DOT 1101.16C 05-03-2024

Subject: DEPARTMENT OF TRANSPORTATION, OFFICE OF THE CHIEF INFORMATION OFFICER ORGANIZATION MANUAL

1. PURPOSE. This Order updates the mission and functions of the Office of the Chief Information Officer (OCIO).

2. CANCELLATION. This Order cancels DOT 1101.16B, Department of Transportation (DOT or Department), Office of the Secretary Organization Manual, Office of the Chief Information Officer.

3. EXPLANATION OF CHANGES. This Order updates the functions of the Department's OCIO to improve sector cyber coordination and enhance the efficiency and effectiveness of the Department's role—led by the Office of Intelligence, Security, and Emergency Response (S-60)—as a Co-Sector Risk Management Agency (Co-SRMA), alongside the Department of Homeland Security, for the Transportation Systems critical infrastructure sector. The changes reflect the Department's role in supporting effective sector cyber coordination between the DOT Operating Administrations (OAs), Secretarial offices, DOT's Co-SRMA leadership within S-60, and DOT's regulated community. These changes will enable OCIO to better support the President's 2023 National Cybersecurity Strategy Implementation Plan.

   Documented below is information addressing the organizational realignment and specific changes included in the OCIO section of the DOT Organizational Manual:

   - The Office of Sector Cyber Coordination (S-88) will be led by the Associate Chief Information Officer for Sector Cyber Coordination

   - S-88 will include the following functional areas:

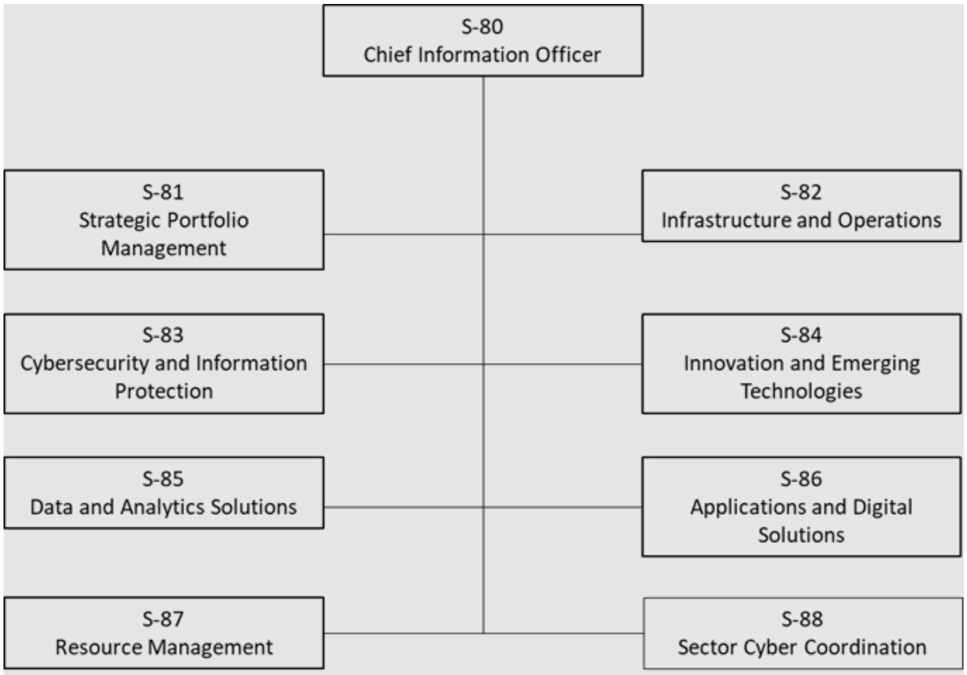
     - Division Management
     - Sector Cyber Coordination
     - Sector Cyber Support
     - Sector Cyber Engagement

   Additionally, changes are memorialized here to recognize the transfer of records management functions for the Office of the Secretary (OST) from the Office of the Assistant Secretary for Administration to OCIO, and to provide other clarifications.

4. MISSION. To enable the Department's Safety, Infrastructure, Innovation, and Accountability mission priorities through the delivery of effective digital services and solutions.

5. FUNCTIONS. The DOT Chief Information Officer (CIO) is the principal advisor to the Secretary and to DOT OAs on matters involving Information Technology (IT) including portfolio management, IT infrastructure and operations, cybersecurity, information protection, cyber risk management, information assurance, innovation and emerging technologies, enterprise data management, and application and digital solutions.

