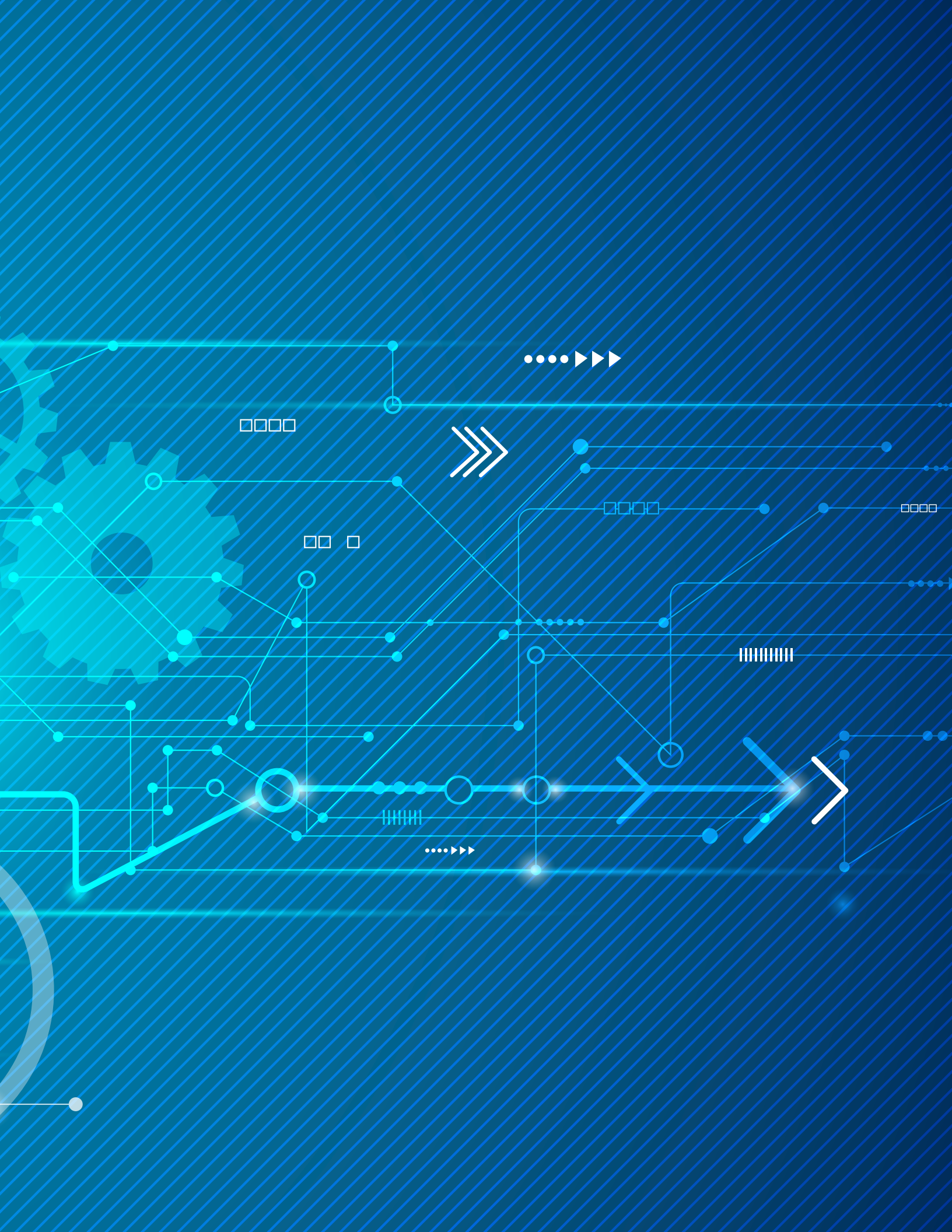
DEPARTMENT OF STATE

INFORMATION TECHNOLOGY STRATEGIC PLAN

FISCAL YEARS 2017–2019



MESSAGE FROM THE CHIEF INFORMATION OFFICER

I believe we are on the verge of a new era of diplomacy. Rapid changes in technology are transforming how we advance U.S. foreign policy by altering the way we connect with others and communicate information. Our diplomats are using powerful new technologies to advocate policy positions, promote awareness, and enhance transparency.

This plan is intended to embrace and seize on the opportunities presented in the new information technology (IT) environment. It is the culmination of more than a year of extensive conversations with stakeholders in bureaus, offices, and overseas posts to identify strategic themes that reflect the Department's IT priorities. The three themes that emerged from these discussions were **Innovative Diplomacy**, **Global IT Infrastructure**, and **IT Business Management**. With these priorities as drivers, the IT Strategic Plan (ITSP) articulates how innovative technology, sound governance practices, and a committed workforce contribute to mission effectiveness and operational efficiency within a constantly changing IT landscape.

The Department's IT strategic vision is to fulfill its diplomatic mission through a secure infrastructure and innovative technologies for our workforce. It sounds simple enough, but we must think boldly to identify and implement forward-leaning solutions that support operational tempo and real-time diplomacy. We must take calculated risks to give our customers reliable products that access the Department's data and allow our diplomatic workforce to make informed decisions. We must maintain optimal performance of IT systems while protecting our users, information, networks, and global IT assets. We must promote accountability through transparent communication with our customers and stakeholders.

As we work to achieve this vision, we will engineer IT solutions that meet our strategic goals, objectives, and requirements while balancing security and usability. Together, we can make the Department more effective in using IT to fulfill its mission while encouraging mobility and accessibility.

Let us not settle for anything short of fully realizing that vision.

