be manifested and measured.
- **Incremental acquisition and implementation** – IT projects will be managed using agile and DevOps methodologies with incremental and phased implementations to include high levels of visibility. This will reduce risk, encourage innovation, and allow for ongoing transparency and oversight.
- **Independent oversight and audit** – Projects will be audited by the E-Gov PB on a periodic basis to ensure they are proceeding as expected and reported.

The sum total of the above will eliminate the need for much of the documentation produced for IT projects today. Rather than spending time and resources developing detailed requirements specifications, alternatives analyses, and similar documents, project managers will develop rapid statements of objectives and select from available shared and commercial cloud and consulting services. Within each portfolio, there will be a portfolio owner, a program manager, and an area product owner, each with specific responsibilities defined. Each manager, or collection of managers, must understand their role in the agile process, as well as what can be expected from an agile project or portfolio as it progresses.

Table 4

Goal 4 – Strengthening IT Management	
<ul style="list-style-type: none"> • Streamlined Acquisitions 	<p>Outputs:</p> <ul style="list-style-type: none"> • Develop a comprehensive IT Acquisition Reform Strategy – Q1 FY 2019 • Develop a recruiting and training plan to build up and retain an IT acquisition cadre – Q2 FY 2019 • Increase the use of ELAs and BPAs by 20% annually and expand the ELA program to include hardware and services – FY 2019 - FY 2021 • Develop and execute a plan to optimize and automate the IT acquisition review process – FY 2019 - FY 2021 • Consolidate and standardize IT acquisition vehicles by 10% annually – FY 2019 - FY 2022 <p>Impacts:</p> <ul style="list-style-type: none"> • Increased efficiency in the acquisition process resulting in lowering IT acquisitions cost • Less friction in the acquisition process resulting in improved time to market • Fewer redundant contracts and improved IT acquisitions transparency • Compliance with IT contract standards and business and regulatory requirements for modern IT systems • Improved FITARA scorecard
<ul style="list-style-type: none"> • IT Service Delivery 	<p>Outputs:</p> <ul style="list-style-type: none"> • Develop and execute a tactical plan to implement an enterprise-wide IT Service Delivery Service – Q3 FY 2019 • Implement a Business Process Re-Engineering and Requirements Service – Q4 FY 2019 • Develop and execute all tenets of the Department’s Cloud Strategy – Q1 FY 2020 • Decrease the number of cloud production environments by 20% annually – FY 2019 - FY 2021 <p>Impacts:</p> <ul style="list-style-type: none"> • Delivery of automated capabilities in the most cost effective, secure, and agile way • Fewer cloud environments to secure and maintain • Reduction in the average time for customer approval requests for new technology implementation • Improved FITARA scorecard
<ul style="list-style-type: none"> • Create agile governance processes and architecture that effectively support the Department’s mission 	<p>Outputs:</p> <ul style="list-style-type: none"> • Establish authoritative Enterprise Architecture that includes business, technical, data and security Sub-EA artifacts – Q3 FY 2019 • Optimize existing governing boards under the E-Gov Program and Advisory Board Governance Program – FY 2019 - FY 2021 • Deploy TBM in accordance with OMB guidelines – FY 2019 - FY 2021 • IRM ensures distribution of the Department’s ITSP to all stakeholders and will provide necessary instruction and training related to the ITSP objectives and associated legal requirements • IRM will coordinate with BP and other Department stakeholders to ensure the Department’s IT strategic goals are addressed in future iterations of the JSP.

Goal 4 – Strengthening IT Management (Continued)

- **Increased coordination between the CIO and Chief Financial Officer of the roles and responsibilities in budget formulation and budget execution**
Impacts:
 - Improved FITARA scorecard
 - Accomplishment of JSP Performance Goal 4.2.3

Goal 5: IT Workforce of the Future

A key driver of the FY 2018 – 2022 JSP is to enhance workforce performance, leadership, engagement, and accountability to execute the Department’s mission efficiently and effectively. The ITSP parallels this focus.

Rapid technology advances and changing business requirements make it essential to recruit and retain the best talent and to empower a diverse, user-focused IT workforce with advanced skills in the latest technologies. The Department’s future IT workforce must include experienced IT analysts who can consult and advise customer bureaus in addition to assisting in the identification of the best IT solutions for their needs. This requires that the Department close critical competency gaps – particularly in the areas of cloud solutions, cloud security, IT project and program management, IT acquisitions, and risk management.

