INFORMATION RESOURCES MANAGEMENT (IRM) STRATEGIC PLAN with OPEN DATA PLAN

SELECTIVE SERVICE SYSTEM
JULY 2025

MESSAGE FROM THE DIRECTOR

The Selective Service System's (SSS) Information Resource Management (IRM) Strategic Plan reflects the Agency's commitment to optimize and maintain its IT infrastructure. The plan identifies areas for IT efficiency and innovation, as well as how best to invest in the workforce. This plan directly supports the Agency's strategic plan and reflects the Agency's mission to be prepared to provide untrained manpower to the military in the event the country returns to a military draft.

SSS is nearing the completion of a critical modernization effort involving the migration of its Registration Compliance and Verification (RCV) system — a designated High-Value Asset (HVA) from an on-premises environment to a FedRAMP Moderate-compliant cloud service provider. This IRM Strategic Plan was developed by the Office of Information Technology in conjunction with the Acting Chief Information Officer, the Acting Deputy Chief Information Officer, the Chief Information Security Officer, the Chief Data Officer, and other IT specialists. These collective efforts across the Agency provide the means for ongoing IT transformation. This framework builds on best practices and follows the Agency's recently revised Enterprise Architecture plan.

Managing IT is a demanding business. Data and cybersecurity management, reliable service, application of artificial-intelligence technologies to automate, enhance, and transform various IT processes and operations, and lifecycle management are but a few of the factors that need to be managed successfully to facilitate mission readiness. SSS takes its job seriously, and the staff is dedicated to the Agency's mission.

The IT staff work across the Agency to provide current IT solutions that meet security requirements and fulfill mission requirements. SSS is committed to taking the next steps in development, maintenance, and enhancement of the network to support the Agency's mission and to provide for the country's defense.

Jeffrey Steinlage

Digitally signed by Jeffrey Steinlage
Date: 2025.09.05 11:40:22 -04'00'

Jeffrey Steinlage

Acting Chief Information Officer

EXECUTIVE SUMMARY

The Selective Service System (SSS), part of the U.S. executive branch, is responsible for mobilizing manpower during national emergencies. By law, men aged 18–26 must register, or risk losing access to federal and state benefits and facing delays in naturalization. SSS maintains a system to quickly meet national, and Department of Defense (DoD) needs when authorized by Congress and the President.

The following is a short list of activities that directly support the Agency's strategic plan to be prepared to provide unskilled manpower to the DOD:

- **Online registration and verification**. A young man may meet his registration obligation by registering online at https://www.sss.gov/register/ within 30 days of his 18th birthday. The registration page also provides online registration verification for those who need to confirm their eligibility for benefits tied to the registration requirement.

- **Online information**. The Agency's website at Selective Service System, provides information to the public regarding SSS and the requirement to register, along with other information concerning the military draft and its history.

- **Ensuring registration compliance.** SSS works to identify young men who haven't registered, as part of its compliance program. Reminder notices are sent to encourage registration before age 26—after which individuals become permanently ineligible for key federal and state benefits. The goal is **compliance, not prosecution**. Encouraging timely registration helps individuals retain access to life-enhancing opportunities and ensures fairness if a draft is ever reinstated.

Accomplishing these plans is dependent upon:

- availability of funding.
- IT security requirements.
- availability of IT resources needed to support daily operations and projects.
- life-cycle management that follows accepted IT project-management practices.
- considerable planning.

This IRM Strategic Plan aligns with the SSS Strategic Plan for Fiscal Years 2024–2026, and follows the guidance of Office of Management and Budget (OMB) Circular A-130 for managing Federal information resources. It outlines the Agency's approach to enterprise architecture, cybersecurity, FISMA compliance, and data governance.

In FY 2025,SSS advanced its national defense mission by strengthening its **secure, modern IT infrastructure**. Key initiatives included: successful RCV cloud migration under Technology Modernization Fund (TMF-1) and deployment of AI-driven tools to automate reporting, streamline workflows, and boost efficiency.

To enhance compliance and data protection, SSS: began tagging Controlled Unclassified Information (CUI) using Microsoft Purview; adopted Zero Trust Architecture (ZTA) to improve access control and reduce risk; and continued regular reviews of System of Records Notices (SORNs) and Privacy Impact Assessment (PIAs)/

SSS ensures transparency and accountability by tracking measurable outcomes—such as ZTA milestones, CUI tagging rates, and registration compliance metrics-enabling data data-driven oversight and continuous improvement.