6. ORGANIZATION.


S-80
Chief Information Officer
S-81
Strategic Portfolio Management
S-82
Infrastructure and Operations
S-83
Cybersecurity and Information Protection
S-84
Innovation and Emerging Technologies
S-85
Data and Analytics Solutions
S-86
Applications and Digital Solutions
S-87
Resource Management
S-88
Sector Cyber Coordination

7. ORGANIZATION.

a. Office of the Chief Information Officer (CIO) (S-80): The immediate office of the CIO supports front office duties. The office includes the following functional areas:

1) Chief Information Officer
2) Deputy Chief Information Officer
3) Staff and Program Management

b. Office of Strategic Portfolio Management (S-81): The Office of Strategic Portfolio Management (SPM), led by the Associate CIO for Strategic Portfolio Management, ensures the strategic alignment of IT resources to the mission of the Department. The SPM office provides an enterprise-wide view for IT resource management by working with program and mission offices to match OCIO IT capabilities with their mission needs. The office maintains department-level IT policy, governance, and enterprise risk, and compliance programs to ensure an enterprise-wide perspective. Additionally, the office develops and maintains department-level IT acquisition strategies and approvals. The office also performs these functions for OST and is the primary focal point for governance and coordination of IT within OST on behalf of the DOT CIO.

The office performs its IT Investment and Budget functions in coordination with the DOT Chief Financial Officer (CFO) and the OCIO Office of Resource Management and includes the following functional areas:

1) Division Management
2) IT Governance, Policy, and Oversight

3) IT Investment and Budget
4) Architecture and Acquisition Strategy
5) IT Workforce
6) Enterprise Software License Management
7) IT Supply Chain Risk Management
8) OCIO Audit Liaison

c. Office of Infrastructure and Operations (S-82): The Office of Infrastructure and Operations, led by the Associate CIO for Infrastructure and Operations, provides commodity IT Shared Services to enable DOT program offices to carry out mission activities. The services include activities related to infrastructure operations, help desk, network, server, storage, desktop, Cloud, email, wireless/mobile, telephony, Internet, telecommunications, data center management, disaster recovery, and all other infrastructure/platforms as service commodity IT offerings, including assistive technologies. The office includes the following functional areas:

1) Division Management
2) Technical Architecture
3) Configuration Management
4) End User Services
5) Infrastructure and Service Delivery

d. Office of Cybersecurity and Information Protection (S-83): The Federal Information Security Modernization Act of 2014 (FISMA or the latest version of FISMA) and the Office of Management and Budget (OMB) Circular A-130 require the Department of Transportation to maintain a DOT-wide Cybersecurity Program that collaboratively maximizes resources; protects DOT information systems and operations; and establishes the governance framework, policy requirements, and standards for managing the cybersecurity and privacy of departmental electronic information and associated assets. In accordance with these requirements, DOT Order 1351.37 and the compendium establishes and explicates the DOT Cybersecurity Program and through this Program, DOT must continue to develop and implement its mission to protect itself against malicious attempts to damage, disrupt, or gain unauthorized access to its information systems. The DOT Chief Information Security Officer (CISO) and S83 manages and oversees the Department's Cybersecurity Program which performs the following functions:

- Serves as the central focal point for cybersecurity
- Deploys and manages a department-side common security strategy
- Promotes awareness of security risks and policies
- Develops standards for and performs security and privacy control monitoring and evaluation
- Protects the privacy of individuals
- DOT Security Operation Center as a shared service directed by the FAA CISO, with governance under S83 and the DOT CISO

The office also performs these functions for OST, including the risk executive function as defined by the National Institute of Standards and Technology[1], and is the primary focal point for IT cybersecurity and privacy risk management within OST on behalf of the DOT CIO.

The office performs its privacy, information collection, records management and forms management functions in coordination with the Department's Chief Data Officer and includes the following functional areas:

1) Division Management
2) Privacy and Information Governance
3) FISMA Compliance
4) Cybersecurity Engineering, Operations, and Incident Response
5) Risk Management and Authorization
6) Information Collection under the Paperwork Reduction Act
7) Forms Management
8) Enterprise and OST level Records Management
9) National Security Systems

e. Office of Innovation and Emerging Technologies (S-84): The Office of Innovation and Emerging Technologies, led by the Chief Innovation Officer, leads the Department's use of artificial intelligence, robotic process automation, and other emerging technology solutions. The office has a detailed understanding of technology innovation that is required to advance the mission of the Department and helps identify programs to support mission activities at the OAs. In addition, the office promotes the use of IT and innovative technology solutions to improve the operations, productivity, accessibility, efficiency, effectiveness, and service delivery of the Department. The office includes the following functional areas:

