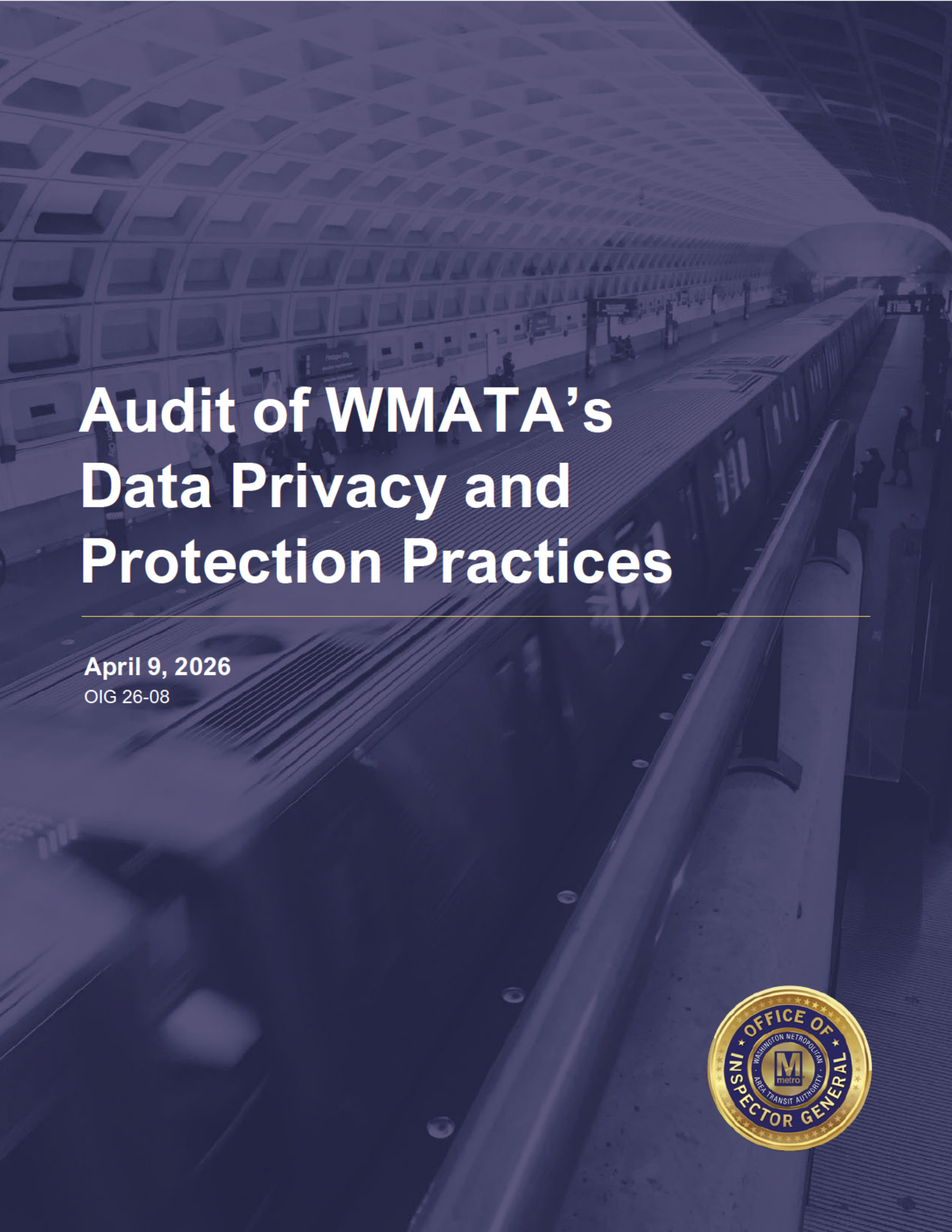


Audit of WMATA's Data Privacy and Protection Practices

April 9, 2026

OIG 26-08

Results in Brief

Audit of WMATA's Data Privacy and Protection Practices

Audit Objective

The audit objective was to assess the Washington Metropolitan Area Transit Authority's (WMATA's) compliance with applicable data privacy laws, regulations, and standards.[1]

Why We Did the Audit

- To evaluate the effectiveness of controls protecting WMATA's sensitive and personal data from unauthorized access or misuse is critical, as failures in this area can expose the authority to substantial legal, financial, and reputational risks.

- This audit was included in the Fiscal Year (FY) 2024 Annual Audit and Evaluation Plan in response to WMATA management's concerns regarding WMATA's data privacy practices.

Recommendations

This report identified seven recommendations. WMATA can strengthen data privacy controls and cybersecurity processes by addressing these recommendations.

What OIG Found

OIG found that WMATA had not developed a data privacy program that fully incorporated applicable requirements and leading standards. The audit revealed systemic weaknesses in WMATA's data privacy posture, including the absence of a comprehensive data privacy framework, insufficient deployment of automated security tools, and a lack of centralized encryption standards and enforcement. WMATA also lacks enterprise-wide coordination and enforcement mechanisms, which further increases the risk of data breaches and non-compliance.

These deficiencies suggest that WMATA's current data privacy posture and practices do not adequately safeguard sensitive data in accordance with the National Institute of Standards and Technology, the Health Insurance Portability and Accountability Act, or other best-practice privacy standards.

The Digital Modernization department, which oversees the Authority's information technology infrastructure, recognizes the importance of maintaining a robust data privacy program and has taken steps toward ensuring data protection. However, WMATA needs to make further improvements to enhance its data privacy posture, achieve full compliance with its own Cybersecurity Policy Manual, and strengthen WMATA's ability to protect data across the enterprise.

[1] *WMATA's Cybersecurity Policy Manual describes and includes by reference the applicable data privacy and protection guidance and standards.*

Table of Contents

Data privacy refers to the right of organizations and individuals to control how personal and sensitive information is collected, used, stored, and shared.[2] Organizations rely on data governance frameworks comprising policies and technical, physical, and organizational controls to ensure data protection and regulatory compliance. These controls typically include data-handling procedures, cybersecurity measures such as access management and encryption, and safeguards that protect facilities, systems, and personnel. Together, they support the confidentiality, integrity, and availability of data.

For the Washington Metropolitan Area Transit Authority (WMATA), these principles apply to a wide range of data, including customer information, employee records, operational data, and information managed by third-party vendors. WMATA's data privacy controls are inherently complex due to the diverse nature of its operational and personal data.

Organizations that do not implement or maintain strong data privacy controls are more susceptible to attacks from malicious actors, with serious consequences for their business, employees, and clients. In the last several years, multiple transit systems have been hit by cyberattacks, including an August 2020 attack on the Southeastern Pennsylvania Transportation Authority in Philadelphia, an April 2021 attack on the New York City Metropolitan Transportation Authority, and a January 2023 attack on the Bay Area Rapid Transit Authority in San Francisco.[3] More recently, in August 2025, the Maryland Department of Transportation experienced a ransomware attack that exposed employee and customer data, including social security numbers and driver's license details.

These events underscore the importance of strong data privacy and cybersecurity practices for organizations that manage sensitive information. WMATA faces similar risks due to its reliance on third-party systems and its collection of sensitive and personally identifiable information (PII). Consequently, WMATA has the responsibility to ensure the protection of customer and employee data through strong data privacy controls and practices.

---

[2] For purposes of this audit, the term "Data Privacy" encompasses the protection of personal data and personally identifiable information, as well as broader categories of sensitive organizational information, including financial data, proprietary information, security-sensitive information, and other confidential data, consistent with the NIST framework referenced in this report.

[3] See Jonathan Greig, San Francisco BART investigating ransomware attack, The Record, January 8, 2023 (available at https://therecord.media/san-francisco-bart-investigating-ransomware-attack); Kelly McLaughlin and Lauren Frias, Suspected Chinese Hackers Breached NYC's MTA Computers in April, Business Insider, June 2, 2021 (available at https://www.businessinsider.com/suspected-chinese-hackers-breached-nyc-mta-computers-2021-6); and Michael Tanenbaum, SEPTA working through messy aftermath of August cyberattack, August 26, 2020 (available at https://www.phillyvoice.com/septa-cyberattack-malware-august-2020-emails-security-philadelphia/).

Departmental Responsibility for WMATA's Data Privacy Governance

The Digital Modernization (DM) department oversees WMATA's IT infrastructure, including computers, servers, databases, and other hardware and software. DM's responsibility for IT infrastructure includes implementing cybersecurity programs, standards, and controls to enhance the safety and reliability of WMATA's data protection. Within the DM department, the Office of Cybersecurity (DMCS) has the added responsibility of working with other WMATA departments and employees to prevent data breaches. WMATA's Office of General Counsel is responsible for providing legal advice and counsel regarding applicable laws and regulations, as well as administering Metro's Privacy Policy and Public Access to Records Policy.

