Functional Bureau Strategy

Information Resource Management (IRM)

FOR PUBLIC RELEASE

Approved: May 31, 2022

Table of Contents

Approved: May 31, 2022

1. Executive Statement and Mission Statement

During the two years of the COVID-19 pandemic, the workforce of the Department of State turned to mobile and remote-work technologies that fostered greater worldwide collaboration and sharing of information. Our previous Functional Bureau Strategy (FBS) laid the groundwork for these new technologies, which enabled the work of diplomacy to continue and thrive. IRM responded to the need for remote and collaborative technology in a swift and effective manner, bringing online new capabilities in record time. We provided the most current tools industry had to offer and, in the hands of our talented workforce, ushered in a new era for the Department. In a tactical response to unpredictable events, we drew upon the strength and determination of a committed workforce to establish an unprecedented telework capability.

IRM leadership will use this FBS to communicate its broad vision, mission, and strategic direction, and to align our strategy to our budget requests. It establishes a plan to ensure that the Department will capitalize on the IT gains realized over these incredibly difficult two years. The goals and objectives spelled out herein align to the U.S. Department of State and U.S. Agency for International Development FY 2022-2026 Joint Strategic Plan and the upcoming FY 2022-2026 IT Strategic Plan. Also reflected are new and existing Executive and Legislative Branch mandates that join with the agency-level strategies to address key activities such as implementing a zero-trust cybersecurity framework, establishing a more customer-centric culture, optimizing our multi-cloud environment, IT modernization, performance management, and advancing diversity, equity, inclusion, and accessibility.

This strategy establishes measurable goals to carry out the President’s Management Agenda by empowering the Department’s workforce, providing an excellent customer experience, and supporting the Department’s management and governance. Updated annually, this FBS establishes outcomes that IRM will accomplish over the next four years to support and enhance the Department’s foreign affairs mission.

IRM's FBS focuses on five strategic goals, including one management goal:

- **Goal 1: Cybersecurity**
- **Goal 2: Governance**
- **Goal 3: Innovation**
- **Goal 4: Customer**
- **Goal 5 (Management): Workforce**

IRM Mission: Deliver an innovative, accessible, and secure IT foundation for American diplomacy.

2. Bureau Strategic Framework

Bureau Goal 1: Cybersecurity – Enabling the mission while protecting assets.

- **Bureau Objective 1.1:** Adopt a Zero Trust security model.
- **Bureau Objective 1.2:** Secure the IT enterprise with advanced technology.
- **Bureau Objective 1.3:** Implement mission-effective Risk Management.

Bureau Goal 2: Governance – Strengthened IT management and service delivery.

- **Bureau Objective 2.1:** Establish oversight structures and processes.
- **Bureau Objective 2.2:** Build Agility into IT processes.
- **Bureau Objective 2.3:** Create a standardized IT acquisition program.

Bureau Goal 3: Innovation – Mission effectiveness and modernization.

- **Bureau Objective 3.1:** Leverage a shared, secure cloud environment.
- **Bureau Objective 3.2:** Improve Business intelligence and automation.
- **Bureau Objective 3.3:** Modernize mission and management systems.

Bureau Goal 4: Customer – Supporting our diplomats through IT services and human-centered solutions.

- **Bureau Objective 4.1:** Improve end user experience.
- **Bureau Objective 4.2:** Empower system owners with effective tools and processes**.**
- **Bureau Objective 4.3:** Create a service-oriented culture.

Bureau Cross-Cutting Management Goal 5: Workforce.

- **Bureau Cross-Cutting Management Objective 5.1:** Identify, attract, and hire a talented and diverse workforce.
- **Bureau Cross-Cutting Management Objective 5.2:** Promote employee learning.
- **Bureau Cross-Cutting Management Objective 5.3:** Mentor and develop IT Professionals.

3. Bureau Goals and Objectives

Bureau Goal 1: Cybersecurity – Enabling the mission while protecting assets.