FISMA

SSS undergoes an annual FISMA audit to identify security weaknesses. The IT department strives to resolve security issues quickly, and this annual audit is one of the best tools to identify potential vulnerabilities. FISMA audits typically run from May through September, and preliminary findings are usually available in August, allowing time for IT to mitigate vulnerabilities quickly.

As of June 2025, the current FISMA audit is underway. FISMA metrics from previous years have been uploaded to Cyberscope. In 2024, the agency earned an "Effective" rating, with a maturity score of 4.5. In 2023, the Agency earned an "Effective" rating with a maturity score of 4.1.

The Agency has two in-progress findings from previous years: one, the need for a redundant information-processing site; and two, the need to strengthen processes and procedures related to counterfeit information resources.

Annual Assurance Memoranda

The IT directorate also has self-assurance checklists to follow regarding network security and operational maintenance. An annual assurance memorandum, which is due to the Director in August and signed by the CIO, is required to certify that IT follows these checklists.

Federal Information Technology Acquisition Reform Act

The Federal Information Technology Acquisition Reform Act (FITARA), passed by Congress in December 2014, marked the first significant reform of Federal information-technology acquisition in nearly two decades. In response, SSS is actively working to streamline its IT procurement processes to enhance efficiency and compliance. This initiative supports key FITARA mandates, including the adoption of cloud-based computing solutions, the enhancement of training programs for IT personnel, and improved management of IT budgets. These efforts collectively position SSS to modernize its IT infrastructure, optimize resource allocation, and meet evolving technological and operational demands.

Continuity of Operations (COOP)

Under Phase One of the agency's IT infrastructure update plan, the Agency is planning a new COOP site to meet all requirements related to disaster recovery and emergency relocation. The refactoring of RCV to the cloud will support this objective. This effort is funded by the Technology Modernization Fund (TMF) project.

The Agency is also addressing high-availability requirements during the current infrastructure update and the contract migration from NetWorx to EIS. The SSS network is highly virtualized, and this environment provides high-availability support needed to ensure that the Agency remains capable of meeting its primary mission of supplying manpower to the DOD.

Selective Service System IT Goals

To support the SSS Strategic Plan for Fiscal Years 2024–2026 and advance mission readiness, the agency's IT leaders have established the following key goals:

1. Modernize and refresh the network infrastructure to ensure operational resilience and scalability.
2. Identify and implement opportunities to improve IT efficiency and service delivery.
3. Strengthen network security posture and maintain configuration-management compliance.
4. Optimize the management of human and capital resources to support IT mission success.
5. Maintain a high state of system readiness to enable rapid scalability during mobilization.

Goal 1: Modernize and refresh the network infrastructure to ensure operational resilience and scalability.

This goal completes the ongoing network lifecycle refresh to replace such aging equipment as servers, routers, and switches. It also involves strengthening the Agency's foundational IT infrastructure to support increased demand, enhancing system performance, and reducing system downtime. Modernization efforts will enable SSS to

deliver reliable services to internal and external stakeholders, while ensuring rapid scalability to meet surge requirements during mobilization. This goal directly supports Strategic Objective 1.4 by ensuring that technology infrastructure is robust and ready for the future.

Goal 2: Identify and implement opportunities to improve IT efficiency and service delivery.

This goal involves continuously assessing and optimizing IT processes to enhance efficiency, reduce operational costs, and improve customer experience. It also involves implementing data-driven decision-making and adopting modern methodologies, such as DevSecOps, to accelerate deployment cycles and improve software quality. SSS also seeks to promote a culture of innovation and continuous improvement, thus aligning IT service delivery with evolving mission needs and Agency priorities. This goal advances Strategic Objectives 3.1 and 3.2 by encouraging excellent customer experience and effective resource management.

Goal 3: Strengthen network security posture and maintain configuration-management compliance.

This goal implements and enforces strong cybersecurity measures to protect systems and sensitive data against emerging threats. It also involves aligning security practices with Federal mandates and Zero Trust Architecture principles, including continuous monitoring, multifactor authentication, and strict access controls. Maintain comprehensive configuration management to ensure that systems are consistently compliant, and vulnerabilities are rapidly addressed. This goal supports Strategic Objective 3.5 by proactively managing risks to information systems and maintaining operational readiness.

Goal 4: Optimize the management of human and capital resources to support IT mission success.

This goal enhances workforce planning, training, and resource allocation to ensure that IT personnel are well-prepared and equipped to meet mission demands. It also aims to improve financial stewardship of IT investments by ensuring that expenditures align with strategic priorities and deliver measurable value. In addition, it seeks to foster interdepartmental collaboration and to strengthen partnerships to maximize resource effectiveness and organizational resilience. This goal aligns with Strategic Objectives 3.2 and 3.7 by emphasizing efficient resource management and professional development**.**

Goal 5: Maintain a high state of system readiness to enable rapid scalability during mobilization.