Sincerely,

Frontis B. Wiggins
Chief Information Officer

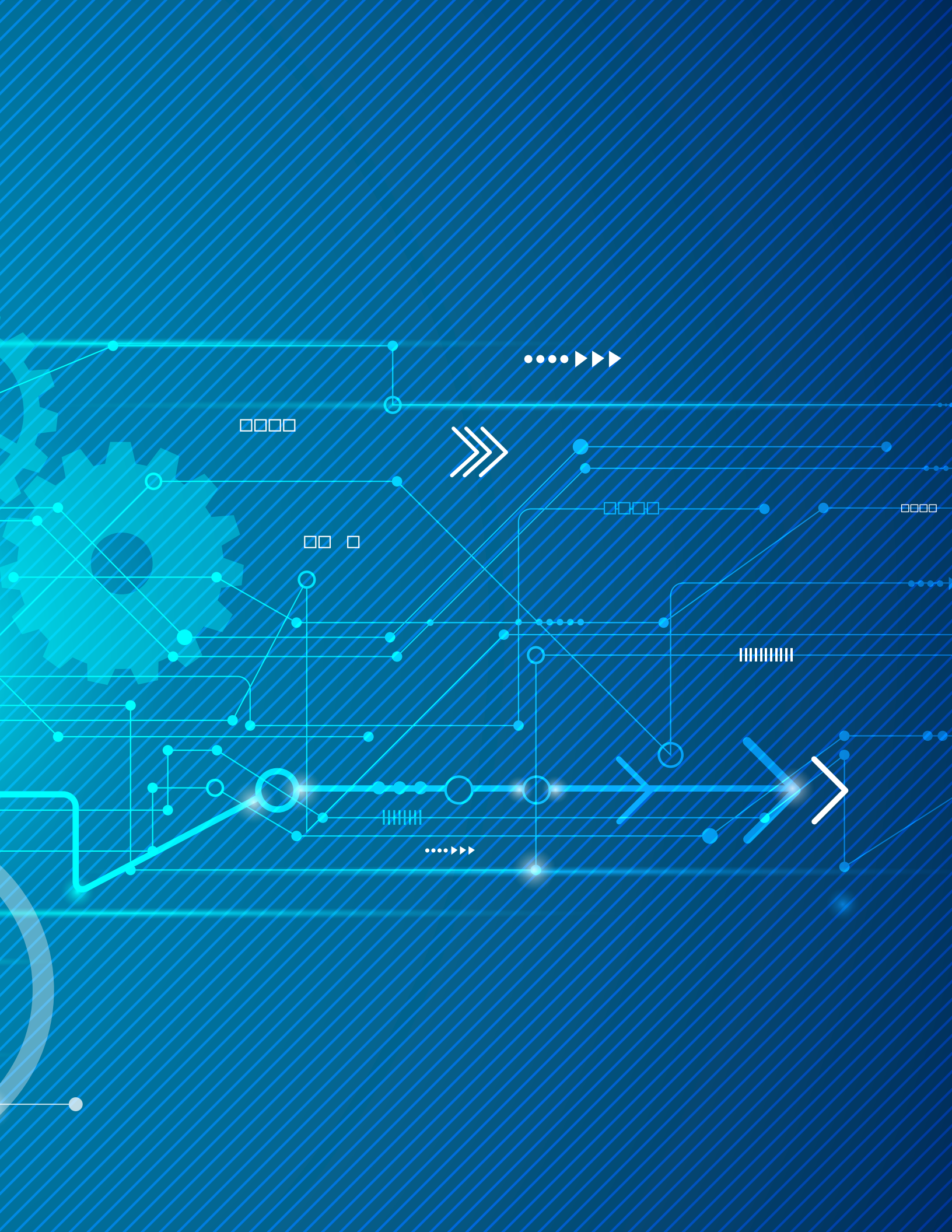
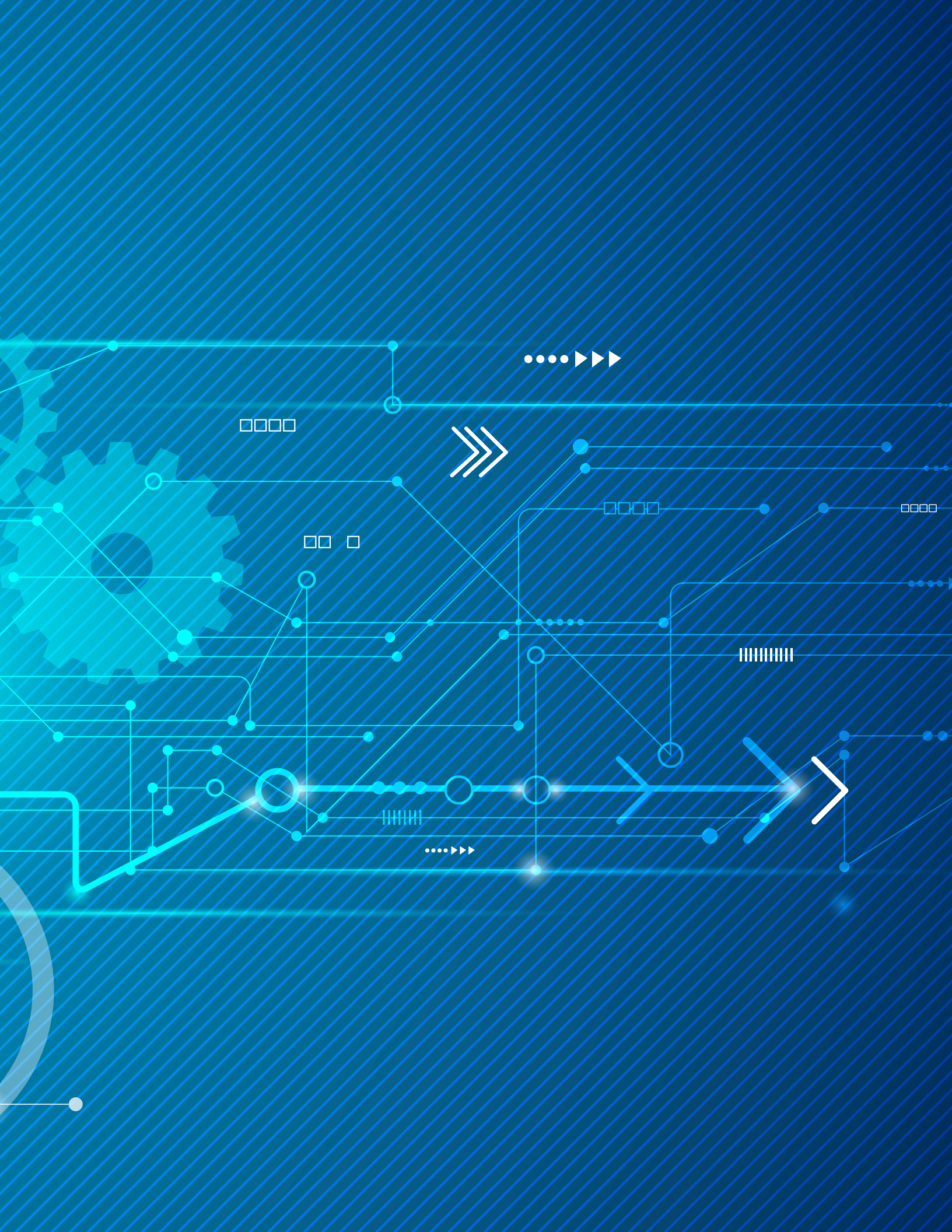


