OFFICE OF INSPECTOR GENERAL | UNITED STATES POSTAL SERVICE

Corporate Information Security Office Workforce

AUDIT REPORT

Report Number 22-194-R23 | September 29, 2023

Table of Contents

Cover

Highlights 1

- Background 1
- What We Did 1
- What We Found 1
- Recommendations 1

Transmittal Letter 2

Results 3

- Introduction/Objective 3
- Background 3
  - CISO Mission, Organization, and Strategic Goals 3
  - Workforce Planning Best Practices 4
- Finding Summary 4
- Finding #1: Corporate Information Security Office Workforce Planning 5
  - CISO Workforce, Position Descriptions, and Metrics 5
  - Workforce Plan 6
  - Recommendation #1 8
  - Recommendation #2 8
- Management's Comments 8
- Evaluation of Management's Comments 9

Appendices 10

- Appendix A: Additional Information 11
  - Scope and Methodology 11
  - Prior Audit Coverage 12
- Appendix B: Management's Comments 13

Contact Information 16

Highlights

Background

The U.S. Postal Service's Corporate Information Security Office (CISO) plays a pivotal role in safeguarding data and assets of one of the largest and most critical networks in the nation. The Postal Service network links more than 31,000 facilities and connects more than 653,000 employees and hundreds of systems for the efficient processing and delivery of mail to everyone living in the U.S. and its territories. Staffing challenges such as an increasing demand for cybersecurity professionals with a limited applicant pool and recruiting and retaining a skilled CISO workforce are crucial for the Postal Service to overcome and protect its network and information resources against evolving cyber threats. Effective workforce planning is essential to addressing these challenges.

What We Did

Our objective was to determine whether the CISO is adequately staffed by assessing recruitment, retention, and performance measurements. For this audit, we reviewed the CISO workforce and strategic staffing activities for fiscal year (FY) 2021 through FY 2023 and interviewed headquarters personnel.