This goal ensures that all IT systems are continuously mission-capable by means of rigorous testing, proactive maintenance, and ongoing validation exercises. Develop and maintain contingency plans, conduct regular drills, and implement robust monitoring to

guarantee that systems can scale rapidly and support critical operations in a mobilization scenario. Reinforce system resilience to support the Agency's ability to deliver manpower to DOD within the required M+193 timeline. This goal supports Strategic Objectives 1.1 and 1.2 by prioritizing operational preparedness and readiness.

CIO Authority

The CIO of SSS is responsible for ensuring that the Agency remains at the forefront of technology. The CIO also supports enterprise-wide mission readiness, modernization, and plays a critical role in advancing organizational strategic goals by delivering secure, efficient, and forward-leaning IT capabilities.

In today's environment — where agencies are expected to do more with fewer resources — strong IT governance and disciplined management are essential. The CIO is accountable for the effective oversight of the IT Directorate's budget, infrastructure, software assets, and workforce. This oversight includes ensuring that daily operations, IT system development, and project execution are tightly aligned with mission needs and Federal standards.

The CIO's authority is derived from Agency directives, Federal mandates, standard operating procedures, and enterprise IT policies. Given the rapidly evolving nature of Federal IT requirements, the CIO relies on such tools as the Agency's IT tasking database to track and manage ongoing initiatives and priorities.

In support of the SSS mission, the CIO is charged with leading and safeguarding the following key areas:

- IT governance.
- IT program and service management.
- cybersecurity and information assurance.
- enterprise architecture and systems integration.
- IT acquisition and vendor management.
- regulatory and security compliance oversight.

Cybersecurity Management

SSS's security plan addresses cybersecurity priorities by establishing objectives and target outcomes to meet security mandates and ensure that the data with which the Agency is entrusted remains secure.

Objective: Identify, prioritize, and mitigate risk to SSS IT assets. SSS will:

- implement and execute appropriate security practices to ensure protection of the agency's data while striving for efficiency.
- ensure that security practices are integrated into all IT processes.
- ensure that security IT equipment remains current and operational.

- ensure that shared security services are implemented appropriately with participating Federal agencies.

SSS will judge the effectiveness of its cybersecurity efforts by:

- monitoring security attacks and breaches.
- becoming compliant with all FISMA requirements.
- monitoring for insider threat activity.
- ensuring that security issues are addressed quickly.
- ensuring that the CIO is kept regularly apprised of security matters.

The SSS monitors incidents on an ongoing basis. Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal and Information Systems*, along with various OMB memoranda, specify security requirements for all Federal agencies. The Agency is subject to these requirements and is evaluated during each annual FISMA audit.

The Agency also operates a configuration change board, which is responsible for evaluating proposed network system changes before implementation. This board has authority to deny changes that might negatively affect information security, and serves to ensure operational stability, proper security management, and configuration control management.

Managing Information as a Strategic Asset

In conjunction with training employees in compliance, security, and ethical data usage so as to ensure responsible data handling, the SSS will implement initiatives to manage information as a strategic asset by:

- implementing high-availability architectures (e.g., distributed databases, failover mechanisms) to ensure uninterrupted access to critical data.
- maintaining data accuracy and consistency through automated validation, version control, and governance framework.
- implementing user-friendly data tools and dashboards that allow employees to access, interpret, and utilize data independently.
- applying Zero Trust Architecture principles, encryption, and role-based access controls to prevent unauthorized access, and by tagging CUI data to prevent leakage.
- using cloud-based and hybrid solutions that can dynamically scale to meet sudden operational needs.
- analyzing demographics, behaviors, and registration patterns to pinpoint high-risk areas and optimize outreach efforts.
- using data insights to tailor compliance programs, personalized reminders, and process improvements to drive higher registration rates.
- ensuring clean, standardized, and well-governed data across all registration sources for accurate analysis.

- using machine learning, predictive analytics, and trend analysis to identify compliance risks and opportunities.

Shared Services

SSS continues to evaluate shared services as a strategic solution to meet IT requirements, improve efficiency, and reduce operational costs. While this initiative requires careful research, planning, and coordination, shared services present significant potential benefits for the Agency. SSS completed an initial evaluation and has since identified opportunities to leverage federal shared services for functions such as identity management, cloud hosting, and cybersecurity support. As of FY25, efforts to explore and integrate shared services are ongoing, with further analysis and phased implementation planned to align with modernization goals.