TABLE OF CONTENTS

Introduction 1
Department IT Vision and Mission 2
IT Strategic Goals and Objectives 3
    Goal 1: Innovative Diplomacy 3
    Goal 2: Global IT Infrastructure 6
    Goal 3: IT Business Management 10
Performance Metrics 14
IT Governance Structure 15
    Structure of IT Governance Boards 15
    IT Budget Review 15
    Chief Information Officer Roles and Responsibilities 15
    Chief Information Security Officer Roles and Responsibilities 15
Acronyms 16
Acknowledgments 17



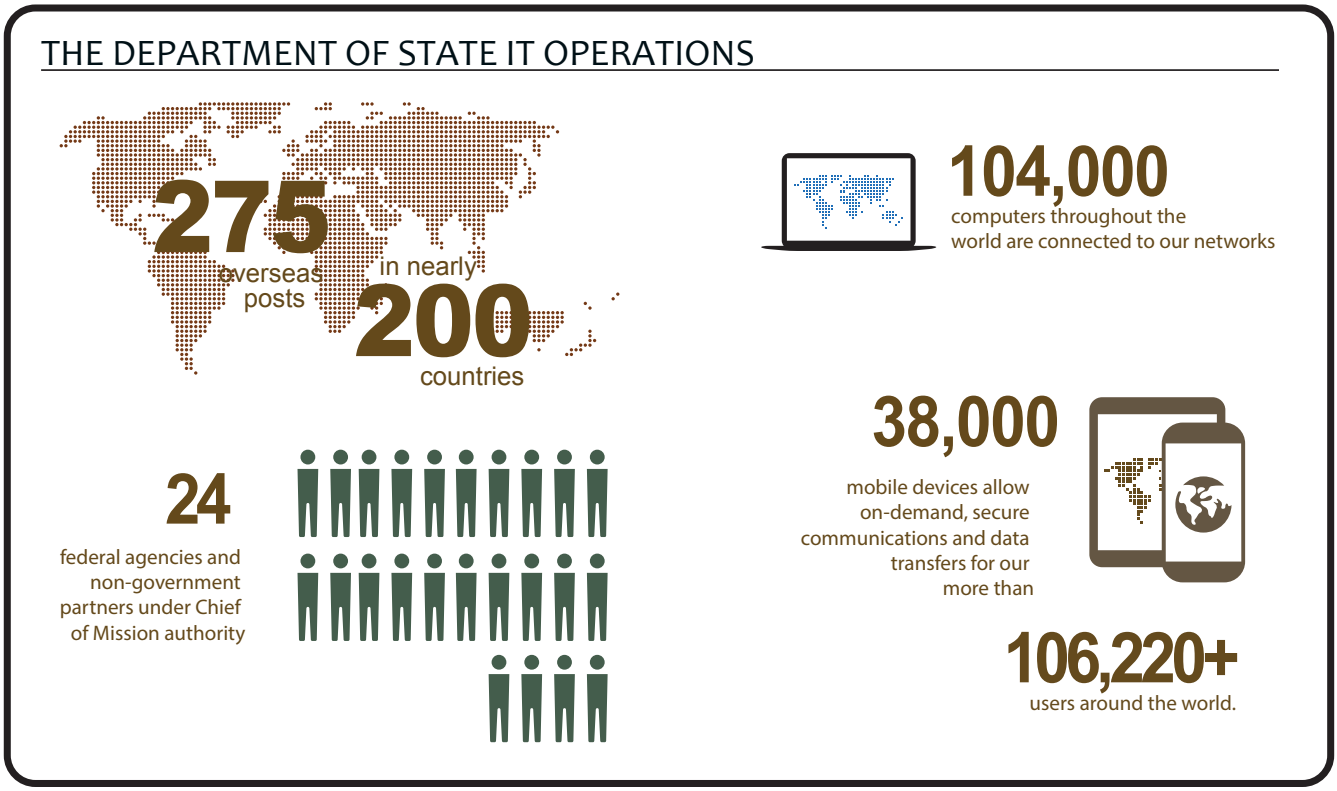
INTRODUCTION

Since it was founded in 1789, the Department of State has played a key role in advancing America's interests around the world. The work of our diplomats has never been without risk, yet the pace and scale of modern challenges is without equal. This requires the Department to leverage emergent technologies that empower our diplomats and professionals to accomplish the foreign policy mission.

The Department's IT operations are complex and far-reaching. We maintain hundreds of applications, and provide around-the-clock IT services, domestically and abroad at over 275 overseas posts in nearly 200 countries, including 24 federal agencies and non-government partners under Chief of Mission authority. More than 104,000 computers throughout the world are connected to our networks, and 38,000 mobile devices allow on-demand, secure communications and data transfers for our more than 106,220 users around the world.

The purpose of this plan is to drive the Department's future IT programs and resources, and to maximize value to an increasingly mobile customer base. The vision and strategic goals reflected in this plan are in alignment with the Quadrennial Diplomacy and Development Review (QDDR), the Department of State and U.S. Agency for International Development (USAID) Joint Strategic Plan (JSP), and Department functional bureau and regional strategies.

The ITSP, together with the Enterprise Architecture Roadmap, provides a comprehensive view of the Department's IT capabilities, current and target architecture states, and prescribes a plan for transitioning forward.