- **Bureau Goal 1 Description:** Cybersecurity is an enduring priority and a key consideration in every Department IT decision. IRM will continue to employ an effective cybersecurity program to identify, protect, detect, respond, and recover from cybersecurity incidents in collaboration with the Bureau of Diplomatic Security. We will also ensure that security policies, tools, and solutions enable diplomacy and are an integral part of the functional mission and administrative IT solutions available domestically and overseas.

  We will design security controls into systems as they proceed through their life cycle and protect all IT assets with contingency and recovery plans. For systems authorization, we will implement an ongoing authorization program to continually manage risk, transitioning systems that meet the criteria into ongoing authorization and ultimately eliminating the three-year Authorization to Operate (ATO) process.

  IRM will build the foundations for a zero-trust network environment with a defined strategy and CIO-approved implementation plan that moves us to an assured security posture. We will enhance and strengthen our IT security architecture to enable software defined networking, mobile security, and end-point security. IRM will build and provide secure internal and external tools to support collaboration with civilian and military agencies, non-governmental organizations, contractors, the American public, and other nations. We will closely examine and implement the necessary technologies and processes in support of supply chain risk management. In addition, we will collaborate with the Bureau of Diplomatic Security to instill robust security technologies with improved detection and response, increased monitoring of our assets, as well as leveraging automated capabilities and increased cyber workforce capabilities.

Bureau Objective 1.1: Adopt a Zero Trust security model.

- **Bureau Objective 1.1 Justification and Linkages:** Adopting a Zero Trust cybersecurity model is mandated by OMB memorandum M-22-09 to improve the federal government's cybersecurity approach beyond the traditional perimeter defense. IRM will pattern its implementation on the Cybersecurity and Infrastructure Security Agency (CISA)'s maturity model. Zero Trust is one of the Agency Priority Goals in Objective 4.3 in the JSP.
- **Bureau Objective 1.1 Risk Considerations:** Risks of failing to secure the Department's mission critical infrastructure and information include adversaries accessing sensitive or classified diplomatic information, damage to the Department's credibility (e.g., Wikileaks), loss of critical operational data, loss of operational capabilities, and a myriad of other negative impacts to the Department's operations.

Bureau Objective 1.2: Secure the IT enterprise with advanced technology.

- **Bureau Objective 1.2 Justification and Linkages:** This objective links to the JSP's security goal 4.3. IRM will use new cybersecurity technologies that harness the power of artificial intelligence (AI) to create intelligent protection that can spot and thwart threats immediately, reconfiguring networks and systems on the fly, and automatically trace a breach to its source. An updated security architecture will focus on information secured at the data level as opposed to the perimeter or system level, thereby enabling shared data in the cloud and access to information by a wide variety of devices.

  IRM will adhere to the National Cyber Strategy, President's Management Agenda (PMA), National Institute of Standards and Technology (NIST), Federal Information Security Management Act (FISMA), Agency Performance Goals, and Federal IT Acquisition Reform Act (FITARA) Scorecard assessment areas. It will incorporate a high-level cybersecurity governance framework applied to specific, tactical-level cybersecurity activities and programs.

- **Bureau Objective 1.2 Risk Considerations:** Risks of failing to incorporate emerging technologies in securing the enterprise include increased numbers of successful breaches, increased data exfiltration, and higher probably of undetectable attacks.

Bureau Objective 1.3: Implement mission-effective Risk Management.

- **Bureau Objective 1.3 Justification and Linkages:** The primary goal of cyber risk management is to balance mission requirements with the likelihood and severity of threats, enabling the rapid introduction of new technology while implementing cybersecurity best practices. IRM will expand our cyber risk management program, fully integrating it into the Department's enterprise risk program. In alignment with NIST SP 800-39 "Managing Information Security Risk" and NISTIR 8286 "Integrating Cybersecurity and Enterprise Risk Management," IT investment and portfolio decisions will align with the Department's IT cybersecurity objectives while in full support of all mission objectives. IRM will implement OMB guidance on supply chain risk management.

