

Information Technology Strategic Plan (ITSP)

Fiscal Year: 2024-2026



“First, we go back to this proposition that we’re in a moment of intense competition to shape what comes next. Technology, innovation, entrepreneurship – they are at the heart of that. This is how we are going to retool economies for the future. This is, through technology, how we are quite literally reshaping people’s lives.” – Secretary Antony Blinken

Table of Contents

| | |
|-----------------------|----|
| A Letter from the CIO | 3 |
| Introduction | 4 |
| Mission & Vision | 5 |
| Goals & Objectives | 6 |
| Goal 1 | 7 |
| Goal 2 | 9 |
| Goal 3 | 11 |
| Goal 4 | 13 |

Information Technology Strategic Plan

Emerging technologies and digitization are driving both opportunities and challenges for our global diplomatic mission. Capitalizing on these opportunities requires modernization and making systems more secure, usable, and mobile. We must also ensure that we use our IT resources efficiently and effectively, including our greatest resource: our IT workforce.



Recently, the Department adopted a modern approach to IT to empower users to meet our mission. We have already begun to employ agile development methods, deploy cloud technologies, strengthen our cybersecurity, and use data in strategic decision-making. We have responded to the changing needs of our workforce by providing reliable and secure remote access to enterprise data, systems, and equipment, in addition to equipping users with advanced collaboration tools. But there is still more work to do.

To build on the great work we have already accomplished, I am pleased to share the Department of State's Information Technology Strategic Plan (ITSP) for Fiscal Years 2024-2026. The ITSP focuses on driving innovation with four goals:

1. Enhance Cybersecurity – Secure diplomacy by protecting the Department's data against the growing threat.
2. Enable Modernization – Deliver modern, secure, integrated solutions that enable the diplomatic mission both domestically and overseas and enhance the user experience.
3. Expand Governance – Increase collaboration and enterprise-wide approaches across the Department.
4. Workforce Excellence – Hire and retain a talented and diverse IT workforce supported by continued learning.

I look forward to collaborating across the State Department and with other agencies, our industry partners, and the public to achieve the goals that will drive diplomacy with technology.

A handwritten signature in black ink, reading "Kelly E. Fletcher". The signature is fluid and cursive, with a long horizontal line extending to the right.

Dr. Kelly E. Fletcher

Chief Information Officer, U.S.
Department of State

Introduction

The Department of State has the unique mission of promoting security, prosperity, and democracy across the world. With bureau, office, and post locations in over 190 countries, the Department's 100,000+ users must access IT systems, services, and data securely and reliably.

IT has shaped the way the Department operates. It is a key enabler for increased productivity, efficiency, and user communications across the globe. IT is also used to secure and enhance the resiliency of Department data, protecting the enterprise from growing threats and providing uninterrupted service. As IT technologies evolve, the Department will continue to embrace new systems and tools to best support the workforce.

The Department of State Information Technology Strategic Plan (ITSP) for Fiscal Years (FY) 2024-2026 is a three-year strategy that describes the agency's technology and information resource goals, objectives, and priorities that support the Department's diplomatic mission. [Office of Management and Budget \(OMB\) Circular A-130](#) requires publication of an ITSP that describes how the Department's information and technology resources support its mission, and the [Government Performance and Results Modernization Act of 2010 \(GPRM\)](#) requires the ITSP to align with the [Department of State United States Agency for International Development \(USAID\) Joint Strategic Plan \(JSP\)](#) and the [President's Management Agenda](#). The ITSP also aligns with the [National Cybersecurity Strategic Plan](#) and [National Security Strategy](#).

The Department is modernizing the way it manages and delivers IT services. As emerging technologies and new tools are deployed, the Department will adhere to these goals by implementing best practices across the enterprise, updating and automating IT service and system management processes, and maintaining an environment of continuous monitoring and improvement. A continued customer-centric focus is essential to understanding user needs and delivering high-quality services that are critical to our mission.

The FY 2024-2026 ITSP establishes four critical, high-level IT goals: enhance cybersecurity, enable modernization, expand governance, and workforce excellence. These goals drive toward a Department with secure, accessible data and modern systems and devices that are governed efficiently and fueled and maintained by a talented, diverse workforce. Achieving these goals will enable the Department to:

- Better prepare for and defend against cyber threats.
- Equip users with modern tools and technologies they need while improving customer service.
- Enhance information sharing and mobility through deployment of enterprise services.
- Support the career progression and continued learning for the IT workforce

Department of State Mission

To protect and promote U.S. security, prosperity, and democratic values and shape an international environment in which all Americans can thrive.