WMATA's Data Protection Framework

WMATA's data privacy controls are outlined in its Cybersecurity Policy Manual (Manual), which is primarily aligned with the National Institute of Standards and Technology's (NIST's)[4] Cybersecurity Framework (CSF) Version 2.0. The CSF outlines six core functions, which represent the lifecycle of managing cybersecurity risk:

1. Govern – establish and monitor the organization's cybersecurity risk management strategy, policies, and roles.
2. Identify – understand and manage cybersecurity risks to systems, assets, data, and capabilities.
3. Protect – implement safeguards to ensure delivery of critical services and limit the impact of potential events.
4. Detect – develop and implement activities to identify the occurrence of a cybersecurity event.
5. Respond – take action regarding a detected cybersecurity incident to contain its impact.
6. Recover – restore capabilities or services impaired by a cybersecurity incident.

The Manual also incorporates guidance from NIST Special Publications (SPs). For example, the manual references NIST SP 800-53, which outlines security and privacy controls for federal information systems, and NIST SP 800-171, which focuses on protecting controlled unclassified

[4] Congress established NIST in 1901 to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

information in non-federal systems. NIST SPs provide best practices for implementing security controls, safeguarding sensitive data, and evaluating cybersecurity.

In addition, WMATA's Manual cites to and relies on guidance from the Federal Information Security Modernization Act (FISMA) and the Health Information Portability and Accountability Act (HIPAA). FISMA requires federal agencies to implement information security programs, while HIPAA sets rules for how healthcare providers, insurers, and their business partners must handle protected health information, including medical records, test results, and billing data.

Moreover, the Manual draws from industry-recognized best practices. For example, the Manual includes language from the Center for Internet Security (CIS)'s Critical Security Controls designed to help organizations improve their cybersecurity posture. The Manual also includes language from an international standard that provides a framework for organizations to manage and protect sensitive information.

Together, these requirements and best practices create a comprehensive and adaptable framework intended to strengthen WMATA's cybersecurity posture and readiness against evolving threats, such as data privacy breaches, and to maintain compliance with applicable laws and regulations.

DMCS's Self-Assessment of Overall Data Privacy Posture and Maturity

In October 2024, DMCS completed a self-assessment titled *Data Security Framework – Maturity Assessment* (*see* **Appendix B**). The self-assessment was conducted to identify framework vulnerabilities and gaps in the current program, using NIST Standards as the basis.[5] Based on DMCS's Self-Assessment, the program was at [redacted] Based on OIG's review of this self-assessment, DMCS concluded that data processing relationships are poorly understood, training is outdated, and responsibilities are unclear. In short, DMCS recognized that WMATA needed to undertake additional work to improve its data privacy posture and protection practices.

[5] *NIST defines data privacy posture as: the status of the information systems and information resources (e.g., personnel, equipment, funds, and IT) within an organization based on information assurance resources (e.g., people, hardware, software, policies, procedures) and the capabilities in place to comply with applicable privacy requirements and manage privacy risks and to react as the situation changes.*

[6] *A rating that describes the degree to which organizational unit processes meet the intentions and values articulated in a predefined set of practice areas. The rating is based on the achievement of a specified set of practice group levels within the predefined set of practice areas (e.g., 1 = Initial/Ad hoc, 2 = Developing, 3 = Defined, 4 = Managed and Measurable, 5 = Optimized).*

Finding 1: WMATA's Data Privacy Posture Needs Improvement, and Practices Require Expansion

WMATA's data privacy posture, which includes its systems, resources, and controls for meeting privacy requirements, has multiple weaknesses that limit WMATA's ability to safeguard sensitive information. WMATA lacks key governance roles and foundational documents, such as a Chief Privacy Officer (CPO) and a System Security Plan (SSP). Additional weaknesses include organizational silos, insufficient collaboration between DM and operational technology (OT) groups from other departments,[7] inadequate training, incomplete data inventory and mapping, insufficient enforcement resources, and poorly defined communication protocols. These gaps increase WMATA's exposure to data breaches, noncompliance with applicable regulations, and reputational harm.

Absence of a CPO

NIST, whose technology standards are widely adopted across the public and private sectors, recommends appointing a CPO to manage organization-wide privacy.[8] Although WMATA is not a federal agency, it adheres to NIST best practices in other areas, such as conducting maturity assessments.[9] According to NIST SP 800-53A, Release 5, the CPO role is essential for overseeing privacy requirements, conducting impact assessments, and ensuring compliance with applicable laws.

Currently, WMATA's DMCS assigns enterprise data privacy and protection responsibilities to the Senior Manager, Cybersecurity Officer, within the Cybersecurity Unit and two part-time support staff, [redacted]. The Officer's job description is generic, the role is positioned below executive leadership, and does not include the duties, authority, and resources of a CPO role. Without the proper hierarchical positioning, authority, and human resources normally afforded to a CPO, the senior cybersecurity manager is limited in their role to implement the required privacy measures and enterprise-wide data policies.

---

[7] OT groups are the WMATA departments that own the various OT systems. WMATA OT departments primarily include Operations and Infrastructure.

[8] NIST SP 800-53A Release 5: Assessing Security and Privacy Controls in Information Systems and Organizations.

[9] A NIST maturity assessment uses the NIST Cybersecurity Framework's (CSF's) structured approach to gauge an organization's cybersecurity program. The assessment progresses from ad hoc (Partial) to optimized (Adaptive) through four defined levels (Partial, Risk-Informed, Repeatable, Adaptive), identifying current gaps, setting improvement targets, and creating a roadmap for enhanced risk management and resilience. It often involves self-assessments against the framework's functions, categories, and subcategories.

DMCS's 2024 self-assessment (*see* **Appendix B**) acknowledged the importance of a CPO and supports the Office of Inspector General's (OIG's) observation. DMCS representatives stated they were unaware of any plans to fill the position. Without a designated CPO, WMATA falls short of its own best practice goals and industry standards.

Gaps in Data Privacy and Protection Policies Implementation

The Manual serves as the foundation for WMATA's data privacy and protection framework, outlining requirements for handling personally identifiable information (PII) and other sensitive information across the enterprise. However, interviews with DMCS management indicated that WMATA has struggled to implement, monitor, and enforce these policies on an enterprise-wide basis. Key gaps include:

1. *Insufficient communication and awareness* – Lack of coordination and communication among stakeholders responsible for implementing, monitoring, enforcing, and complying with the policy has hindered consistent understanding and execution.

2. *Technical challenges* – WMATA had not yet fully implemented the technical capabilities needed to adequately implement, monitor, and enforce policy requirements.

3. *Organizational structures* – Decentralized security administration, organizational silos, shadow IT, and autonomous groups with independent IT functions have slowed the adoption and implementation of new policies.

4. *Inadequate monitoring and evaluation mechanisms* – Without clear mechanisms to track progress and measure the impact of a policy, it is difficult for WMATA to identify problems or make necessary adjustments.

5. *Difficulty collecting relevant data* – Challenges in collecting accurate and timely data from the various systems impede effective monitoring.

6. *Insufficient enforcement resources* – DM has not fully assessed the personnel, funding, or equipment necessary to monitor and enforce compliance with policy requirements.

These gaps collectively impede policy adoption and limit WMATA's ability to achieve enterprise-wide oversight and compliance.

Absence of a System Security Plan

The Manual requires that WMATA maintain a System Security Plan (SSP), which is "a formal document(s) that provides an overview of the security and privacy requirements for an information system and describes the security and technical privacy controls in place or planned for meeting those requirements."[10] The SSP outlines the baseline security requirements for accessing, processing, and storing data, as well as privacy requirements, along with the controls in place to meet them. WMATA has not yet developed an SSP as required by policy. As a result, the baseline requirements for data access, data handling, and data storage are not incorporated into a formal data privacy protection framework. This lack of an SSP weakens WMATA's data security posture and limits its ability to address data security vulnerabilities effectively.

Organizational Fragmentation of Compliance Responsibilities for Data Privacy and Protection

Data privacy, protection, compliance, and policy responsibilities at WMATA are fragmented, with departments such as DM, Legal, and the Metro Transit Police Department maintaining separate policies and practices. While departments may manage different data and have varying data security requirements, data privacy must be handled as a cohesive, unified organizational approach. OIG found that communication among these groups is informal and inconsistent, and no consolidated policy defines communication and coordination among the departments. This approach allows individual departments, and potentially others, to manage data protection independently, creating additional management challenges, inconsistencies, and gaps in data protection application and compliance across the organization.

Challenges in Data Inventory and Data Mapping

NIST recommends maintaining a comprehensive inventory of data sources and mapping data flows, enabling organizations to precisely plan and allocate resources by targeting encryption, applying appropriate access controls, and prioritizing compliance requirements for the data.[11] DMCS lacks a formal data-mapping process and visibility into how data flows across systems.[12] According to NIST, maintaining an inventory list and mapping is critical because it shifts data

---

[10] *WMATA's Cybersecurity Policy Manual, version 1.1, Appendix E, p. 174.*

[11] *NIST SP 800-53A Release 5: Assessing Security and Privacy Controls in Information Systems and Organizations.*

[12] *Data flow refers to the movement, processing, and transformation of data through a system, organization, or application from its source to its eventual destination or use. It encompasses the path data takes, any changes made to it along the way, and how it is stored and retrieved.*

protection from a reactive approach to a proactive, strategic one. This deficiency limits DM's ability to enforce security controls across the entire enterprise.