To accomplish this, we will define in detail the skill and experience requirements of the domestic and overseas IT workforce required to support this Plan and the Cloud@State ecosystem that will drive IT service delivery and consumption over the next five years and beyond. Next, the Department will develop a recruiting and training plan to ensure we hire and retain personnel with the right knowledge, skills, and abilities (KSA). The Department will also assess and restructure, as appropriate, the type of on-premises expertise needed as we shift from a “build and maintain” to a “service delivery and consumption” methodology.

Much of the current contractor workforce maintains the Department’s in-house data centers and network infrastructure. We anticipate that much of this workload will be reduced and replaced with other skill sets as we move to the cloud. We also expect inherently governmental functions to increase, requiring increases in our federal workforce with new skills to function well in these positions. To carry out this goal, we will pursue the following initiatives:

- Detailed workforce planning to identify and address needs through recruiting and training
- In-depth training on the Department’s mission needs and the technologies that will help users satisfy those needs
- Expansion of the Skills Incentive Pay (SIP) program
- Rotational assignments in other federal agencies
- Fellowship programs
- Self-paced and self-selected career development options

As digital transformation moves from wired workstations to mobile and cloud-based technologies, the Department faces increasing expectations for faster and more reliable collegial interactions. Our IT workforce will meet these challenges by embracing agile methodologies, expanded consulting services, business requirements-driven solutions, and a customer-focus service approach – all to enhance the IT user experience. IT will remain a fast-paced and ever-evolving field. To encourage innovation and agility, the Department is increasing the use of mobile environments, migrating enterprise-wide technologies to the cloud, and emphasizing the human element of managing IT. The Department envisions an adaptive IT organization, driven

by a modern and empowered workforce who are equipped with the skills and knowledge to carry out the user's mission-first needs.

Objective 5.1: IT Workforce Planning

The Department's IT workforce will be a key element in the success of this ITSP. Government, contractor, and Locally Employed staff (LE staff) must have the skills, capabilities, and aptitudes to embrace the new agile, cloud-based environment and to assist bureaus and project managers in making and implementing wise decisions. Under this objective, the Department will put in place an enterprise-wide IT workforce planning process and develop an initial plan.

The Department will use human resource and contract data to develop the workforce plan. We will also use authoritative data to inform the recruiting, assignment, deployment, and career development of IT professionals to support diplomatic, consular, and managerial assets around the world. The Department will assess the maturity and effectiveness of existing data management systems to identify and close gaps. These data processes will assess the availability of skills, as well as determine workload demand and the appropriate mix of Foreign Service (FS); Civil Service (CS); LE staff; interns and fellows; Eligible Family Members (EFM); and contractors.

We will also use human resource data to support the measurability of the Department's IT workforce strategy. In addition, we will institute dashboards to report and visualize the workforce gaps needed to support the IT environment of the future. Analytics will facilitate decisions regarding reduction or eliminating staffing gaps that impact performance, recruiting individuals with mission-critical skills, and deploying valuable human resources more effectively. With strong foundational elements, the Department will effectively use data to enhance the forecasting of retirement, separation, and attrition rates to improve succession planning.

Objective 5.2: IT Competencies

To empower the IT workforce fully, the Department will pursue initiatives that engage and develop individuals throughout the career lifecycle. Numerous pathways exist for such development, including fellowship programs, streamlined career paths, rotational assignments, expanded access to learning approaches, and incentivized skill enhancement.

As IT migrates to the cloud, cloud service providers from commercial vendors and other agencies will replace a substantial amount of the current operational contractor workforce. The necessary changes will be reflected in acquisition strategies, as well as in human resource plans. Short- and long-term plans will be developed in coordination with the Bureau of Human Resources for modernizing the FS, CS, LE staff, and EFM workforces through retraining, recruiting, and career development plans.

Lastly, the Department will take steps to foster a culture of IT consultancy - an attitude of intellectual curiosity that continuously seeks development opportunities while staying abreast of changing IT trends. A consulting skill set requires that IT professionals enhance abilities to translate business needs and proactively collaborate with colleagues to deliver services and technologies that improve the user experience and mission support. A workforce with an IT consulting skill set enables the adoption of cloud and other emerging technologies across the enterprise. Empowering the IT workforce in these ways will position the Department to meet its mission of delivering 21st century American diplomacy by effectively leveraging information and communications technologies.