DEPARTMENT IT VISION AND MISSION

Vision

Drive necessary and effective IT capabilities for improved operations and collaboration across the Department, its partners, and foreign audiences.

Mission

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

INNOVATIVE DIPLOMACY

GOAL 1: DELIVER ADVANCED CAPABILITIES TO FOSTER COLLABORATION, KNOWLEDGE MANAGEMENT, AND ANALYTICS

Technological advances in today's digital IT environment offer an almost borderless arena for collaboration, knowledge management, data analysis, and innovation. Capabilities are developing at an exponential rate to capture, manage, analyze, and retrieve vast amounts of information in order to build relationships, engage with broader constituencies, foster openness, and achieve transparency. Technology and innovation are invaluable tools for engaging our foreign partners, and will continue to connect people to the knowledge and information they need when they need it in support of foreign policy and operations.

We will continue to broaden access to institutional knowledge and expand collaborative tools to enhance problem-solving throughout the Department. In addition, we will work to achieve the vision that information we are producing should become part of a comprehensive, shared, secure, and easily accessible knowledge system. Armed with IT tools, our employees will be better prepared to communicate and collaborate in real-time. Through these efforts, we will build and sustain interpersonal connections and workplace relationships in a technology-driven era.

INNOVATION THROUGH TECHNOLOGY

The School of Applied Information Technology (SAIT) at the Foreign Service Institute (FSI) established the Innovation Sandbox in 2016 to explore the nexus between technology and diplomacy with the ultimate goal of fostering more effective diplomacy through better uses of IT. The Sandbox will promote both procedural and programmatic innovation in the use of IT in the conduct of American diplomacy by gathering best practices from industry leaders and researchers in academia about new and emerging technologies, and lessons learned from diplomats about their experiences in the conduct of diplomacy and the ways in which existing IT applications have facilitated or impeded the execution of their work overseas.

Objective 1.1 (Collaboration)

Enhance collaboration across the Department through digital solutions to inform and engage internal and external audiences.

More than ever, our work depends on tools and methods that allow us to share and develop information across the enterprise, with external partners, and the public. Our experience shows us that new uses of interactive technologies have the capacity to expand and strengthen relationships. We continue to make progress engaging the expanding population that lives online, through social media and the increased use of mobile audio and video conferencing technologies. Today's collaborative tools deliver tailored content and messaging that is available and accessible to Department employees, and shareable to members of the public and foreign audiences.

Within the Department, we must create ways for employees to exchange ideas, information, and questions by employing tools to allow our professionals to seek answers from their peers, strengthen connections between colleagues, and transfer knowledge. Implementation of an enterprise-wide social network aimed at increasing collaboration and connecting the Department's many subject matter experts will enable us to preserve and share information.

Objective 1.2 (Knowledge Management)

Ensure the availability of and access to information that enables customers to make timely, informed decisions by strengthening data and knowledge management approaches.

Knowledge management represents a systematic approach to capturing, organizing, and retrieving information to support the Department's activities and enhance decision-making. It involves the processes for creating, storing, sharing, and integrating data to increase the flow of information between offices, bureaus, and posts. Engaging experts from across the Department will improve records management practices, streamline the information lifecycle, and capitalize on existing systems and platforms, such as internal wikis, geographic information systems, and new and emerging enterprise software. Knowledge management will be enriched by data sharing between internal systems in order to index and analyze data and by providing open data sets for the public. We will improve knowledge discoverability, and will further develop knowledge management tools, training, and methodologies.

The Department produces and stores vast amounts of knowledge and data every day. Managing these elements requires centralized knowledge repositories and standard data elements to reduce duplication, facilitate sharing, improve accessibility, and automate workflows among bureaus and offices. Not only will these repositories serve as a portal to shared knowledge, they will expedite our ability to reduce the number of paper-based processes and records. Improving knowledge management will increase our capacity to enable faster retrieval and more accurate results. Coupled with evolving knowledge management tools, we will facilitate for our users better insight and a heightened understanding of the vast quantities of knowledge and information available to them.

Objective 1.3 (Data Integration and Analytics)

Promote an enterprise approach to information sharing that fosters decision-making through the use of analytic technology.

Harnessing the power of voluminous and complex datasets (big data) can offer more meaningful insights required for informed decisions, problem-solving, and risk analysis. While aggregate data is important, distilling datasets into actionable intelligence through innovative analytics and business intelligence support rapid decision-making and improve operational efficiencies.

Expanding the use of research and analytic tools will provide Department decision-makers more complete and accurate reporting that can be used to align bureau core functions, develop policy priorities, and identify emerging trends and future demands. Through advanced data integration and analytics, we will make it easier for decision-makers and employees to find data. Our efforts to foster information sharing will require execution of a broad array of data disciplines, including data warehousing, data integration, data quality, and analytics. This will advance the integration of standard and non-standard data, and support the Department's strategic data and technology objectives in the QDDR.

PERFORMANCE METRICS
Define and implement standard policies, procedures, formats, and tools for managing all permanent electronic records electronically by December 2019.
Adopt new information technologies to improve business and IT operations.
Increase number of datasets registered in the enterprise data catalog to reduce data redundancies.
Apply data policies and associated standards from the Master Reference Data platform to support data integrity.
Establish a research and development (R&D) function and customer requirements office for IT solutions.
Increase the use of data analytics tools to inform policy and business decisions.

GLOBAL IT INFRASTRUCTURE

GOAL 2: PROVIDE A ROBUST AND SECURE IT INFRASTRUCTURE THAT SUPPORTS ON-DEMAND ACCESS TO INFORMATION

Department of State diplomats and the global workforce that supports them depend on a modernized, secure, and scalable IT infrastructure to accomplish their mission. Hardware, software, network connectivity, and cybersecurity protections must support the seamless operation of digital tools and a diverse suite of applications. The IT infrastructure must be secure, resilient, and meet worldwide conditions for on-demand access, including increased mobility through wireless connectivity on an array of devices. In addition, modernization efforts enable us to adopt new energy efficient technologies and practices to promote sustainability. Cloud computing initiatives allow us to achieve our goals for increased collaboration, sharing, productivity, mobility, and security. Ongoing investments in cloud-based programs and services enhance the Department's IT infrastructure lifecycle and allow for rapid scalability.