DMCS management recognized the challenges of implementing security controls across the enterprise and identified it as a priority initiative. They noted plans to catalog approximately 155 systems, classify them, and apply legal notices accordingly. DMCS intends to use [redacted] for automated mapping and classification; however, DMCS representatives stated that this goal will not be realized in the immediate future. Until a complete inventory and mapping process is in place, WMATA cannot proactively and effectively manage security risks.

Collaboration Between DM and OT Groups Needs Improvement

WMATA policy establishes DM as the overall responsible party for managing WMATA's IT assets and data security. However, to leverage specialized expertise, the OT groups from Operations and Infrastructure manage their OT systems[13] that support Bus and Rail operations. Such systems include operational applications, train control devices, communication systems, and Supervisory Control and Data Acquisition (SCADA)[14] platforms. Therefore, OT groups are responsible for the daily oversight and maintenance of these critical systems. These OT systems contain sensitive operational and passenger data that must be identified, consistently protected, and continuously monitored to ensure the integrity and safety of WMATA's services. Accordingly, DM and OT groups must improve coordination to adequately manage data privacy practices across the enterprise.

While formal and informal collaboration between DM and OT groups exists, DMCS management stated it remains incomplete and is a work in progress. This lack of full visibility into OT systems limits DMCS's ability to implement and enforce security controls, thereby increasing susceptibility to associated risks. DMCS plans to address each environment progressively in a phased approach; however, DMCS has not yet developed a formal action plan or timeline.

Absence of Training on Data Privacy Controls, Protocols, and Policies

WMATA policy requires all employees to complete yearly computer-based cybersecurity training, including safeguarding data practices. Additionally, DMCS conducts data privacy and

---

[13] NIST defines OT as programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

[14] A type of computer system used to monitor and control industrial processes from a central location.

security awareness training and routinely issues bulletins. However, WMATA lacks specific role-based, technical training for those who must implement and use data privacy control mechanisms, data encryption standards, protocols, and related policies. As a result, these personnel lack a uniform standard or clear guidance on which data protection controls to implement and how to implement them, leading to inconsistent and ad hoc application of data protection measures. Without targeted training, they are neither aware of all required protocols nor equipped to implement them correctly, leaving critical gaps in WMATA's privacy defenses.

DMCS's Self-Assessment of Program Supports OIG Observations

DMCS's self-assessment aligns with OIG's observations outlined in this finding (see **Appendix B**). The DMCS self-assessment highlighted leadership and organizational changes, along with the lack of a dedicated privacy program, as key factors in the organization's low maturity. This low maturity adversely impacts strategic direction, operational continuity, staffing, and budgeting. To address these issues, a DMCS representative is initiating efforts to achieve NIST Tier 4 and enhance data privacy through risk assessments, data-handling protocols, and stakeholder engagement. Management plans to hire skilled staff and secure funding essential for program success. Additionally, DM is committed to prioritizing and increasing collaboration with OT groups from other departments to provide for a more integrated data privacy approach. Despite these plans, WMATA lacks a comprehensive data privacy program, leaving gaps that must be addressed to achieve a higher level of maturity. Currently, there is no formal plan or timeline for implementation.

Recommendations

OIG recommends the GM/CEO:

1. Develop and implement a formal enterprise-wide Data Privacy Program strategy and plan, with defined milestones, timelines, and performance metrics to achieve its target maturity level (e.g., NIST Tier 4), and at a minimum, address the following:

    a. Establishment of a senior-level position with authority, resources, and organizational positioning necessary to implement enterprise-wide privacy policies.

    b. Development of a formal SSP, to formalize the baseline requirements outlined in the Manual.

c. Development of data mapping and inventory practices, to catalog all systems, and an interim process for manual data mapping to gain immediate visibility into critical data flows.

d. Implementation of a formal governance committee or structure with representatives from DM and OT leadership to create and mandate a unified set of data privacy and security controls for all OT systems.

e. Inclusion of a strategy for automated data privacy tools and processes.

f. Development of a formal, ongoing privacy risk assessment process, integrated with best practices to proactively identify, assess, and prioritize data privacy risks across the entire enterprise, including both IT and OT environments.

g. Implementation of quality assurance and quality control processes to continuously monitor, validate, and audit the effectiveness of all deployed data privacy controls, policies, and tools. This includes defining metrics, conducting periodic reviews, and performing internal audits to ensure ongoing compliance and identify areas for improvement.

h. Implementation of role-based data privacy training for personnel responsible for implementing technical controls (e.g., encryption, data labeling) and handling sensitive data.

Management Response

1a. Digital Modernization (DM) concurs with this recommendation. WMATA intends to assign this role to a planned Governance Board responsible for enterprise data to consolidate and oversee enterprise data related functions within the (DM) organization. This emerging Governance Board will be coordinated by DM and comprised of senior-level individuals with representation from across the enterprise. The enterprise Data Privacy Program will be formally positioned under this Governance Board, with appropriate authority, organizational placement, and accountability to implement and enforce enterprise-wide data privacy policies and standards. The Governance Board will be responsible for coordinating privacy governance across DM, consistent with NIST best practices of accountability.

1b. DM agrees with this recommendation and appreciates the auditors' focus on strengthening WMATA's data privacy posture. DMCS is already developing and authorizing System Security and Privacy Plans (SSPPs) for major enterprise platforms

and services under its ownership.

Consistent with NIST SP 800-37 Rev. 2 and NIST SP 800-53, an information system is defined as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." Accordingly, SSPPs are scoped to well-defined system boundaries and are developed collaboratively with data owners.

In alignment with this recommendation, DMCS has defined General Support System (GSS) 10 as the collection of tools and technologies used by Cyber to support data privacy and sensitive data protection. The system SSPP currently exists in RSA Archer and is undergoing control assessment and validation to ensure compliance and effectiveness.

Through the Governance Board (addressed in 1a), DMCS will continue coordinating with Metro stakeholders to formalize SSPPs where appropriate, including documenting existing controls and associated Plans of Action and Milestones (POA&Ms). Milestones for completion of GSS 10—and for the subsequent identification and documentation of sensitive data repositories across WMATA—will be coordinated with the appropriate stakeholders and incorporated into the Corrective Action Plan (CAP).

1c. DM concurs with this recommendation. The Enterprise Architecture Office is developing an Enterprise Information Repository (EIR) to establish a centralized, authoritative, and governed inventory of systems and data assets across the enterprise. The EIR will provide standardized visibility into system ownership, data sensitivity, and high-level data flows. As an interim measure to gain immediate visibility into critical data flows, structured manual data mapping will be conducted for known systems while the EIR is incrementally implemented and expanded through a minimum viable- product (MVP) approach.

1d. DM concurs with this recommendation. DM will govern and maintain the Enterprise Inventory Repository (EIR) using formal data governance, data quality, and change management practices. Updates to the EIR will be mandated as part of the Change Control Board (CCB) approval process for system changes, and monitoring mechanisms will be used to identify- stale or incomplete records. This governance structure will support coordination between DM leadership and enable the consistent application of unified data privacy and security controls across all systems. (DM recommends combining 1a, 1c, and 1d into one CAP).

1e. DM agrees with this recommendation. Metro has an approved and funded roadmap for Secure Foundation, a core component of the broader Digital Ecosystem strategy, and

multiple related initiatives are already underway.

As part of this work, Metro is implementing protection measures that include automated Data Loss Prevention (DLP), controls for removable/USB storage, and capabilities to identify and monitor sensitive data. These efforts are currently in varying stages of implementation across the environment. To provide clear management tracking and visibility, Metro will create a corrective action plan (CAP) to consolidate and document the strategy, including relevant milestones, timelines, and accountable owners for these capabilities. Metro will use the CAP to monitor progress and report status through established governance mechanisms.

1f. DM concurs with this recommendation. DM has partnered with Audit and Compliance on this effort. The Risk & Business Advisory Services team will support management's efforts to establish a formal, ongoing privacy risk assessment process to strengthen the organization's enterprise-wide data privacy posture. This initiative will align with existing Enterprise Risk Management practices and support management's responsibilities to proactively identify, assess, and prioritize privacy risks across IT and OT environments.

1g. DM agrees with this recommendation. Audit and Compliance has agreed to provide independent assurance on data privacy compliance. These efforts will focus on supporting DM management's goal of identifying opportunities for improvement in data privacy-lane. The performance of any assessment has Data Privacy program dependencies that must happen before any reviews can be conducted.

1h. DM agrees with this recommendation. DM, in partnership with Human Capital, will create role-based data privacy training for personnel responsible for implementing technical controls and handling sensitive data.

OIG Comment

OIG considers management's comments responsive to the recommendations 1a through 1h, and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

2. <u>After developing a formal enterprise-wide Data Privacy Program strategy and plan, implement unified policies, procedures, and processes for coordinating and communicating for all entities that share responsibility for disseminating and protecting sensitive data.</u>

Management Response

DM agrees with this recommendation. Based on the Board-approved enterprise-wide Privacy Policy, the Cybersecurity Policy, and the establishment of a Data Privacy Program, DM will implement the strategy and plan to ensure programmatic governance and consistency in securing our data assets. This will require several dependencies, consistent with a proper inventory of WMATA-wide data assets, data asset categorizations, and the appropriate processes and procedures that drive Metro-wide conformity. This approach will be a multi-year effort that will enable validity, unified alignment, and effective coordination with the relevant business owners across WMATA.