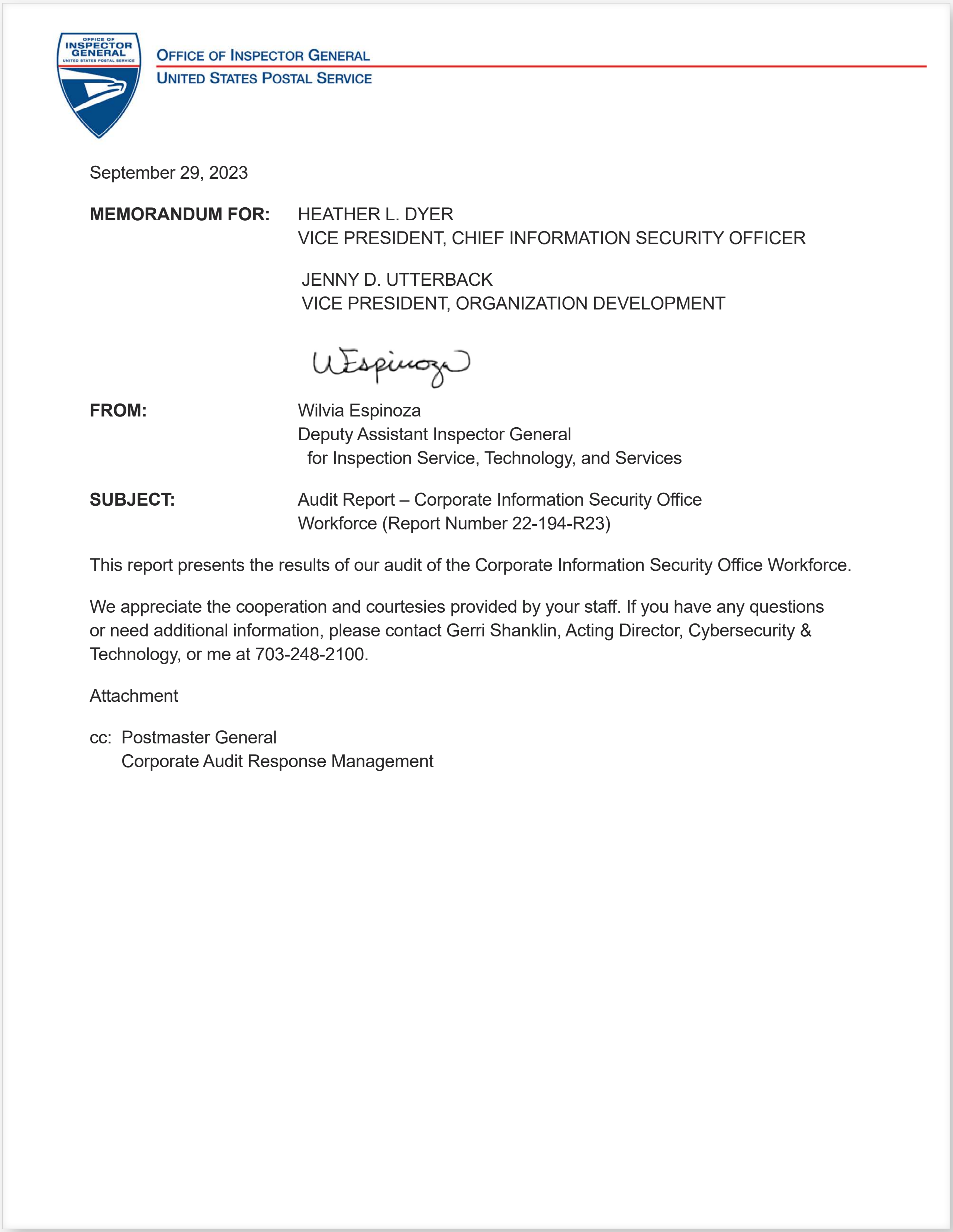
What We Found

Although the CISO workforce remained stable with low turnover in FY 2023, and while it maintains well-defined job roles and monitors some workforce related metrics, we could not determine whether the CISO is adequately staffed because the CISO leadership had not established necessary elements of an effective workforce planning process to ensure personnel are qualified to meet the organization's mission and strategic goals. Specifically, we found that the CISO leadership did not document key components of a workforce plan to ensure ongoing initiatives aligned to strategic goals, despite highlighting recruitment and retention as a goal in its five-year strategic plan. The CISO leadership did not believe there was a need for formal documentation of a workforce plan and stated that workforce planning information is documented in current strategic planning and budgeting activities. Additionally, the CISO leadership stated that they have the ability to determine when to continue or end workforce initiatives.

Recommendations

We recommended management establish and document a workforce plan and develop a process to track employee and contractor training and certifications to monitor progress toward addressing the skills gaps identified in periodic skills assessments.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

September 29, 2023

MEMORANDUM FOR: HEATHER L. DYER
VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER

JENNY D. UTTERBACK
VICE PRESIDENT, ORGANIZATION DEVELOPMENT

WEspinoza

FROM: Wilvia Espinoza
Deputy Assistant Inspector General
for Inspection Service, Technology, and Services

SUBJECT: Audit Report – Corporate Information Security Office Workforce (Report Number 22-194-R23)

This report presents the results of our audit of the Corporate Information Security Office Workforce.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Gerri Shanklin, Acting Director, Cybersecurity & Technology, or me at 703-248-2100.

Attachment

cc: Postmaster General
Corporate Audit Response Management

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the Corporate Information Security Office (CISO) Workforce (Project Number 22-194). Our objective was to determine whether the U.S. Postal Service's CISO is adequately staffed by assessing recruitment, retention, and performance measurements. See Appendix A for additional information about this audit.

Background

The Postal Service's CISO plays a pivotal role in safeguarding data and assets of one of the largest and most critical networks in the U.S. The Postal Service's network links more than 31,000 facilities and connects more than 653,000 employees and hundreds of systems for the efficient processing and delivery of mail to everyone living in the U.S. and its territories. In fiscal year (FY) 2022, the Postal Service processed on average 421.4 million mailpieces daily, including items such as medications, Social Security benefits and notices, and official mail sent from other federal agencies. Therefore, defending this critical infrastructure is vital to ensure reliable delivery of these important mailpieces. In light of an increasing demand for cybersecurity professionals, a limited applicant pool, and other staffing challenges, like the Great Resignation,[1] strategies for recruiting and retaining a skilled CISO workforce are crucial for the Postal Service to protect its information resources. Secure information resources are essential to efficient and reliable mail delivery and to defend against ever-evolving cyber threats.