One of our top priorities is protecting our information and IT assets against increasing cyber threats and vulnerabilities. We depend on network and information systems for essential operations and data security. Any failure or disruption of services resulting from a cyber-attack may have adverse consequences for the Department. To address these threats, the Department is investing resources into cyber defense capabilities to mitigate risks and strengthen our cybersecurity posture.

Objective 2.1 (Modernized IT Infrastructure)

Deploy a modernized IT infrastructure that enables seamless access to information resources.

The modernization of our systems, networks, and platforms is imperative to protect business-critical applications and data. The Department must adapt the network architecture to counteract increasingly sophisticated threats by isolating and segmenting critical business data and IT assets to protect sensitive and personally identifiable information (PII). Domestic and overseas virtualization, in addition to hardware and software refresh efforts, will create more secure, flexible server and desktop environments. Virtual capabilities also support data replication to off-site locations, including Department data centers for quicker backups and reliable continuity of operations.

Developing a modernized and secure IT infrastructure that harnesses new information delivery models will enhance the Department's voice, network, data, radio, and video capabilities, providing secure platforms for Department communications and emergency life-safety and command and control situations. Our continued commitment to green and sustainable computing strengthens the Department's environmental stewardship and reduces its environmental footprint. By optimizing data centers, adopting energy efficient technologies, leveraging enterprise licensing, maximizing the use of shared services and acquisition vehicles for IT purchases, and executing strategic sourcing initiatives, we will lower IT operational costs and energy consumption.

Objective 2.2 (Cybersecurity)

Protect the integrity of the Department's information and IT assets by strengthening our cybersecurity posture.

The Department is under constant assault from threat actors seeking to steal sensitive information regarding high-profile diplomacy matters such as trade, economics, politics, and national policy. Our cybersecurity strategy outlines an approach to securing our perimeter and preventing intrusions through a holistic cybersecurity program led by the Chief Information Security Officer (CISO). The strategy implements leading practices for comprehensive cybersecurity from the National Institute of Standards and Technology's (NIST) Risk Management Framework and cybersecurity best practices, and reflects practices outlined by the Federal Information Security Modernization Act (FISMA).

In partnership with the Bureau of Diplomatic Security (DS), the Bureau of Information Resource Management (IRM) will collaborate with Department stakeholders, technical experts, and federal partners to detect, identify, respond to, and recover from the impact of known and potential threats, evaluate the effectiveness of countermeasures, and address remaining residual risks. Through rigorous assessment methods and programs such as the federal Continuous Diagnostics and Mitigation (CDM) program, we will continue to mature our cybersecurity program to safeguard our infrastructure, networks, and applications against cyber threats and malicious activity.

In order to effectively carry out a comprehensive cybersecurity strategy, we will partner with federal agencies and industry leaders to leverage best practices to train our IT workforce. We recognize that the first line of defense in maintaining the security and integrity of the Department's networks is the ongoing education of employees about their role in identifying and preventing malicious activity. The Department will also focus on recruiting and training talent with cybersecurity expertise. Additionally, we will control user access to resources by assigning associated user rights and restrictions using the least privileges principle to protect the confidentiality, integrity, and availability of Department communications and data.

Objective 2.3 (Cloud Computing)

Drive centralized and streamlined cloud adoption to meet the business needs of the Department.

Cloud computing technologies offer the Department a platform for enabling convenient, on-demand network access to a shared pool of configurable computing resources. Cloud resources can be rapidly provisioned with minimal management effort or service provider interaction, and offer reliable, flexible, scalable access to secure cloud portfolio services. These new IT solutions will provide access to real-time collaboration tools and enable increased productivity and mobility. Simultaneously, we will enhance the Department's private cloud to address internal business requirements.

The Department's Cloud Computing Governance Board (CCGB) streamlines cloud adoption and institutes a single authority for cloud evaluations based on business needs, security risks, and efficiencies. The CCGB strives to achieve the right balance between security, agility, and transparency. The planned activities of the CCGB to mature the private and hybrid cloud environments bring the Department closer to industry standards.

Objective 2.4 (Mobility)

Improve secure mobile and remote access to appropriate Department resources.

Mobility is a top priority for the Department, as much of our relationship building and mission execution takes place outside the walls of our physical Department facilities. Our approach to enterprise mobility reflects our understanding of the people, processes, and technology required to effectively and securely manage mobile devices, their associated wireless networks, and mobile computing services and applications.

As the demand for mobile access grows, the Department will expand the number of platforms and devices supported. Through enterprise-based offerings, we will protect and secure all mobile data. Centralized configuration management and security services will continue to enhance remote access options and the user's experience. As our Department- and bureau-wide governance policies, processes, and standards for mobile application development evolve, we will enable bureaus and overseas posts to build functional applications that support the local or global mission within a secure framework.

WE'VE GOT AN APP FOR THAT

The Department is committed to pursuing Cloud First initiatives. By following standards set forth by the Department's Cloud Policy and the Cloud Computing Governance Board (CCGB), bureaus have the opportunity to develop approved cloud products and services to enhance productivity and mobility, securely. For example, the Bureaus of European and Eurasian Affairs (EUR) and International Organization Affairs (IO) Application Development Group (ADG) is a collaboration initiative to standardize application development and use at EUR and IO posts. The ADG Governance Board guides the development of applications and solutions in the cloud for the benefit of multiple EUR and IO posts. The Governance Board ensures regional applications meet policy, security, and information assurance requirements before deployment.

PERFORMANCE METRICS
Invest in core IT infrastructure at overseas posts by completing 200 Enterprise Converged Platform (ECP) installations.
Increase development, modernization, and enhancement (DME) spending by 15 percent.
Increase virtualization in data center modernization and optimization projects.
Update the enterprise architecture and segregate high value IT assets.
Complete installation of Continuous Diagnostics and Mitigation (CDM) software to enhance end-point protection.
Develop enterprise-wide identity management system (IDMS) to materially enhance the cybersecurity and utility of the Department's systems and applications across networks and databases.
Enhance and mature the Department's cybersecurity risk management initiatives.
Mature the Cloud Computing Governance Board (CCGB).
Establish standardized cloud computing contract guidance and templates.
Increase IT investments that evaluate the use of cloud computing by 30 percent.
Increase the adoption of cloud computing services by 15 percent.
Increase number of employees with a mobile device by 30 percent.