1) Division Management
2) Innovation and Emerging Technologies

f. Office of Data and Analytics Solutions (S-85): The Office of Data and Analytics Solutions, led by the Assistant CIO for Data and Analytics Solutions, is responsible for managing the Department's data, including geospatial data, as an asset. The office's mission is to manage and use data to reduce information collection burdens on the public; increase program efficiency and effectiveness; and improve the integrity, quality, and utility of data for all users within and outside the agency. The office is responsible for lifecycle data management; managing the Department's data assets, promoting best practices for data; maximizing the use of data in the agency, including the production of statistics, cybersecurity, and the improvement of agency operations, and engaging employees, contractors, and the public in using and analyzing data. The office architects, delivers, and delivers data platforms and other shared services that support data and

[1] NIST SP 800-37 rev 2; December 2018; https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

analytics for the entire Department, regularly reviewing the impact of the infrastructure of the agency on data asset accessibility and continually improving such infrastructure to reduce barriers that inhibit data asset accessibility. The office includes the following functional areas:

1) Division Management
2) Geospatial Management
3) Data Engineering and Analytics
4) Data Platform Services and Operations

g. Office of Application and Digital Solutions (S-86): The Office of Application and Digital solutions, made up of program managers, developers, engineers, and analysts, and led by the Associate CIO for Application and Digital Solutions, provides advisory services relating to the Department's application development and digital solutions to ensure a modern, accessible, and user-centered approach to mission and support systems. Working with modal CTOs and program offices across the Department, the office ensures the design and development of user-centered solutions. The office also provides leadership and program management for the Department's Section 508 IT accessibility program. The office also designs, builds, delivers, and maintains enterprise platform technologies that are for use across the Department. Finally, the office conducts and supports IT program management to ensure the effective delivery of IT results to users and stakeholders inside and outside the Department. The office includes the following functional areas:

1) Division Management
2) Information Technology Accessibility Program Management
3) Enterprise Platform Delivery
4) Mission System Support
5) Project Management
6) Strategic Communication Services

h. Office of Resource Management (S-87): The Office of Resource Management, led by the Associate CIO for Resource Management, helps to support the daily functions of OCIO to ensure proper and consistent business processes. In coordination with the OST Office of the Chief Financial Officer (B-20), the office provides financial and budget management services across the OCIO operating budgets and ensures a transparent billing process associated with the Working Capital Fund. In addition, organizational management and outreach including procurement support, talent outreach and development, event logistics management, asset management, and space planning and management are provided. The office performs its OCIO IT Budget and Finance functions in coordination with the Office of Strategic Portfolio Management, the OST Chief Financial Officer, and the Working Capital Fund, and includes the following functional areas:

1) Division Management
2) OCIO IT Budget and Finance

3) Procurement Operations
4) Organizational Management
5) Administrative Services
6) Contract and Customer Support

i. Office of Sector Cyber Coordination (S-88): The Office of Sector Cyber Coordination, led by the Associate CIO for Sector Cyber Coordination, is responsible for coordinating with, supporting, and engaging DOT offices (including S-60, OST-P, DOT OAs, and other DOT offices as needed), Transportation Systems Sector Co-SRMA partners, interagency partners, stakeholders, and DOT's grant recipient and regulated community on transportation sector cybersecurity issues and needs. The Office coordinates and develops cybersecurity language for inclusion in financial assistance agreements with DOT offices and OAs. The Office coordinates with OAs to understand stakeholder cyber needs and requirements and participates in the DOT Cybersecurity Topical Cybersecurity Research Working Group and other relevant working groups. The Office, in coordination with OST-P, relevant DOT offices, and OAs, explores and determines grantee cyber risk for funded projects and recommends appropriate cybersecurity mitigation requirements. The office, in coordination with S-60, provides inter- and intra-agency liaison on cybersecurity and administers the DOT Cyber Coordination Council. The Office inspects cybersecurity programs of financial assistance recipients as required to harvest best practices, as well as lessons-learned following cyber events. When requested by law enforcement, the Office assists in the investigation of cybersecurity events. In coordination with S-60 and relevant interagency partners, the Office develops periodic assessments of cyber risk in the transportation sector. Additionally, the Office aggregates and, in coordination with S-60, the OAs, and interagency partners, makes available cybersecurity best practices for the transportation sector. In coordination with S-60 the Office also actively provides cybersecurity updates to the Office of the Secretary. The Office provides cybersecurity outreach and leads other cybersecurity messaging and engagement opportunities with DOT and OA Public Affairs and other relevant DOT offices. The Office includes the following functional areas:

1) Division Management
2) Sector Cyber Coordination
3) Sector Cyber Support
4) Sector Cyber Engagement

CORDELL SCHACHTER Digitally signed by CORDELL SCHACHTER Date: 2024.03.21 16:05:08 -04'00'

Cordell Schachter
Chief Information Officer