IT Mission & Vision

Mission: Deliver world-class, global, secure IT that supports the Department's mission and workforce.

Vision: A secure, modern, accessible, and reliable IT environment that empowers diplomacy, collaboration, and analytics across the Department and with our external stakeholders.

Guiding Principles

- Ensuring **resiliency and security** of Department data.
- Providing **excellent customer service**.
- Promoting **innovation** and adoption of emerging technologies.
- Relying on **evidence-driven decisions** to promote effectiveness and efficiency.
- Driving the **use of Department data** to inform decisions.
- Fostering **workforce talent and diversity** across the Department.

Goals and Objectives

1

ENHANCE CYBERSECURITY

Secure diplomacy by protecting the Department's data against the growing threat.

OBJECTIVES

- 1.1 Modernize cyber defense.
- 1.2 Rapidly meet cybersecurity requirements with end-to-end visibility.
- 1.3 Implement mission-effective risk management through continuous monitoring.

2

ENABLE MODERNIZATION

Deliver modern, secure, integrated solutions that enable the diplomatic mission both domestically and overseas and enhance user experience.

OBJECTIVES

- 2.1 Modernize legacy networks and systems and improve user experience.
- 2.2 Leverage shared secure solutions.
- 2.3 Improve business intelligence and automation.

3

EXPAND GOVERNANCE

Increase collaboration and enterprise-wide approaches across the Department.

OBJECTIVES

- 3.1 Modernize policies and processes.
- 3.2 Streamline adoption of new technology.
- 3.3 Enable economies of scale.

4

WORKFORCE EXCELLENCE

Hire and retain a talented and diverse IT workforce supported by continued learning.

OBJECTIVES

- 4.1 Identify, attract, hire, and support a talented and diverse IT workforce.
- 4.2 Promote employee learning and development.

Goal 1: Enhance Cybersecurity

Secure diplomacy by protecting the Department’s data against the growing threat. (JSP Goals 1.4.2, 4.3.1, 4.3.2)

Imperative

The Department must continuously address evolving cyber threats to the diplomatic mission.

Solution

Rapidly implement cybersecurity defenses and modernize the security environment.

1

1.1 MODERNIZE CYBER DEFENSE

Adhere to federal cybersecurity strategies and guiding principles, including those related to adoption of a Zero Trust Architecture (ZTA).

GUIDING PRIORITIES

1. Ensure alignment to: (a) Executive Order 14028: Improving the Nation's Cybersecurity (b) National Security Memorandum/NSM-8: Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems; (c) The federal ZTA Strategy.
2. Enable consistent alignment and adoption by providing enterprise cybersecurity services.

2

1.2 RAPIDLY MEET CYBERSECURITY REQUIREMENTS WITH END-TO-END VISIBILITY.

Deploy emerging technologies and tools that provide end-to-end visibility across the Department.

GUIDING PRIORITIES


1. Centralize visibility of all assets and users on the Department’s networks.
2. Implement an enterprise asset and centralized user management solution.
3. Proactively respond to cyber directives, notices, and alerts.

3

1.3 IMPLEMENT MISSION-EFFECTIVE RISK MANAGEMENT THROUGH CONTINUOUS MONITORING.

GUIDING PRIORITIES

1. Evolve the Authorization to Operate (ATO) process and implement ongoing authorization.



Enable automated, continuous monitoring using technology to collect, analyze, and respond to cyber threats and vulnerabilities across the Department.

2. Ensure real-time reporting 24x7.
3. Reduce the number of end-of-life hardware and software instances on Department networks.
4. Secure IT management and acquisition including through effective supply chain risk management.
5. Expand education regarding ATOs, cybersecurity risks, and risk management techniques.

Goal 2: Enable Modernization

Deliver modern, secure, integrated solutions that enable the diplomatic mission both domestically and overseas and enhance the user experience. (JSP Goal 4.2.3)

Imperative

The Department must ensure access to modern IT to meet mission requirements and improve user experience.

Solution

Implement innovative technologies that enhance user experience, connectivity, and productivity.