Section 508 Compliance

The agency is dedicated to ensuring that all IT purchases and services comply with Section 508 accessibility standards. Oversight of compliance is the responsibility of the CIO and his/her staff, who research and apply the necessary standards. The IT Directorate maintains comprehensive documentation to demonstrate that all acquired systems, public-facing websites, and internal IT platforms used by SSS and the public meet Section 508 accessibility guidelines. This approach supports the Agency's commitment to accessibility and inclusive technology use.

OPEN Data Plan

SSS is committed to making data accessible to the public, thereby fostering transparency and accountability. Public access to data builds trusts by showing how decisions are made. The public can then better understand and engage with policies, services, and decision-making.

The OPEN Government Data Act (OGDA), signed into law in January 2019 as part of the Foundations for Evidence-Based Policymaking Act, mandates that Federal agencies make their data available in open, machine-readable formats, thereby promoting transparency and citizen engagement. The SSS's Chief Data Officer (CDO) plays a critical role in shaping, executing, and sustaining an open-data plan. The CDO ensures that open-data efforts align with privacy laws and security standards to ensure that sensitive data is protected and anonymized. The CDO manages a comprehensive inventory of the Agency's data assets. The CDO also leads the efforts to identify which datasets are safe to release for disclosure in the Federal Data Catalog. The CDO drafted guidelines for such disclosure in collaboration with the Selective Service Data Governance Board.

The Open Data Plan shall be updated annually and made available through the SSS' Strategic Information Resources Management Plan. Per M-19-23 Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018, the

Office of Management and Budget's (OMB) released Phase 2 Implementation for the Foundations for Evidence-Based Policy Act of 2018: Open Government Data Access and Management Guidance on January 15, 2025 provides agencies further guidance necessary to implement the Evidence Act's Open Data Plan requirement.

Data Strategy

The SSS FY24-26 Strategic Plan advances readiness, registration, and management excellence at SSS by driving large-scale readiness enhancements, increasing registration compliance through strategic and data-driven approaches, modernizing IT and cybersecurity capabilities, improving the customer experience, and encouraging other actions that enhance the Agency's IT performance, resilience, and adaptability. This strategic plan aligns with the National Security Strategy, President's Management Agenda, recent congressional direction, National Defense Strategy, SSS Strategic Vision, and findings from the report of the bipartisan National Commission on Military, National and Public Service.

SSS developed and integrated its Data Strategy into the SSS IRM Strategic Plan. The data strategy plan has three main goals: 1) ensure real-time data availability, integrity, and security to support seamless operational continuity and rapid decision-making during high-demand scenarios, such as conscription; 2) leverage advanced analytics and data-driven insights to assess registration trends, identify compliance gaps, and implement targeted interventions that improve overall compliance rates across the country; and 3) cultivate a data-driven workforce by providing data skills training, fostering a culture of collaboration, and equipping employees with the tools and knowledge needed to leverage data effectively in decision-making.

Data Governance Board

On July 15, 2020, SSS established its Data Governance Board (DGB) to address data management standards, priorities, policies, and best practices. The DGB serves as the leader for coordinating and facilitating implementation of Agency-wide processes and standards to optimize the value of data assets for use in Agency missions. The members of the DGB are appointed by the Director in accordance with the Office of Management and Budget (OMB) Memorandum M-19-23.

Data Governance Board Charter

When the DGB was established in July 2020, a Data Governance Board Charter was also drafted by the DGB. The DGB, chaired by the CDO, provides enterprise guidance and direction for achieving data-management objectives as defined in the Federal Data Strategy and the Foundations of Evidence-Based Policy Making Act. The Board serves as the leader for such guidance.

Comprehensive Data Inventory

Under the OGDA, Federal Government agencies are required to create a comprehensive data inventory that lists all data assets and datasets created by, collected by, under the control or direction of, and/or maintained by an agency. In accordance with this requirement, SSS has begun building its comprehensive data inventory using Data Catalog Vocabulary (DCAT) standard for metadata. SSS has one High Value Asset (HVA), the RCV system. The RCV system supports the SSS mission, which is governed by the MSSA. It provides a central repository for all data related to active registrants and potential violators. The RCV system is an intranet application used by authorized SSS personnel only. Although the database itself is not available to the public because it contains sensitive PII, the analytics and statistical reports derived from the data are public and can be shared. When requested by (the CIO/ADIT) , the SSS's Office of the General Counsel and the Senior Agency Official for Privacy will review the datasets from the comprehensive data inventory and decide which datasets will be published in the public platform, such as Data.gov.