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

Finding 2: DMCS Has Not Fully Implemented Comprehensive Enterprise-Wide Automated Security Solutions to Protect Vulnerable Data

WMATA's Cybersecurity Manual requires DMCS to employ automated tools to enhance security and prevent malicious or unintentional access to sensitive data. Despite this requirement, DMCS has not fully implemented enterprise-wide computerized tools to avoid data loss, including systems to detect sensitive information, identify vulnerabilities, enforce labeling protocols, and control the use of removable media. These gaps leave WMATA more susceptible to risks of data loss and security incidents.

Data Security Applications Have Not Been Fully Deployed or Integrated

[redacted]

A DMCS representative stated that implementing DLP enterprise-wide is challenging due to the diversity and volume of data sources at WMATA, as well as WMATA's fragmented data environment, which spans both on-site and cloud-based systems. This diversity, along with legacy systems, OT environments, and WMATA's constantly evolving infrastructure, complicates the enterprise-wide implementation and integration [redacted]. This fragmentation creates entry points for cyber threats and leaves sensitive data inadequately protected.

Lack of Automated Controls for Removable Storage Devices

The Manual restricts the use of portable storage devices[16] and prohibits the use of non-WMATA-issued devices without an identifiable owner. Although DMCS has the technical capability to enforce these restrictions, it has not fully deployed automated technical controls across the

[15] *DLP - Detecting and addressing data breaches, exfiltration, or unwanted destruction of data.*

[16] *Portable storage devices include, but are not limited to, USB flash drives, external hard drives, and other removable media.*

enterprise. Instead, it continues to rely on manual processes due to organizational fragmentation, independent departmental practices, and ongoing structural changes. The absence of automated controls increases susceptibility to associated risks, as removable media can easily be used to extract sensitive data undetected. Reliance on manual controls increases the potential for human error and unauthorized data transfers, undermining WMATA's data loss prevention efforts. Furthermore, the lack of automated controls weakens the effectiveness of WMATA's existing DLP policies.

DMCS representatives stated that WMATA's current data management approach impedes the enterprise-wide implementation of specific data management controls. They noted that some departments operate independently, leading to varied practices in the use and management of removable storage devices. They also stated that WMATA's leadership and organizational structure changes have affected DMCS's progress in implementing these data security solutions and that implementing the necessary tools and programmatic infrastructure (people, processes, technology) remains ongoing.

Recommendations

OIG recommends the GM/CEO:

3. Create a funded, time-bound project plan to achieve enterprise-wide deployment and configuration of automated data security tools that can (1) resolve, detect, and categorize sensitive information, (2) identify DLP vulnerabilities, (3) implement data sensitivity labeling protocols, and (4) enforce data encryption requirements enterprise-wide.

Management Response

DM agrees with this recommendation and will establish a time-bound project plan to support a Metro-wide configuration and deployment of automated data security tools capable of categorizing sensitive information, detecting and resolving DLP vulnerabilities, implementing data sensitivity labeling protocols, and enforcing established data encryption requirements across Metro. Due to Metro's unique information technology environment, the deployment will be executed with a risk-based deployment, prioritizing our systems based on assessed criticality factors. DM feels this approach is the best method to address our legacy systems, operational technologies, cloud-based services, and third-party solutions. Coordination for enterprise-wide integration with data owners will occur through the Data Governance Board and other applicable stakeholders to sequence implementation in a manner consistent with mission and business needs.

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

4. Implement enterprise-wide automated DLP solutions fully to enforce existing policies and to monitor, control, and encrypt data transferred to removable storage devices to mitigate the identified risks.

Management Response

DM agrees with this recommendation and will implement a DLP solution that fully enforces our existing policies, provides enhanced monitoring capabilities and greater control, and enables data encryption when transferred to removable storage devices. These actions are already in progress, as DM has been addressing these program gaps by integrating our USB control efforts into CAP 590. DM is already working to implement measures to restrict, monitor, and audit the use of removable media and storage devices. These strategic approaches will reduce the risk of unauthorized data transfers. These actions are consistent with the approach outlined in recommendation response 1e.

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

Finding 3: Lack of Centralized Data Encryption Standards, Controls, and Enforcement

WMATA has not implemented an enterprise-wide policy and protocols for encrypting sensitive systems and applications, as required by the Manual, Section 2d. The manual directs WMATA to "[e]nsure all sensitive information is encrypted in storage and in transit . . ." but does not detail how the encryption will be accomplished. Instead, DMCS management stated that individual departments are permitted to manage their own encryption methods without a centralized framework. This decentralized approach has resulted in inconsistent practices and a lack of enforceable standards. These limitations, compounded by the absence of an enterprise-wide encryption training program, leave sensitive passenger and operational data vulnerable to unauthorized access and cyber threats.

DMCS acknowledges these deficiencies in its data privacy program and is working to address them. However, progress has been significantly hindered by resource constraints, including limited staffing and budget. Currently, only one employee is dedicated to these efforts, and encryption tools are being deployed incrementally rather than comprehensively across all WMATA IT environments. Implementing robust encryption standards and centralizing control over encryption practices are essential for safeguarding WMATA's data, whether it is in transit, at rest, or in use.

Furthermore, WMATA has not implemented an enterprise encryption training program to train staff in data privacy protection best practices for adopting and implementing encryption and WMATA's standards.

Recommendations

OIG recommends the GM/CEO:

5. Develop a phased, time-bound implementation strategy and plan to deploy and configure existing capabilities (e.g., [redacted], encryption tools) and other measures across all IT environments, including cloud services and OT systems.

Management Response

DM, in coordination with Business Operations, and non-DM Operational Technology (OT) partners, will develop and execute a **phased, timebound implementation plan** to strengthen data protection controls across the enterprise. This effort will address all

applicable environments, including on-premises systems, cloud services, and OT platforms.

The approach will focus on establishing clear priorities, sequencing, and accountability based on data sensitivity, risk, and operational impact.
Implementation will be conducted incrementally, beginning with higher-risk environments and expanding in subsequent phases to achieve broader enterprise coverage. This phased execution is intended to ensure alignment with operational realities while maintaining consistent enterprise standards.

The strategy will align with existing governance structures, approved enterprise capabilities, and ongoing corrective action activities, and will include defined milestones and progress tracking to support transparency and oversight. DM will continue to coordinate with relevant stakeholders to ensure requirements are applied consistently across organizational and technology boundaries.

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

6. After developing the strategy and plan to deploy and configure existing capabilities, implement an enterprise-wide policy, aligned with industry best practices, that mandates standardized practices, protocols, and oversight for all sensitive systems, irrespective of departmental ownership.

Management Response

DM agrees with this recommendation. Following the implementation and maturation of enterprise-sensitive data protection capabilities, Metro's Data Governance process will ensure that data owners across the organization are informed of their responsibilities under the Privacy Policy, Cybersecurity Policy, and data governance framework. Data owners will be required to either provide implementation schedules and timelines that align with business needs and Metro's risk tolerance for capabilities implemented by Digital Modernization (DM) or be trained and enabled to use approved self-service data protection capabilities, as appropriate. This approach ensures consistent application of enterprise protections while maintaining risk-based, operationally appropriate implementation.

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

7. Provide initial and refresher training to relevant staff, focusing on WMATA encryption technologies, requirements, and best practices, to ensure they are equipped to protect sensitive data.

Management Response

DM concurs. DMCS will develop and deliver a focused refresher for Cybersecurity and Digital Modernization staff on WMATA's encryption technologies, requirements, and best practices—covering selection, configuration, and validation of encryption for data at rest and in transit in Metro's hybrid environment. This training, separate from the Recommendation 1.h data privacy tool training, will be coordinated with WMATA Training, updated as capabilities are deployed, and aligned with enterprise data-handling standards and data-owner requirements as the Data Governance Board's functionality matures. Milestones and training adherence will be tracked in the appropriate CAP.

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

Audit Scope

The audit included reviewing and assessing WMATA's compliance with applicable data privacy standards and its own policy requirements.

Methodology

To achieve the audit objective, OIG performed the following:

- Reviewed and documented the organizational infrastructure responsible for managing and administering WMATA's compliance with data privacy laws, regulations, or standards.
- Reviewed relevant laws, regulations, policies, and procedures, as well as best practices and guidance, such as WMATA Policy Instructions, Privacy Policies and Procedures, and Standard Operating Procedures.
- Reviewed prior audits conducted by other OIG, Audit and Compliance, General Accountability Office, and other organizations.
- Reviewed relevant management recommendations, comments, and corrective actions.
- Conducted interviews with responsible management and staff.
- Conducted walkthroughs of relevant processes, operations, and practices to become familiar with administrative, operational, and management processes.