  IRM will establish policies that enable the bureaus to better balance mission accomplishment with the risks introduced by new technologies. The CIO, as the Designated Approval Authority (DAA) for all IT (including cyber) risk management decisions, will consider input from affected stakeholders including information technologists, business owners, and customer bureaus when making decisions about new or enhanced technologies. To manage cyber risk, IRM will implement analysis and reporting capabilities through the Cyber Risk Management (CRM) Program to measure cybersecurity programs' effectiveness in reducing Department risk exposure and in achieving regulatory compliance. IRM will produce quarterly cyber performance scorecards for bureaus across the Department to raise awareness of cyber risk posture and support mitigation of existing cyber risks. We will continue to mature analysis and reporting capabilities, aligning with the Department strategic priorities and newly established FISMA metrics.

- **Bureau Objective 1.3 Risk Considerations:** Without risk management policies in place to enable information owners to make informed risk decisions, the Department could adopt an unnecessarily risk-adverse posture, resulting in lower mission performance and higher costs for security. Conversely, it is possible that the Department could introduce intolerable risks that result in negative impacts to operations.

Bureau Goal 2: Governance – Strengthened IT management and service delivery.

- **Bureau Goal 2 Description:** Efficient IT leadership, governance, and organization will transform IT management and delivery in support of our diplomatic and development mission and customer requirements. New legislation, directives, and plans create a bold challenge for federal agencies to rapidly innovate, modernize, and secure IT assets and programs to improve service delivery and increase efficiency and security. The Department will meet these challenges through disciplined governance through the ITEC processes strengthened oversight processes, increased collaboration with Department bureaus, and increased reliance on shared services, including a streamlined IT acquisition process. We have made considerable progress toward this goal in FY 2021 and this FBS highlights our progress. The bottom line is our commitment to deliver the best IT service, offering customers rapid access to the technology solutions they need by breaking down bureaucratic barriers, and working collaboratively within an Agile framework.

Bureau Objective 2.1: Establish oversight structures and processes.

- **Bureau Objective 2.1 Justification and Linkages:** The Department develops and maintains many mission-critical IT investment programs, many of which are global, complex, and serve a widespread user community. Multiple bureaus manage these investments with expertise in specialized functional and mission areas (e.g., Consular, Finance, Human Resources, Logistics) and supported by specialized integration contractors. A consistent oversight process, executed under the direction of the CIO, is essential for ensuring effective control and governance over the Department's IT investments, aligning all IT investments with the Department mission. This objective links to FITARA, which mandates that the CIO maintain oversight of all IT investments.
- **Bureau Objective 2.1 Risk Considerations:** The risks of failure to provide effective central oversight include cost overruns, duplicative investments, solutions that do not conform to standards, and solutions that do not meet customer requirements or align with the IT Strategic Plan (ITSP).

Bureau Objective 2.2: Build Agility into IT processes.

- **Bureau Objective 2.2 Justification and Linkages:** Agile processes for IT governance and systems development offer numerous benefits including rapid introduction of solutions, incremental processes that reduce risk, and effective engagement and collaboration with customers and other stakeholders. Under this objective, IRM will build agility into the governance process, streamlining the approval process for customers and engaging stakeholders in all governance processes. IRM will also adopt Agile methods for IT solution development. This objective links to President's Management Agenda customer service goal and the JSP Goal 4, Revitalize the diplomatic and development workforce and institutions.
- **Bureau Objective 2.2 Risk Considerations:** The risks of failing to achieve this objective are inability to meet customer and mission requirements for IT solutions, and unnecessary delays in the introduction of new and vital products and services.

Bureau Objective 2.3: Create a standardized IT acquisition program.

- **Bureau Objective 2.3 Justification and Linkages:** The IT acquisition process has substantial influence on IT delivery. It is also a significant cost and risk driver of IT service delivery. Effective management of our resources requires a robust IT acquisition function that delivers the necessary services while providing the budget and investment information required for effective management decisions and oversight. In keeping with the PMA, the Department will remove friction in the IT acquisitions process, break down barriers to entry, and enable just-in-time delivery and greater resiliency of our contracting base. Creating a central, dedicated IT Acquisitions Office in IRM aligns with the requirements of FITARA and establishing a secure IT supply chain is mandated by recent executive orders on cyber security, including E.O. 14028 on Improving the Nation's Cybersecurity.
- **Bureau Objective 2.3 Risk Considerations:** Lack of a central, enterprise-wide IT acquisition functions leads to inconsistent, inefficient, and duplicative procurement actions resulting in higher costs, slower procurement times, failure to capture economies of scale, and non-standard IT solutions that are costly to support. Lack of centralized IT acquisition functions also adds security risk through non-standardized software and hardware, lack of enterprise security controls, and a potentially insecure supply chain.