Objective 5.3: IT Workforce Recruitment and Retention

Rapid advances in technology and changing business requirements make it essential to recruit and empower a diverse, agile, and highly-skilled IT workforce. The Department will continue shaping its workforce to reflect the diverse user-base and culture that its IT services reach. This includes embracing the diversity of individuals with different aptitudes, educations, and functional backgrounds.

Competitive marketplaces and budget constraints remain a top factor in recruiting capability. The transition to the cloud and other mobile technologies greatly affects how and where the Department acquires new skill sets. The Department must capitalize on research, data, and analysis to expand the use of competency-based hiring that relies on the latest input of KSA.

The qualities of KSA must transfer across tasks and work environments and must include industry and Departmental competency needs. In this regard, the Department must close critical competency gaps, particularly in the areas of cloud solutions, cybersecurity, IT program management, customer service, and acquisition management.

The IT professional of tomorrow must quickly adapt and transform over the course of their career from a hands-on, support specialist role to a strategist role who is able to align Department priorities while taking into consideration industry trends. Future recruiting initiatives will use data and strategic decision criteria to inform where and how the Department prioritizes recruiting activities and selects qualified candidates.

Table 5

Goal 5 – IT Workforce of the Future
<ul style="list-style-type: none"> • Develop and retain innovative, user-focused IT professionals with the skills to provide excellent consultative advice and support to managers and users Outputs: <ul style="list-style-type: none"> • Clarify IT job responsibilities and skill requirements for the cloud environment – Q2 FY 2019 • Develop a streamlined set of Foreign Service and Civil Service IT competencies for current and future IT occupations – Q2 FY 2019 • Reduce critical competency skill gaps – FY 2019 - FY 2021 • Develop a comprehensive Department-wide IT workforce planning process and staffing model • Increase the use of the Skills Incentive Pay program – FY 2019 - FY 2021 • Shift workforce from in-house infrastructure management to tasks needed for this plan – FY 2019 - FY 2022 Impacts: <ul style="list-style-type: none"> • Increased customer and user satisfaction ratings from baseline • Improved IT expert performance assessments versus cloud-oriented requirements • Reduced costs for on-premises infrastructure management • Build and recruit a talented, diverse IT workforce that is shaped and incentivized with the skills, talents, abilities, and development opportunities necessary to support modern American diplomacy Outputs: <ul style="list-style-type: none"> • Modernize IT vacancy announcements to support competency-based hiring – FY 2019 - FY 2022 • Expand partnerships for sourcing and recruiting highly qualified candidates – FY 2019 - FY 2022 Impacts: <ul style="list-style-type: none"> • Increased workforce capability to effectively manage cloud-based and upcoming technologies to serve the diplomats, customers, and the American people

Acronyms

Acronym	Meaning
AI	Artificial Intelligence
ATO	Authorization to Operate
BP	Bureau of Budget and Planning
BPA	Blanket Purchase Agreement
CASB	Cloud Access Security Broker
CIC	Cybersecurity Integrity Center
CIO	Chief Information Officer
CRM	Customer Relationship Management
CS	Civil Service
DCOI	Data Center Optimization Initiative
DCS	Department Cloud Strategy
DHS	Department of Homeland Security
DevOps	Development/Operations
DIN	Dedicated Internet Network
DME	Development, Modernization, and Enhancement
DS	Bureau of Diplomatic Security
EA	Enterprise Architecture
EFM	Eligible Family Member
EIMS	Enterprise Identity Management System
E-Gov PB	Electronic Government Program Board
ELA	Enterprise License Agreement
ESS	Enterprise Security Services
FACC	Foreign Affairs Cybersecurity Center
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act
FITARA	Federal Information Technology Acquisition Reform Act
FS	Foreign Service
FY	Fiscal Year
GPS	Global Positioning System
GWAC	Government-Wide Acquisition Contract
HVA	High Value Assets
IaaS	Infrastructure as a Service
IRM	Bureau of Information Resource Management
IT	Information Technology
ITSP	Information Technology Strategic Plan
JSOC	Joint Security Operations Center
JSP	Department of State and U.S. Agency for International Development Joint Strategic Plan
KSA	Knowledge, Skills, and Abilities
LE Staff	Locally Employed Staff
MGT Act	Modernizing Government Technology Act
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
O&M	Operations and Maintenance
PaaS	Platform as a Service
PMA	President’s Management Agenda
SBU	Sensitive but Unclassified
SIP	Skills Incentive Pay
TBM	Technology Business Management
WCF	Working Capital Fund