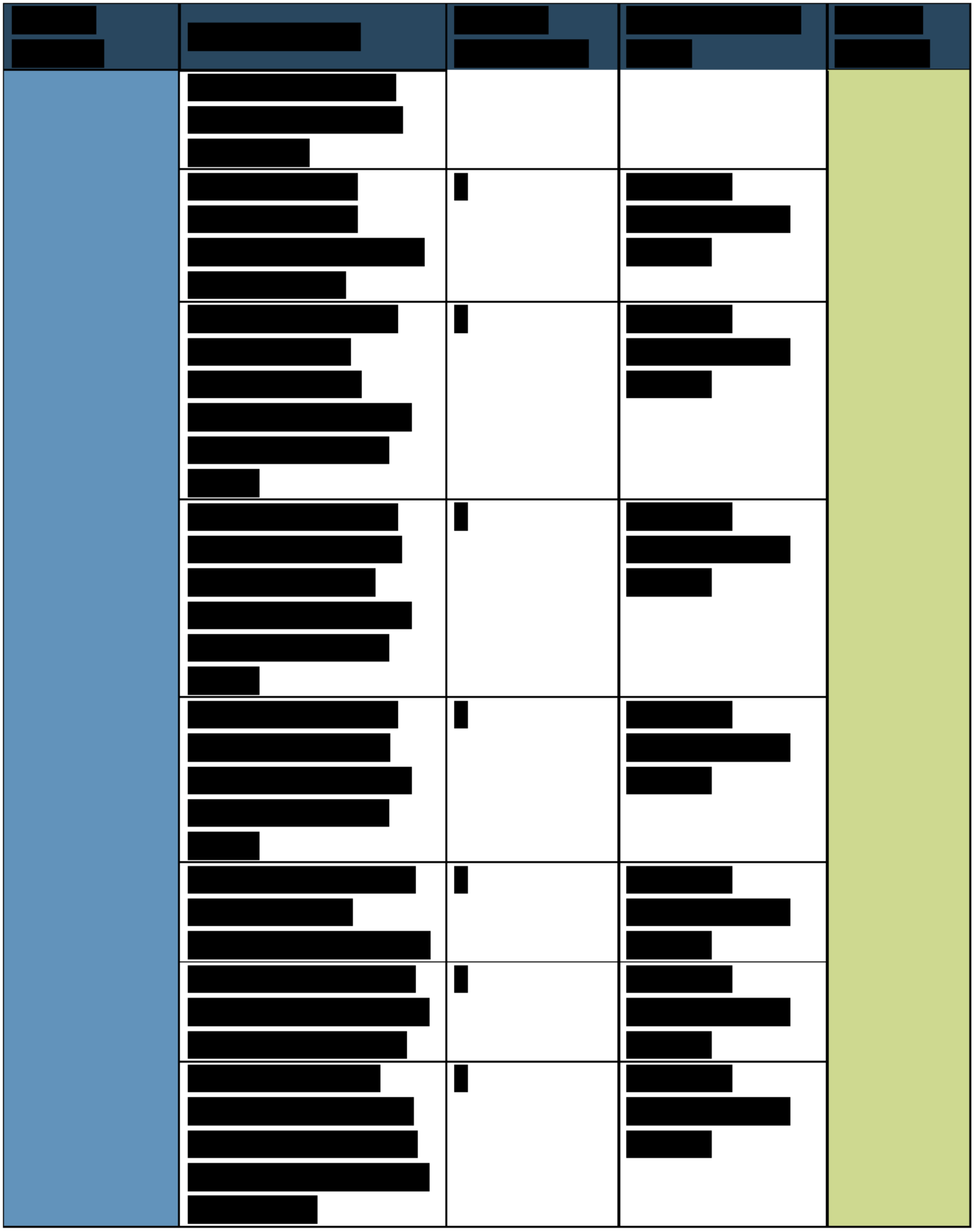
Generally Accepted Government Auditing Standards (GAGAS) Statement

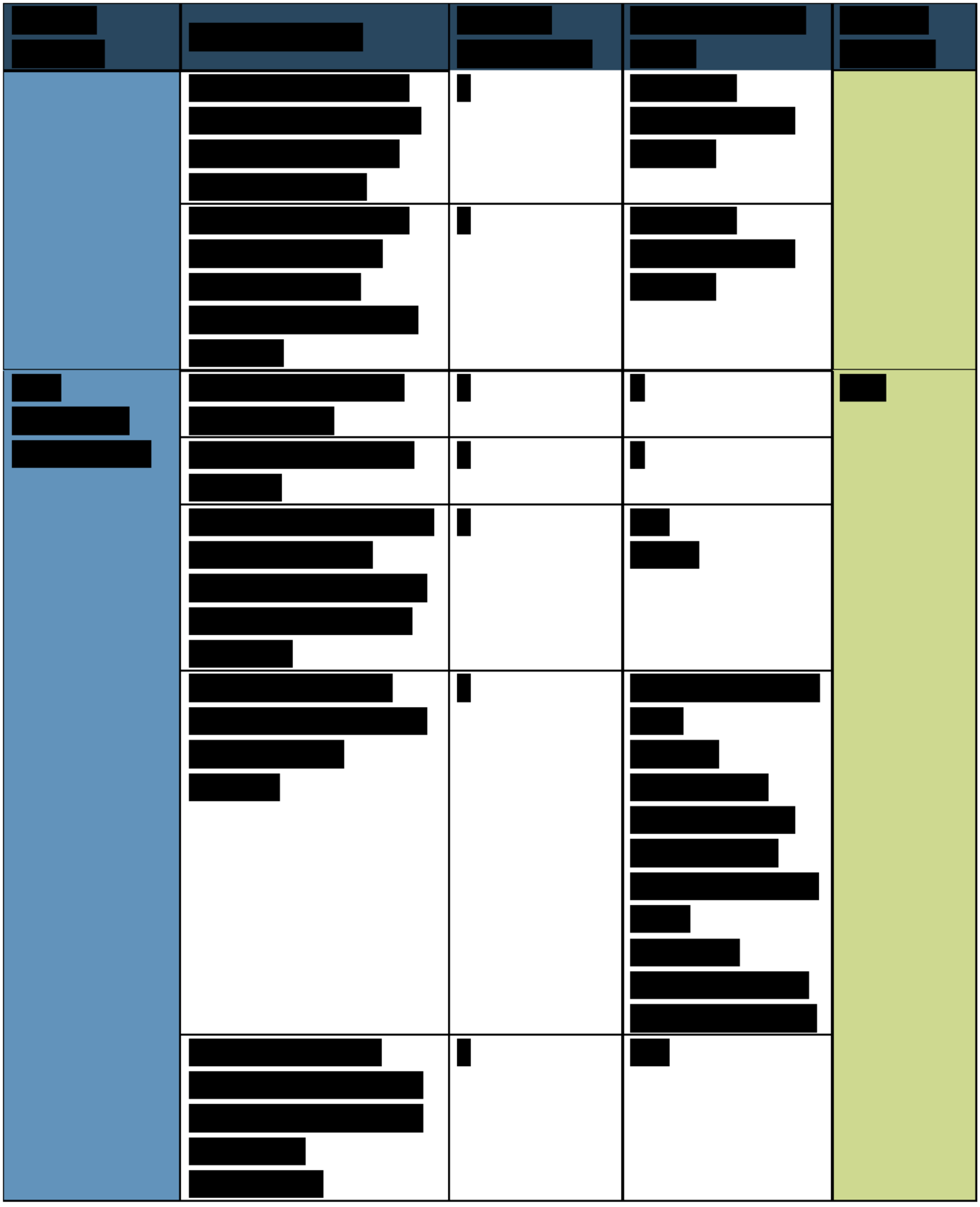
We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