Bureau Goal 3: Innovation – Mission effectiveness and modernization.

- **Bureau Goal 3 Description:** Modernization is a constant of the IT environment, including optimizing our cloud infrastructure, supporting a distributed workforce with mobile technology, replacing aging computers and network infrastructure with more energy efficient devices, deploying Wi-Fi, updating business applications, integrating new technology, and developing applications used by individual missions and bureaus.

Bureau Objective 3.1: Leverage a shared, secure cloud environment.

- **Justification and Linkages:** Under this objective, IRM will establish a multi-cloud environment based on the business needs of our customers, and a holistic approach for managing, securing, and iteratively improving the Department's cloud portfolio. Our approach is based on JSP performance goal 4.2.3 and the CIO's Cloud Strategy. This objective is critical for enabling the Department to adopt cloud technology effectively, in compliance with OMB mandates and strategies, and yielding the benefits of cloud computing such as access to enhanced security technologies, ability to expand and contract access to IT resources, and standardization across the enterprise.
- **Risk Considerations:** The risks of not optimizing and orchestrating cloud use in the Department include duplicative purchases of cloud services, increasing costs, hindering the development of cloud solutions by our customers due to the difficulty of establishing cloud services, and missing vital security precautions in the setup and configuration of cloud services.

Bureau Objective 3.2: Improve Business intelligence and automation.

- **Justification and Linkages:** This objective covers our support of the Department's data and geospatial strategies along with our integration of commercial artificial intelligence and robotic process automation. This section links to JSP performance goal 4.2.1, the Enterprise Data Strategy, and the Geospatial Data Strategy.
- **Risk Considerations:** The risks of not implementing business intelligence and artificial intelligence include not being able to make evidence-based decisions, missed opportunities to save labor and money through gains in efficiency, and missed opportunities to visualize and understand information.

Bureau Objective 3.3: Modernize mission and management systems.

- **Justification and Linkages:** This objective addresses the need for agencies to modernize per the Modernizing Government Technology Act of 2017 and recent OMB guidance. This includes refresh of IT equipment in the Department with more energy efficient devices, the modernization of business system platforms, and integration of new technologies and services to improve our customer service and diplomatic reach.

  The Department will continue deploying wireless technologies such as Wi-Fi and Low Earth Orbit (LEO) satellite systems to improve access to cloud services from mobile devices, reduce latency, and provide reliable backup in case of emergency. These wireless systems will become increasingly important in providing network services to the Department. We expect to resume Wi-Fi deployments in 2023 and reach a rate of deployments to complete installations by calendar year 2025. In 2023 we will initiate LEO deployments assuming the remaining technical issues with LEO are resolved. The plan is to deploy at least one hundred satellites receivers in the next two years in domestic and overseas locations. These numbers might increase dramatically if additional countries grant host nation approval for LEO providers to operate.

- **Risk Considerations:** Not modernizing our equipment and systems will introduce the following risks: security breaches and downtime due to aging and unsupported software and equipment, inability to accommodate new business requirements and share data between systems due to outdated platforms, and lack of relevance in our communications and outreach efforts due to outdated technology.

Bureau Goal 4: Customer – Supporting our diplomats through IT services and human-centered solutions.

- **Bureau Goal 4 Description:** This goal focuses on enhanced service to IRM's customers in response to the PMA customer service goal. IRM will realign its business functions to be more responsive to customer and business needs, delivering customer-centric IT products and services that use Human-Centered Design (HCD). HCD will ensure high levels of usability, identical digital experience whether working remotely or on-site, excellent support for mobile access regardless of device, and one-stop shopping for IRM services. Goal 2 in this FBS (Governance) will also contribute to customer service by engaging stakeholders through Agile processes and streamlined decision-making, approval, and technology introduction.