GOAL 3: ADVANCE BUSINESS MANAGEMENT PRACTICES TO TRANSFORM SERVICE DELIVERY

The Department is committed to delivering world-class IT customer services through effective business management processes and procedures and a high-caliber IT workforce. The ongoing implementation of the Federal IT Acquisition Reform Act (FITARA) will strengthen Department enterprise governance processes, and will increase the efficiency, consistency, and transparency of our business operations. We will improve the performance and security of our IT business systems through integration and modernization, and will identify enterprise solutions to reduce redundancies in core business platforms.

Through user-driven models and best practices we will deliver world-class customer- and user-friendly services and products. We will enhance our business service offering and capabilities through collaborative and cooperative partnerships within the Department. In doing so, we will transform our business model to adapt to evolving requirements in IT management and service delivery. We will capitalize on best practices that are proven, repeatable, and measurable to sustain the efficient management of our business systems and enterprise services in order to reduce redundancies in platforms and systems, automate workflows, and improve core governance and business functions.

Objective 3.1 (IT Policy and Governance)

Establish and employ streamlined policy and governance processes that align IT solutions with customer expectations and mission requirements.

Through holistic policy and governance, we align the Department's IT strategy with its business strategy to ensure our investments deliver value for the Department. Improving the management of IT activities and enabling the Chief Information Officer (CIO) to exercise proper oversight of IT programs and acquisitions, as defined by the successful implementation of FITARA, requires established processes, milestones, and review gates for capital planning, project management, and reporting for IT resources. The result will be quality service delivery, cost control of these services, and increased visibility and transparency across the Department.

The Department has a strong governance framework that meets legislative and federal mandates through its Electronic-Government (E-Gov) management of major investments, which supports FITARA objectives in areas such as reviewing plans, execution, acquisition management, human resources management, and expenditures as part of the Department's Capital Planning and Investment Control (CPIC) program. Through the E-Gov boards, the CIO works in partnership with the Bureau of Budget and Planning (BP), the Comptroller, Chief Acquisition Officer (CAO), and other stakeholders to establish policies and procedures that ensure the accountability that IT assets are designed, developed, and maintained effectively. The Department's E-Gov board structure, combined with the implementation of FITARA, will ensure IT resources are allocated in accordance with our IT strategic direction and evolving priorities.

Objective 3.2 (IT Human Capital Management)

Build, develop, and retain a talented, diverse IT workforce.

Critical to the success of our business management approach is a workforce-planning model that attracts, engages, and retains a highly skilled IT workforce. The Department faces the constant challenge to recruit and retain high-caliber IT professionals whose skills reflect current technology. To address this challenge, the Department will continue to seek the best-qualified candidates, promote career goals across the IT workforce, offer skills incentive pay, and provide appropriate training to nurture the talent required to deliver tomorrow's technology.

Effective human capital planning identifies essential and specific core competencies. In support of our human capital goals, the Department is creating a centralized IT workforce database to assess staffing needs and future trends for IT positions. The database will be a comprehensive effort that accounts for enterprise-wide, regional, and mission requirements. The Department will continue to implement competency-based workforce recruiting, and will develop strategies to maintain a pipeline of diverse and highly qualified IT candidates for both domestic and overseas staffing.

Building and sustaining a workforce with a relevant IT skillset to meet the needs of our customers requires an investment in ongoing training. The Department will expand its training programs to give experienced workers the opportunities to learn new skills, while reaching out to a new generation of workers with training and educational opportunities that pave the way to a fulfilling career at the Department.

Objective 3.3 (IT Service Delivery)

Improve end-to-end transparency and accountability between the customer and service provider.

Our customers expect an engaging, user-friendly online experience. Providing quality customer service and exceptional service delivery is crucial to accomplishing our mission. The Department will continue to implement customer-centric and service-management approaches to smarter IT delivery. This will result in cost-effective enterprise solutions that reduce costs, streamline development, and provide employees access to information and information services.

REDEFINING SERVICE

ConsularOne is the Bureau of Consular Affairs' (CA) modernization initiative. ConsularOne will modernize, consolidate, and/or replace functionality currently delivered by more than 90 discrete systems. It will provide CA employees easier access to data through a single interface, greatly reducing the need to log into separate systems to obtain data. ConsularOne will also provide CA with the opportunity to take an in-depth look at existing business processes, with the goal of improving efficiency, security, and consistency across consular services.

Paramount to good service delivery is customer service. We will continue to nurture relationships and foster communications between customers and providers that improve awareness about IT services, requirements, capabilities, and service levels. This includes increasing customer access to information through catalogs, searches, and forms via mobile and desktop platforms. In doing so, we will continue to raise the bar on customer service satisfaction both in-person and online.

Objective 3.4 (IT Business Systems)

Ensure efficient and effective performance of core business functions and enterprise services.

The Department's next generation of modern core business and management systems will deliver more accurate, complete, and integrated information for analysis and decision-making. Modernized IT business systems will address management information requirements to reduce redundancies, enhance workflows, and improve business functions. Well-designed and well-developed system interfaces will enable reliable connections between systems and improve interoperability. Additionally, in serving our employees and an aging public that includes more individuals with disabilities, it is imperative that the Department provide equal access to information and data. The Department is committed to compliance with Section 508 of the Rehabilitation Act that requires all website content be accessible to people with disabilities. Our Section 508 Program ensures that Electronic and Information Technology (EIT) is usable and accessible in order to meet our customers' needs. By focusing on IT standards and including accessibility requirements in our IT systems requirements, IT management decisions, and our mission, we ensure that the needs of all end-users are properly considered.

The evolving IT environment is redefining how applications are designed and delivered. Enterprise applications continue to optimize digital content and messaging for accessible platform-agnostic delivery to key audiences. Enterprise capabilities, such as a shared pre-production environment, will improve collaboration and communication between Department stakeholders and developers during application creation and deployment. It will also reduce the time, and streamline resources required, to complete application lifecycle.