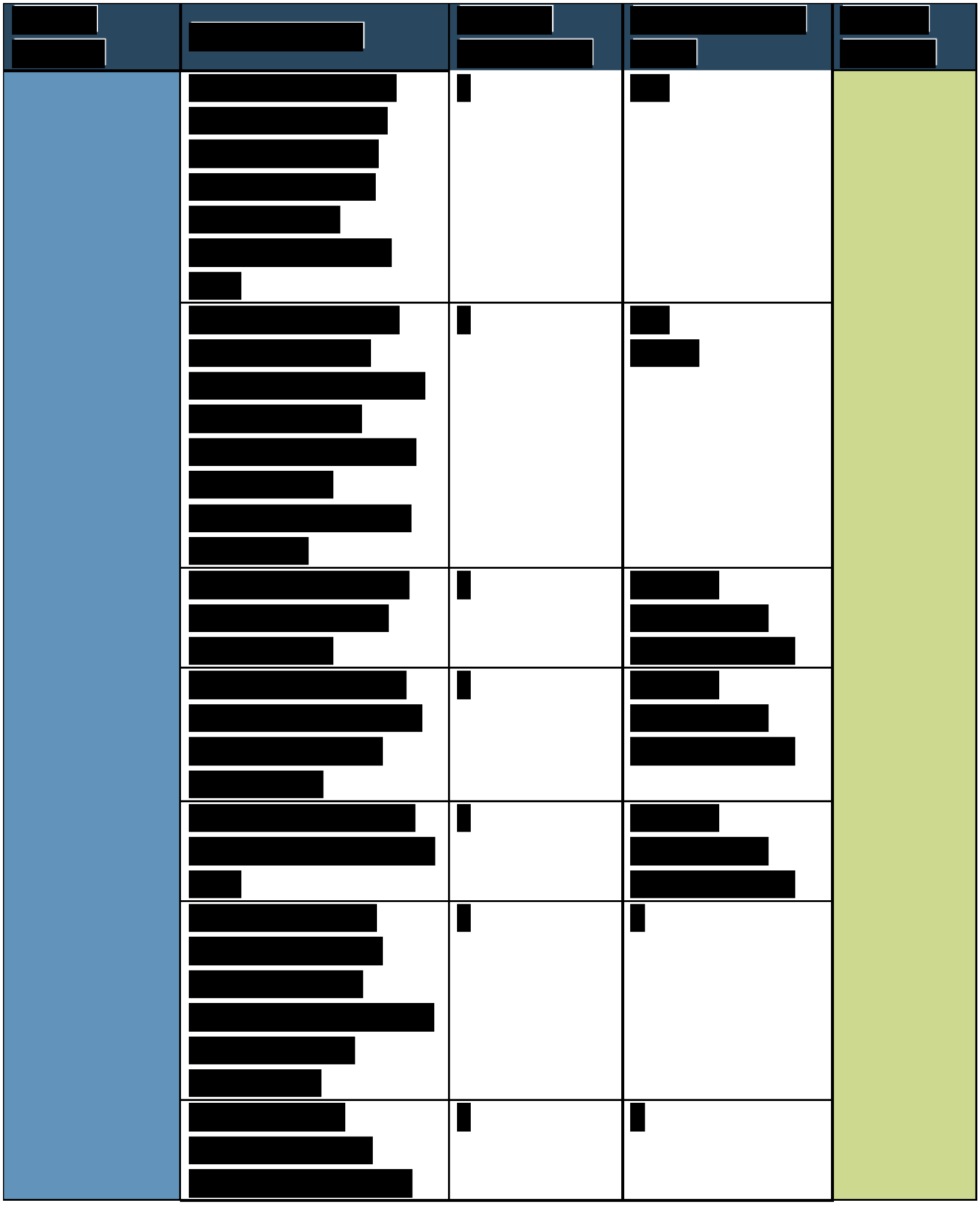
Table 1: Excerpt of DMCS's October 2024 Self-Assessment[17]

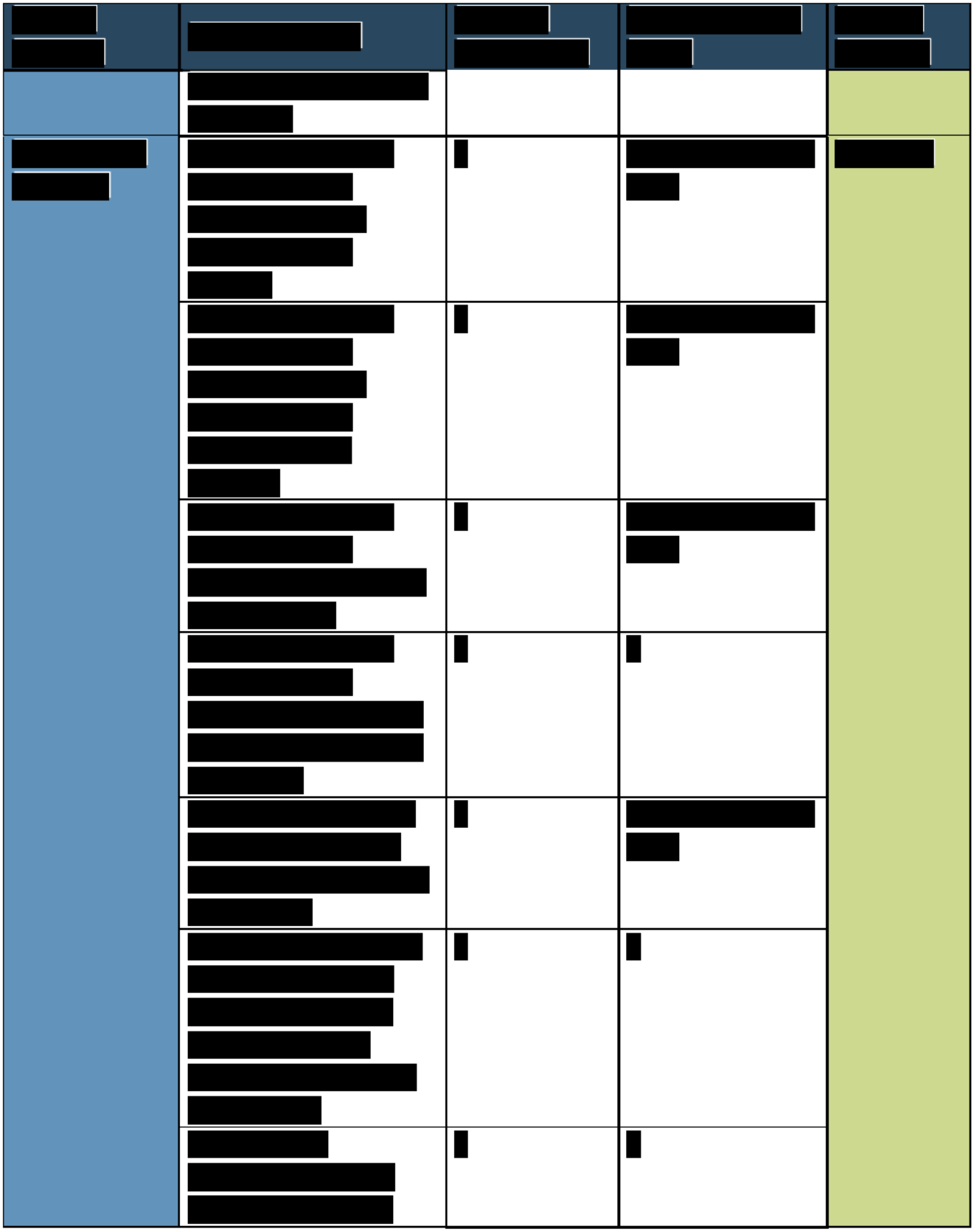
[17] *Excerpt from DMCS's October 2024, DMCS completed a self-assessment titled "Data Security Framework – Maturity Assessment*

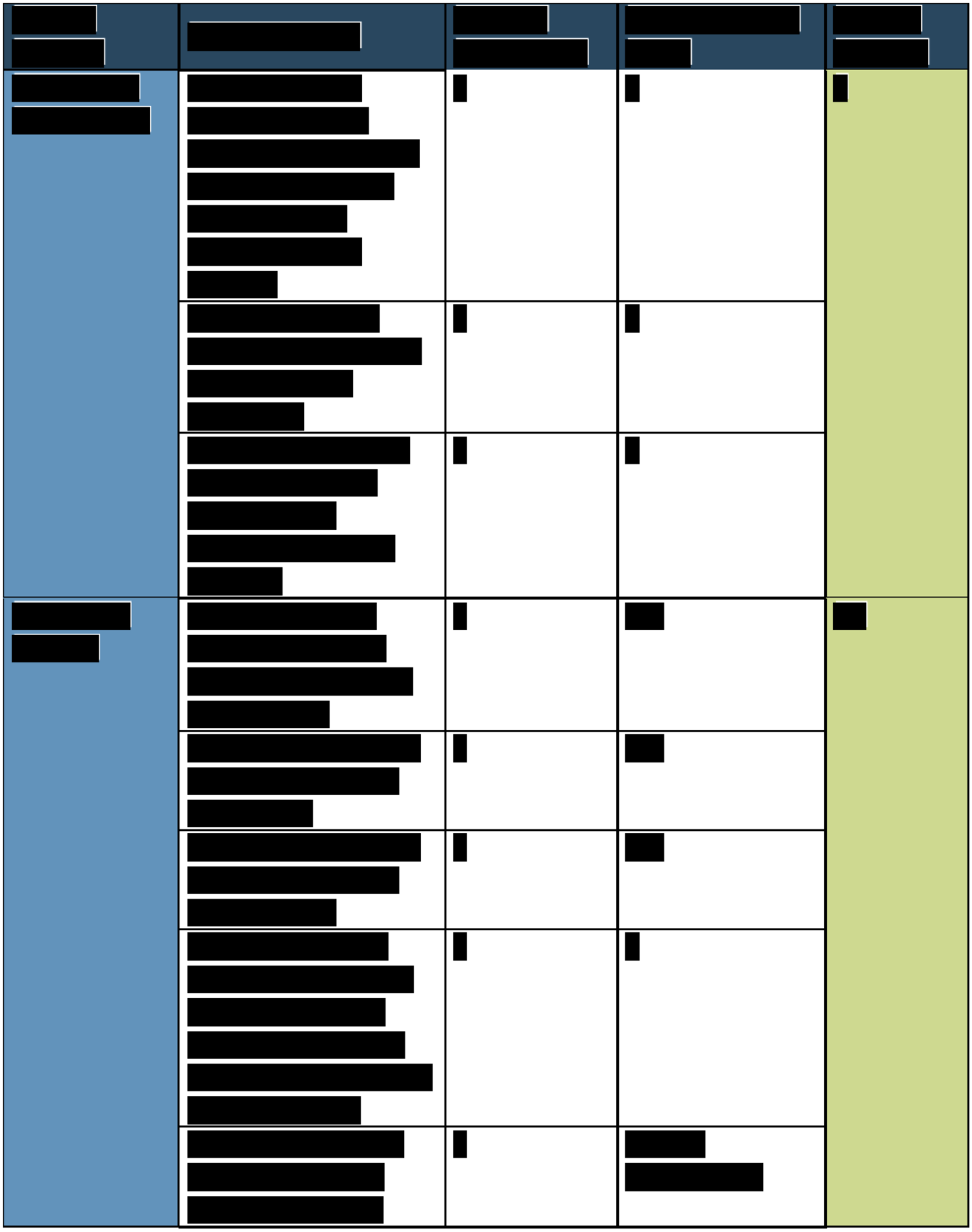
[18] *DMCS used a five-point maturity scale: 1 = Initial/Ad hoc, 2 = Developing, 3 = Defined, 4 = Managed and Measurable, 5 = Optimized.*