Bureau Objective 4.1: Improve end user experience.

- **Bureau Objective 4.1 Justification and Linkages:** The purpose of IT is to enhance users' ability to do their jobs in the service of the Department's mission, and this objective will ensure that IRM's offerings do just that. Regular engagement with customer bureaus and overseas posts will ensure that technology solutions meet user functional and performance requirements and will enable IRM to develop common post applications for worldwide use, minimizing the learning curve as Foreign Service officers move from post to post. HCD will minimize the kinds of frustrations that users experience with software applications, for example, ease-of-use and eliminating duplicative data entry across systems. A consistent interface will also enhance user productivity by providing access regardless of location and device. This objective is linked to the JSP Goal 4, revitalize the diplomatic and development workforce and institutions. IRM will coordinate with other bureaus to ensure that the required hardware and software are available when needed.

- **Bureau Objective 4.1 Risk Considerations:** The risks of failure to deliver this objective are high levels of user dissatisfaction, leading to one-off workarounds that are inefficient, ineffective, duplicative, costly, and create the potential for cyber security vulnerabilities.

Bureau Objective 4.2: Empower system owners with effective tools and processes.

- **Bureau Objective 4.2 Justification and Linkages:** Customer service is a PMA goal, and it is a high priority of the CIO. Providing support to system owners will increase their ability to provide excellent customer service, and that system owner support is linked to JSP performance goal 4.2.3. IRM will establish a dynamic partnership with system owners to streamline the delivery of customer-driven systems. We will provide expert consultation, tools, and training in modern Agile/DevSecOps processes and "no code/low code" solutions, as well as decision support for choosing and adopting technology solutions with an emphasis on promoting available shared services. We will provide AI-based tools to help system owners manage and monitor their systems to ensure high performance and high levels of user satisfaction. We will modernize the management of centralized IT services funded via the Working Capital Fund (WCF) by updating fee structures, service level agreements, centralizing governance across all service lines and gradually expanding the services funded through the WCF. This objective is critical to the transformation of IRM into a high-performing customer service organization.
- **Bureau Objective 4.2 Risk Considerations:** The risks of failure are diminished system owner effectiveness in deploying required IT solutions, increased costs due to inefficiencies and lower levels of use of common solutions, and reduced confidence in IRM as a customer service partner.

Bureau Objective 4.3: Create a service-oriented culture.

- **Bureau Objective 4.3 Justification and Linkages:** Building on internal service offerings in Objective 4.1 and support to system owners in Objective 4.2, IRM will build a corporate culture of customer service to satisfy the PMA customer service goal. This cultural change will entail the following artifacts: updating IRM's Service Catalog, consolidating service delivery to ensure consistency in service level agreements and performance metrics, and consolidating ordering and billing through a one-stop-shop concept. IRM will apply advanced AI and other technologies to monitor and improve customer service and will continue its incorporation of best practices and standards for IT service excellence. This objective is a high priority of the CIO, and it links to efforts to create a modern, dynamic post-Covid work environment. A modern, high performing IRM service infrastructure will achieve economies of scale by eliminating the need for bureaus to maintain their own service operations.
- **Bureau Objective 4.3 Risk Considerations:** The risks of failure in this area include inability to support important Department priorities such as creating a post-Covid work environment, as well as increased costs resulting from inefficiencies and duplicative service centers.

4. Bureau Cross-Cutting Management Goal

Bureau Cross-Cutting Management Goal 5: Workforce.

- **Bureau Cross-Cutting Management Goal 5 Description:** IRM will empower IT talent to meet rapid advances in technology, changing business requirements, and our focus on customer service. To that end, we will close competency gaps by seeking a diverse, equitable, inclusive IT workforce with a strong commitment to the Department's global mission. We will sustain these highly capable IT professionals through continuous mentoring, learning, development, and career progression.

Bureau Cross-Cutting Management Objective 5.1: Identify, attract, and hire a talented and diverse workforce.