PERFORMANCE METRICS
Improve integration of various governance bodies across the Department.
Refine the Department's Capital Planning and Investment Control (CPIC) Pre-Select implementation process.
Develop a baseline IT Workforce Database to assess staffing needs, current statistics, and future trends for IT positions.
Identify Foreign Service (FS) competencies that need to be addressed in new training requirements. Suggest new training requirements for IT professionals as appropriate.
Increase percentage of employees who enroll in IT training opportunities.
Increase IT project managers with the Federal Acquisition Certification for Program and Project Managers (FAC-P/PM) by 15 percent.
Improve customer service satisfaction rating based on quality of service survey.
Increase software development projects using Agile by 25 percent.
Implement a centralized, automated enterprise service management solution to manage requests for services and increase transparency.
Enhance workforce skills to support an environment where Section 508 accessibility requirements are understood, communicated, implemented, and enforced across the enterprise.

PERFORMANCE METRICS

GOAL 1 (Innovative Diplomacy)
Define and implement standard policies, procedures, formats, and tools for managing all permanent electronic records electronically by December 2019.
Adopt new information technologies to improve business and IT operations.
Increase number of datasets registered in the enterprise data catalog to reduce data redundancies.
Apply data policies and associated standards from the Master Reference Data platform to support data integrity.
Establish a research and development (R&D) function and customer requirements office for IT solutions.
Increase the use of data analytics tools to inform policy and business decisions.
GOAL 2 (Global IT Infrastructure)
Invest in core IT infrastructure at overseas posts by completing 200 Enterprise Converged Platform (ECP) installations.
Increase development, modernization, and enhancement (DME) spending by 15 percent.
Increase virtualization in data center modernization and optimization projects.
Update the enterprise architecture and segregate high value IT assets.
Complete installation of Continuous Diagnostics and Mitigation (CDM) software to enhance end-point protection.
Develop enterprise-wide identity management system (IDMS) to materially enhance the cybersecurity and utility of the Department's systems and applications across networks and databases.
Enhance and mature the Department's cybersecurity risk management initiatives.
Mature the Cloud Computing Governance Board (CCGB).
Establish standardized cloud computing contract guidance and templates.
Increase IT investments that evaluate the use of cloud computing by 30 percent.
Increase the adoption of cloud computing services by 15 percent.
Increase number of employees with a mobile device by 30 percent.
GOAL 3 (IT Business Management)
Improve integration of various governance bodies across the Department.
Refine the Department's Capital Planning and Investment Control (CPIC) Pre-Select implementation process.
Develop a baseline IT Workforce Database to assess staffing needs, current statistics, and future trends for IT positions.
Identify Foreign Service (FS) competencies that need to be addressed in new training requirements. Suggest new training requirements for IT professionals as appropriate.
Increase percentage of employees who enroll in IT training opportunities.
Increase IT project managers with the Federal Acquisition Certification for Program and Project Managers (FAC-P/PM) by 15 percent.
Improve customer service satisfaction rating based on quality of service survey.
Increase software development projects using Agile by 25 percent.
Implement a centralized, automated enterprise service management solution to manage requests for services and increase transparency.
Enhance workforce skills to support an environment where Section 508 accessibility requirements are understood, communicated, implemented, and enforced across the enterprise.

IT GOVERNANCE STRUCTURE

The Department established an overall IT governance process and an internal management structure that supports the achievement of the plan's three strategic goals. IT management policies and practices will continue to evolve and improve the effectiveness of IT management.

Structure of IT Governance Boards

The E-Government Program Board (E-GovPB) provides overall oversight and resourcing for the enterprise IT activities. Program Board members include Assistant Secretaries. The objectives of the board are to: set the Department's IT strategic direction; evaluate IT programs and investments; drive innovation through IT capital decisions; and prioritize strategic and resource issues related to IT investments and initiatives. The Department relies on the E-GovPB to promote collaboration with the bureaus and posts, to review strategic goals and performance measures, and to ensure all IT activities remain focused on agreed-upon goals and priorities.

The E-Government Advisory Board (E-GovAB) supports the E-GovPB by identifying issues for the E-GovPB to review, providing assessments and recommendations on the Department's IT initiatives ensuring they align with IT policies, architecture, standards, and goals, and determining strategies, policies, and timelines required to implement the directives of the E-GovPB. The E-GovAB is informed by other governance structures, such as the CCGB, and supported by the E-Gov Program Management Office. Through the E-GovPB and E-GovAB, the CIO works in partnership with BP, the Comptroller, the CAO, and other executive stakeholders to establish policies and procedures that ensure the accountability that IT assets are designed, developed and maintained effectively.

IT Budget Review

The IT governance process is aligned closely with IT Capital Planning. With the implementation of FITARA, IRM and BP will partner to ensure the CIO reviews IT budget resources throughout the funding lifecycle. In collaboration with BP, IRM reviews requested budgets for IT categories, regardless of budget account, for alignment with established IT goals, architectures, priorities, efficiencies, and performance. Through the E-GovPB, the CIO, Director of BP, Chief Financial Officer (CFO), and Comptroller will continue to participate in budget development governance, guiding and performing oversight of enterprise and federal requirements and initiatives.

Chief Information Officer Roles and Responsibilities

The CIO is equivalent to an Assistant Secretary, and manages IRM, providing IT infrastructure and services the Department needs to achieve its foreign policy mission. The CIO leverages the E-GovPB, consisting of senior leaders across the C-suite, manages investments in accordance with applicable Office of Management and Budget circulars through an enterprise CPIC program, and leverages Enterprise Architecture to integrate business requirements. The CIO has full visibility into planning and budgeting, acquisition, program and project management, expenditures, and human capital aspects of IT resources.

Chief Information Security Officer Roles and Responsibilities

The CISO operates under the direction and supervision of the CIO and is the CIO's primary advisor concerning Department information security issues. The CISO is responsible for defining and evaluating the information security posture of the Department's information and information systems and ensures agency compliance with FISMA and other federal mandates and requirements.