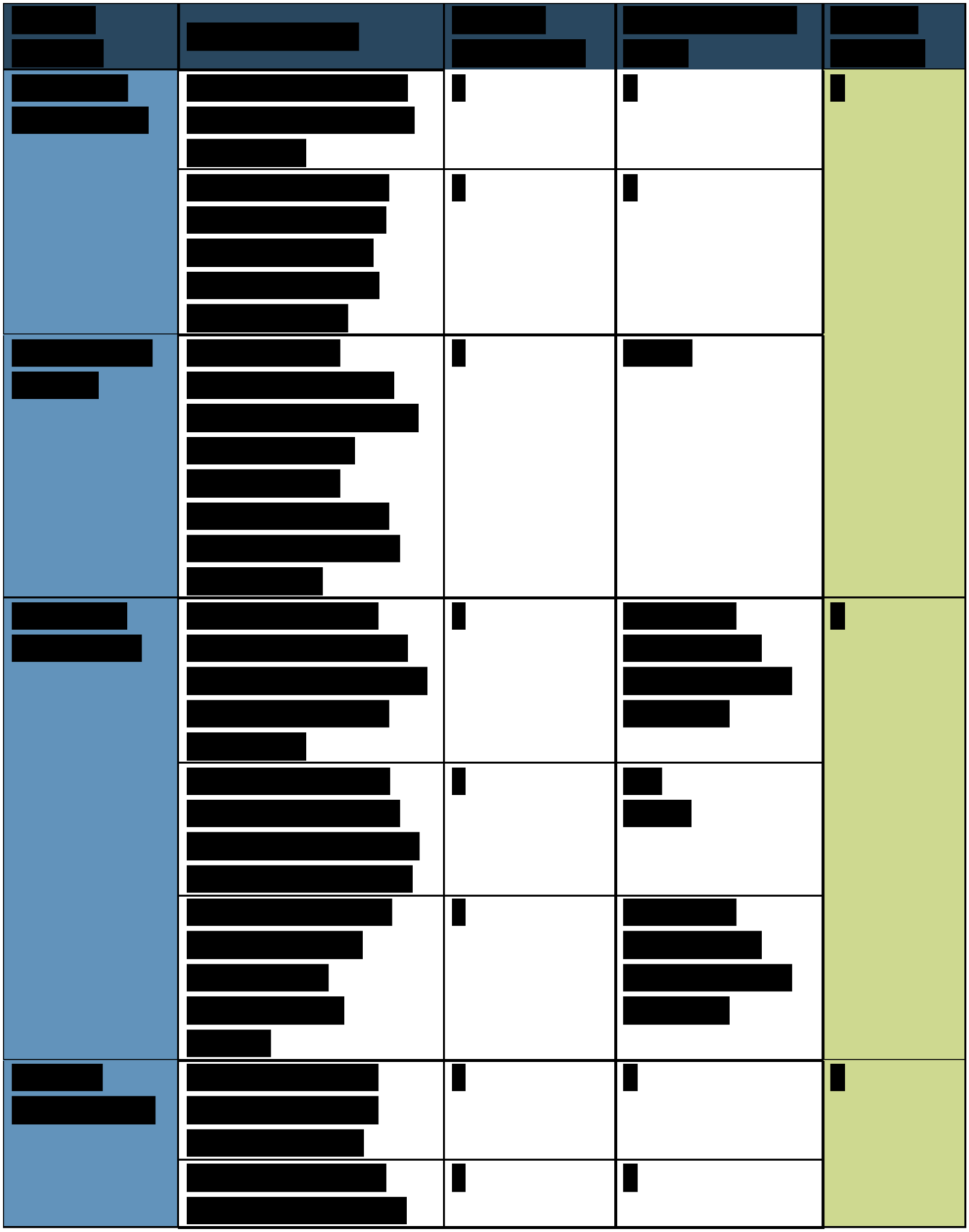


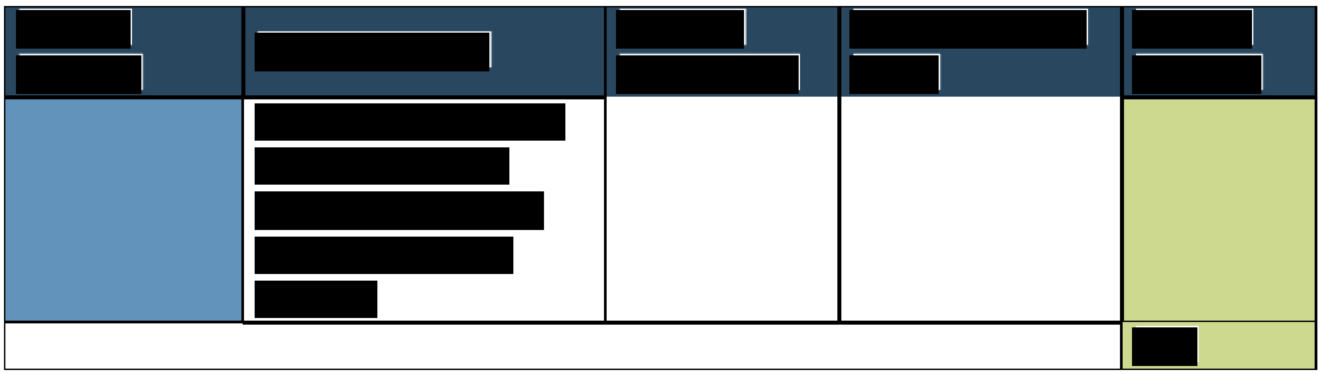












M E M O R A N D U M

SUBJECT: Audit of WMATA's Data Privacy Practices

DATE: March 27, 2026

FROM: Judd Nicholson – Executive Vice President and Chief Digital Officer

TO: Michele Zamarin – OIG

WMATA management has carefully reviewed the Office of Inspector General's (OIG) February 10, 2026, "Audit of WMATA's Data Privacy Practices'.

Finding 1 – WMATA's Data Privacy Posture Needs Improvement, and Practices Require Expansion

1. Develop and implement a formal enterprise-wide Data Privacy Program strategy and plan, with defined milestones, timelines, and performance metrics to achieve its target maturity level (e.g., NIST Tier 4), and at a minimum, address the following:

   a. Establishment of a senior-level position with authority, resources, and organizational positioning necessary to implement enterprise-wide privacy policies.

   Response:

   Digital Modernization (DM) concurs with this recommendation. WMATA intends to assign this role to a planned Governance Board responsible for enterprise data to consolidate and oversee enterprise data related functions within the (DM) organization. This emerging Governance Board will be coordinated by DM and comprised of senior-level individuals with representation from across the enterprise. The enterprise Data Privacy Program will be formally positioned under this Governance Board, with appropriate authority, organizational placement, and accountability to implement and enforce enterprise-wide data privacy policies and standards. The Governance Board will be responsible for coordinating privacy governance across DM, consistent with NIST best practices of accountability.

Washington Metropolitan Area Transit Authority

b. Development of a formal SSP, to formalize the baseline requirements outlined in the Manual.

Response:

DM agrees with this recommendation and appreciates the auditors' focus on strengthening WMATA's data privacy posture. DMCS is already developing and authorizing System Security and Privacy Plans (SSPPs) for major enterprise platforms and services under its ownership.

Consistent with NIST SP 800-37 Rev. 2 and NIST SP 800-53, an information system is defined as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." Accordingly, SSPPs are scoped to well-defined system boundaries and are developed collaboratively with data owners.

In alignment with this recommendation, DMCS has defined General Support System (GSS) 10 as the collection of tools and technologies used by Cyber to support data privacy and sensitive data protection. The system SSPP currently exists in RSA Archer and is undergoing control assessment and validation to ensure compliance and effectiveness.