1

2.1 MODERNIZE LEGACY NETWORKS AND SYSTEMS AND IMPROVE USER EXPERIENCE

Modernize IT networks, systems, and services to support the mission and improve user experience.

GUIDING PRIORITIES

1. Decrease network latency and ensure robust, resilient communication pathways, including voice and data.
2. Replace or modernize legacy solutions at or prior to end-of-life date.
3. Evaluate diverse user needs, and provide technology solutions that are intuitive, easy to use, and accessible to people of all abilities.

2

2.2 LEVERAGE SHARED SECURE SOLUTIONS

Establish an enterprise-level secure multi-cloud environment to effectively meet user needs and expand access and information sharing across the Department.

GUIDING PRIORITIES


1. Leverage and continue to implement enterprise cloud solutions to enable consistent access to systems across different locations.
2. Increase mobility of and access to Department systems and services, including through expanded access to mobile devices, enhanced system compatibility with mobile devices, and an expanded Wi-Fi footprint.

3

2.3 IMPROVE BUSINESS INTELLIGENCE AND AUTOMATION

GUIDING PRIORITIES

1. Implement analytics and visualization capabilities to enhance data-based decision-making.



Leverage emerging technologies to streamline and automate business processes.

2. Determine best practices for leveraging robotic process automation (RPA), AI, virtual reality (VR), and other emerging technologies to support Department missions.

Goal 3: Expand Governance

Increase collaboration and enterprise-wide approaches across the Department. (JSP Goal 4.2.3)

Imperative

The Department must effectively and efficiently govern IT systems and platforms.



Solution

Implement and strengthen Department-wide policy, oversight, and governance to increase interoperability and improve user experience.

1

3.1 MODERNIZE POLICES AND PROCESSES

Establish and communicate consistent policies on interoperability and user experience.

GUIDING PRIORITIES

1. Leverage the community of IT and cyber professionals to implement consistent policies and processes.
2. Develop and issue standards for interoperability and user experience, and measure implementation of services and technologies against these standards.

2

3.2 STREAMLINE ADOPTION OF NEW TECHNOLOGY

Streamline processes and improve IT solution development and delivery.

GUIDING PRIORITIES

1. Develop best practices, trainings, and resources to assist with implementation of agile concepts.
2. Develop and implement change management strategies to support agile IT service delivery and adoption.
3. Conduct regular market research to stay informed of new tools and emerging technologies users need to meet their business requirements.
4. Provision enterprise platforms that enable new capabilities to address evolving user needs.

3.3 ENABLE ECONOMIES OF SCALE

Standardize IT acquisitions to effectively manage resources and eliminate redundancies.

5. Streamline the system development lifecycle process to allow for rapid deployment of technology and improve owners' ability to achieve ATOs.

GUIDING PRIORITIES

1. Enhance transparency of IT contracts.
2. Coordinate market research to identify enterprise-wide IT and cyber contracts.
3. Provision enterprise-wide IT and cybersecurity contracts.

Goal 4: Workforce Excellence

Hire and retain a talented and diverse IT workforce supported by continued learning. (JSP Goals 4.1.2, 4.1.3)

Imperative

The Department must hire and retain a talented and diverse IT workforce.

Solution

Enhance recruiting and retention while promoting employee learning.

1

4.1 IDENTIFY, ATTRACT, HIRE, AND SUPPORT A TALENTED AND DIVERSE IT WORKFORCE

Identify and fill skill gaps while fostering growth, diversity, equity, inclusion, and accessibility.

GUIDING PRIORITIES

1. Increase recruiting efforts Department-wide for IT and cybersecurity positions.
2. Improve recruiting and retention tools and processes.
3. Embed DEIA in hiring and employment practices.
4. Plan and budget for proper staffing levels, in appropriate skill codes, to conduct the work.


2

4.2 PROMOTE EMPLOYEE LEARNING

Establish programs and initiatives that support employee professional development and training.

GUIDING PRIORITIES

1. Identify skill gaps and desired training curricula.
2. Incentivize continuous learning and achievement.
3. Upskill the IT and cyber workforce to keep pace with technology enhancements.
4. Assess the workforce on a recurring basis and provide tools that support career progression.
5. Leverage the NICE Framework, which describes the tasks, knowledge, and skills needed to perform cybersecurity work.

- 
6. Promote opportunities for Foreign Service and Civil Service positions to address gaps in their own experiences or expertise.