ACRONYMS

ADG	Application Development Group
BP	Bureau of Budget and Planning
CA	Bureau of Consular Affairs
CAO	Chief Acquisition Officer
CCGB	Cloud Computing Governance Board
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPIC	Capital Planning and Investment Control
DME	Development, Modernization, and Enhancement
DS	Bureau of Diplomatic Security
ECP	Enterprise Converged Platform
E-Gov	Electronic Government
E-GovAB	E-Government Advisory Board
E-GovPB	E-Government Program Board
EIT	Electronic and Information Technology
EUR	Bureau of European and Eurasian Affairs
FAC-P/PM	Federal Acquisition Certification for Program and Project Managers
FISMA	Federal Information Security Modernization Act
FITARA	Federal IT Acquisition Reform Act
FS	Foreign Service
FSI	Foreign Service Institute
IDMS	Identity Management System
IO	Bureau of International Organization Affairs
IRM	Bureau of Information Resource Management
IT	Information Technology
ITSP	Information Technology Strategic Plan
JSP	Department of State and USAID Joint Strategic Plan
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
QDDR	Quadrennial Diplomacy and Development Review
R&D	Research and Development
SAIT	School of Applied Information Technology
U.S.	United States
USAID	United States Agency for International Development

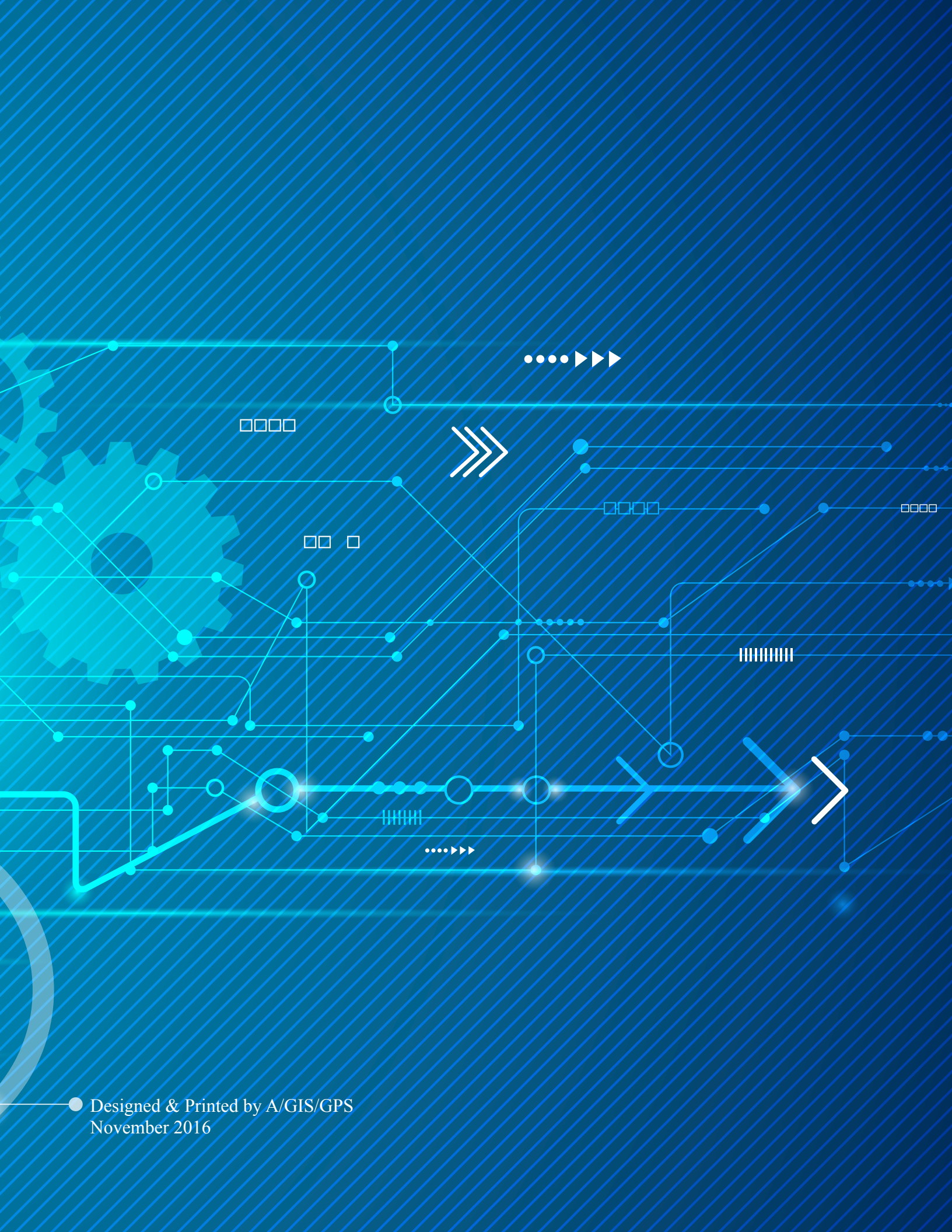
ACKNOWLEDGMENTS

This *Department of State Information Technology Strategic Plan* is the culmination of more than a year of collaborative work that could not have been completed without the concerted effort of many people.

The **E-Government Advisory Board** was involved early in the process and set the technical direction of the plan, and the **E-Government Program Board** served in an advisory role. The contributions of these boards were integral to the development of this plan.

Special thanks go to the following:

- *Robert Adams*, Acting, Principal Deputy Chief Information Officer (PDCIO); *Al Bowden*, Information Assurance DCIO; *Michael Bretz*, Acting, Foreign Operations DCIO; *Glen Johnson*, Operations DCIO; and *Minh-Hai Tran Lam*, Acting, Business Management and Planning DCIO, and Director, Strategic Planning Office, who provided technical guidance, sound advice, and unfailing enthusiasm.
- The Strategic Planning Office, Strategic Planning Division, made up of *Julie Detter, Carrie Fox-Myers, Chris House, Don Hunter, and Mary Yoshioka*, that completed the writing of this plan as well as the research that lies behind it.
- Interviewees from bureaus, offices, and posts across the Department of State who contributed their knowledge and expertise to this plan.
- The many others who reviewed drafts, answered questions, made suggestions, and filled in gaps.



Designed & Printed by A/GIS/GPS
November 2016