Through the Governance Board (addressed in 1a), DMCS will continue coordinating with Metro stakeholders to formalize SSPPs where appropriate, including documenting existing controls and associated Plans of Action and Milestones (POA&Ms). Milestones for completion of GSS 10—and for the subsequent identification and documentation of sensitive data repositories across WMATA—will be coordinated with the appropriate stakeholders and incorporated into the Corrective Action Plan (CAP).

c. Development of data mapping and inventory practices, to catalog all systems, and an interim process for manual data mapping to gain immediate visibility into critical data flows.

Response:

DM concurs with this recommendation. The Enterprise Architecture Office is developing an Enterprise Information Repository (EIR) to establish a centralized, authoritative, and governed inventory of systems and data assets across the enterprise. The EIR will provide standardized visibility into system ownership, data sensitivity, and high-level data flows. As an interim measure to gain immediate visibility into

critical data flows, structured manual data mapping will be conducted for known systems while the EIR is incrementally implemented and expanded through a minimum viable- product (MVP) approach.

d. Implementation of a formal governance committee or structure with representatives from DM and OT leadership to create and mandate a unified set of data privacy and security controls for all OT systems.

Response:

DM concurs with this recommendation. DM will govern and maintain the Enterprise Inventory Repository (EIR) using formal data governance, data quality, and change management practices. Updates to the EIR will be mandated as part of the Change Control Board (CCB) approval process for system changes, and monitoring mechanisms will be used to identify- stale or incomplete records. This governance structure will support coordination between DM leadership and enable the consistent application of unified data privacy and security controls across all systems. (DM recommends combining 1a, 1c, and 1d into one CAP)

e. Inclusion of a strategy for automated data privacy tools and processes.

Response:

DM agrees with this recommendation. Metro has an approved and funded roadmap for Secure Foundation, a core component of the broader Digital Ecosystem strategy, and multiple related initiatives are already underway.

As part of this work, Metro is implementing protection measures that include automated Data Loss Prevention (DLP), controls for removable/USB storage, and capabilities to identify and monitor sensitive data. These efforts are currently in varying stages of implementation across the environment. To provide clear management tracking and visibility, Metro will create a corrective action plan (CAP) to consolidate and document the strategy, including relevant milestones, timelines, and accountable owners for these capabilities. Metro will use the CAP to monitor progress and report status through established governance mechanisms.

f. Development of a formal, ongoing privacy risk assessment process, integrated with best practices to proactively identify, assess, and prioritize data privacy risks across the entire enterprise, including both IT and OT environments.

Response:

DM concurs with this recommendation. DM has partnered with Audit and Compliance on this effort. The Risk & Business Advisory Services team will support management's efforts to establish a formal, ongoing privacy risk assessment process to strengthen the organization's enterprise-wide data privacy posture. This initiative will align with existing Enterprise Risk Management practices and support management's responsibilities to proactively identify, assess, and prioritize privacy risks across IT and OT environments.

g. Implementation of quality assurance and quality control processes to continuously monitor, validate, and audit the effectiveness of all deployed data privacy controls, policies, and tools. This includes defining metrics, conducting periodic reviews, and performing internal audits to ensure ongoing compliance and identify areas for improvement.

Response:

DM agrees with this recommendation. Audit and Compliance has agreed to provide independent assurance on data privacy compliance. These efforts will focus on supporting DM management's goal of identifying opportunities for improvement in data privacy-lane. The performance of any assessment has Data Privacy program dependencies that must happen before any reviews can be conducted.

h. Implementation of role-based data privacy training for personnel responsible for implementing technical controls (e.g., encryption, data labeling) and handling sensitive data.

Response:

DM agrees with this recommendation. DM, in partnership with Human Capital, will create role-based data privacy training for personnel responsible for implementing technical controls and handling sensitive data.

2. After developing a formal enterprise-wide data Privacy Program strategy and plan, implement unified policies, procedures, and processes for coordinating and communicating for all entities that share responsibility for disseminating and protecting sensitive data.

Response:

DM agrees with this recommendation. Based on the Board-approved enterprise-wide Privacy Policy, the Cybersecurity Policy, and the establishment of a Data Privacy Program, DM will implement the strategy and plan to ensure programmatic governance and consistency in securing our data assets. This will require several dependencies, consistent with a proper inventory of WMATA-wide data assets, data asset categorizations, and the appropriate processes and procedures that drive Metro-wide conformity. This approach will be a multi-year effort that will enable validity, unified alignment, and effective coordination with the relevant business owners across WMATA.

Finding 2 – DMCS Has Not Fully Implemented Comprehensive Enterprise-Wide Automated Security Solutions to Protect Vulnerable Data

3. Create a funded, time-bound project plan to achieve enterprise-wide deployment and configuration of automated data security tools that can (1) resolve, detect, and categorize sensitive information, (2) identify DLP vulnerabilities, (3) implement data sensitivity labeling protocols, and (4) enforce data encryption requirements enterprise-wide.

Response:

DM agrees with this recommendation and will establish a time-bound project plan to support a Metro-wide configuration and deployment of automated data security tools capable of categorizing sensitive information, detecting and resolving DLP vulnerabilities, implementing data sensitivity labeling protocols, and enforcing established data encryption requirements across Metro. Due to Metro's unique information technology environment, the deployment will be executed with a risk-based deployment, prioritizing our systems based on assessed criticality factors. DM feels this approach is the best method to address our legacy systems, operational technologies, cloud-based services, and third-party solutions. Coordination for enterprise-wide integration with data owners will occur through the Data Governance Board and other applicable stakeholders to sequence implementation in a manner consistent with mission and business needs.

4. Implement enterprise-wide automated DLP solutions fully to enforce existing policies and to monitor, control, and encrypt data transferred to removable storage devices to mitigate the identified risks.

Response:

DM agrees with this recommendation and will implement a DLP solution that fully enforces our existing policies, provides enhanced monitoring capabilities and greater control, and enables data encryption when transferred to removable storage devices. These actions are already in progress, as DM has been addressing these program gaps by integrating our USB control efforts into CAP 590. DM is already working to implement measures to restrict, monitor, and audit the use of removable media and storage devices. These strategic approaches will reduce the risk of unauthorized data transfers. These actions are consistent with the approach outlined in recommendation response 1e.

Finding 3 – Lack of Centralized Data Encryption Standards, Controls, and Enforcement

5. Develop a phased, time-bound implementation strategy and plan to deploy and configure existing capabilities (e.g., Microsoft Purview, encryption tools) and other measures across all IT environments, including cloud services and OT systems.

Response:

DM, in coordination with Business Operations, and non-DM Operational Technology (OT) partners, will develop and execute a **phased, timebound implementation plan** to strengthen data protection controls across the enterprise. This effort will address all applicable environments, including on-premises systems, cloud services, and OT platforms.

The approach will focus on establishing clear priorities, sequencing, and accountability based on data sensitivity, risk, and operational impact. Implementation will be conducted incrementally, beginning with higher-risk environments and expanding in subsequent phases to achieve broader enterprise coverage. This phased execution is intended to ensure alignment with operational realities while maintaining consistent enterprise standards.

The strategy will align with existing governance structures, approved enterprise capabilities, and ongoing corrective action activities, and will include defined milestones and progress tracking to support transparency and oversight. DM will continue to coordinate with relevant stakeholders to ensure requirements are applied consistently across organizational and technology boundaries.

6. After developing the strategy and plan to deploy and configure existing capabilities, implement an enterprise-wide policy, aligned with industry's best practices, that mandates standardized practices, protocols, and oversight for all sensitive systems, irrespective of departmental ownership.

   Response:

   DM agrees with this recommendation. Following the implementation and maturation of enterprise-sensitive data protection capabilities, Metro's Data Governance process will ensure that data owners across the organization are informed of their responsibilities under the Privacy Policy, Cybersecurity Policy, and data governance framework. Data owners will be required to either provide implementation schedules and timelines that align with business needs and Metro's risk tolerance for capabilities implemented by Digital Modernization (DM) or be trained and enabled to use approved self-service data protection capabilities, as appropriate. This approach ensures consistent application of enterprise protections while maintaining risk-based, operationally appropriate implementation.

7. Provide initial and refresher training to relevant staff, focusing on WMATA encryption technologies, requirements, and best practices, to ensure they are equipped to protect sensitive data.

   Response:

   DM concurs. DMCS will develop and deliver a focused refresher for Cybersecurity and Digital Modernization staff on WMATA's encryption technologies, requirements, and best practices—covering selection, configuration, and validation of encryption for data at rest and in transit in Metro's hybrid environment. This training, separate from the Recommendation 1.h data privacy tool training, will be coordinated with WMATA Training, updated as capabilities are deployed, and aligned with enterprise data-handling standards and data-owner requirements as the Data Governance Board's functionality matures. Milestones and training adherence will be tracked in the appropriate CAP.

cc: Senior Executive Team
Paula Cook – Acting VP & Chief Risk and Audit Officer

Report Fraud, Waste, or Abuse

Please Contact:

Email: hotline@wmataoig.gov

Website: wmataoig.gov/hotline-form/

Telephone: 1-888-234-2374

Facsimile: 1-800-867-0649

Address: WMATA
Office of Inspector General
Hotline Program
500 L'Enfant Plaza SW, Suite 800
Washington, DC 20024