- **Bureau Cross-Cutting Management Objective 5.1 Justification and Linkages:** The Department's overall IT employment has decreased since 2016, but the number of IT positions has increased. These trends have significantly affected IRM, which is experiencing IT vacancies in numerous key job categories. Skill gaps exist for emerging technologies, particularly in the competencies needed for information security (including cybersecurity), IT consulting, enterprise systems and technology (including cloud technologies), project management, and acquisition management.

  Furthermore, over 20 percent of Civil Service and Foreign Service IT employees are at or near retirement eligibility. The bureau will need to attract and hire many new recruits in today's competitive job market. IRM will establish and expand recruiting relationships with organizations that foster IT talent, including universities, trade schools, technology programs, and military transition programs. We will also provide recruits with more representative, realistic job previews. IRM will expand its Cyber Security Incentive Pay for recruitment and retention across the 7 categories as identified in the NICE framework. It will move beyond the pilot state and further create opportunity for inclusion across all bureaus with applicability to cybersecurity professionals. Finally, because IRM recognizes the need for employee retention, IRM will review its organizational culture and talent management processes to identify areas of improvement.

This objective supports higher level strategies and findings contained in the Department's State-USAID Joint Strategic Plan, Goal 4; IT Strategic Plan, Goal 5; the Department's Five-Year Workforce Plan; the Foreign Service Competency Study; and Domestic IT Competency Study.

- **Bureau Cross-Cutting Management Objective 5.1 Risk Considerations:** The Department must be able recruit and fill positions for the competencies required to provide optimal IT services and technologies in a constantly evolving IT environment. This is best accomplished by finding optimal talent from a diverse spectrum of professionals representing all age groups. The risks of not doing this include hiring the wrong candidates, loss of productivity, high turnover, continuous retraining, degraded morale, and the inability to achieve bureau goals and objectives.

Bureau Cross-Cutting Management Objective 5.2: Promote employee learning.

- **Bureau Cross-Cutting Management Objective 5.2 Justification and Linkages:** The diplomatic workforce is becoming more digitally connected and dependent on information technology to do their jobs. This creates rising expectations on IRM's IT workforce to deliver new solutions and provide effective and efficient support and consultative services. IRM's IT professionals need continual development, training, and feedback from leaders. Furthermore, IRM will maintain a close proactive partnership with FSI/SAIT to provide relevant training and curriculums to enable IRM's workforce to close skill gaps in the latest technologies, innovations, and practices. It is important to establish a circle of certified program and project managers. IRM in coordination with AQM will evaluate and expand a program to train project managers across the bureau and organization.

This objective supports strategies and findings contained in the State-USAID Joint Strategic Plan, Goal 4; the Department's Five-Year Workforce Plan; the Foreign Service Competency Study; Domestic IT Competency Study.

- **Bureau Cross-Cutting Management Objective 5.2 Risk Considerations:** Inadequately trained and underdeveloped employees are likely to experience poor job performance and increased levels of work-related stress. The risks of not accomplishing this objective include loss of productivity, poor customer service and innovation, low morale, high turnover, and the inability to achieve bureau goals and objectives.

Bureau Objective 5.3: Mentor and develop IT Professionals.

- **Bureau Cross-Cutting Management Objective 5.3 Justification and Linkages:** Mentoring and robust career paths are important tools for promoting employee learning and growth. Having senior and more experienced employees advise and support employees earlier in their careers has a variety of benefits including job satisfaction, career progression, productivity, skills development, teamwork, customer service, and succession planning. Establishing effective and attractive career paths also helps achieve these benefits. Finally, being able to retain the institutional knowledge of highly experienced career employees prevents the loss of vital skills and information.

  This objective supports higher level strategies and findings contained in the State-USAID Joint Strategic Plan, Goal 4; IT Strategic Plan FY 2019-2022, Goal 5; SWPs IT Workforce Analysis Report, Goal 1, and the Department's Five-Year Workforce Plan.

- **Bureau Cross-Cutting Management Objective 5.3 Risk Considerations:** A mentoring program helps to prevent several risks, including the loss of vital institutional knowledge, poor employee morale, high turnover, lower productivity, and poor customer service. Retaining highly experienced IT professionals also helps to retain our wealth of IT knowledge.