CISO Mission, Organization, and Strategic Goals

The CISO, a sub-organization of the Chief Information Office (CIO), was established in 2015 to protect the Postal Service enterprise against an evolving cyberthreat landscape. The CISO's mission is to protect the Postal Service's employees, customers, network infrastructure, and information systems against present and future cybersecurity threats. In FY 2022, the CISO spent $165 million, of which [redacted] was used for contract support. As of May 2023, the CISO consisted of 423 personnel across five portfolios, of which 112[2] (26 percent) were Postal Service employees and 311[3] (74 percent) were contractors. The five portfolios within the CISO organization are outlined below and in Figure 1 by number of employees and contractors:

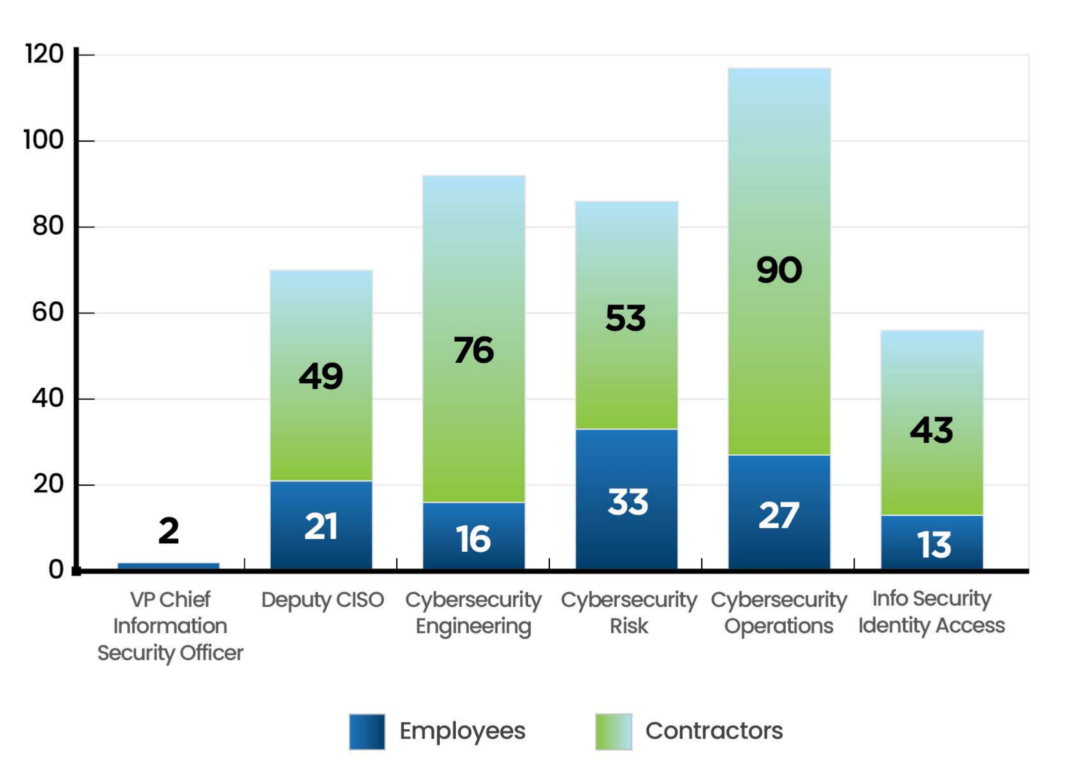
> “Strategies for recruiting and retaining a skilled CISO workforce are crucial for the Postal Service to protect its information resources.”

1. **The Deputy CISO** provides governance and oversight of the CISO and leads key enterprise-wide cybersecurity initiatives.
2. **Cybersecurity Engineering** manages processes and technology to protect Postal Service data, assets, and networks.
3. **Cybersecurity Risk Management** identifies and prioritizes risks, establishes security, and continuously monitors information, assets, and resources to protect the Postal Service network.
4. **Cybersecurity Operations** monitors cyber events and incidents that may potentially impact the confidentiality, integrity, and availability of Postal Service data and systems, keeping the organization's network safe.
5. **Info Security Identity Access** secures Postal Service workforce identities and access to resources; and provides identity verification services for Postal Service applications, customers, and federal partners.

[1] The elevated rate at which U.S. workers resigned from their jobs starting in the spring of 2021, amid strong labor demand, low unemployment, and coinciding with easing of the COVID-19 pandemic.
[2] Employee data extracted from the Human Capital Enterprise System, as of May 2023.
[3] Contractor employment data obtained from CISO, as of May 2023.

Figure 1. CISO Staffing as of May 2023

Source: United States Postal Service (USPS) CISO, USPS Human Resources, and eAccess Application System Reporting data obtained by USPS OIG.



The CISO's five-year strategic plan[4] for FY 2023 through FY 2027 includes "recruiting, investing in, developing, and retaining a skilled cybersecurity workforce" as one of its key goals and primary outcomes associated with accomplishing its strategies to strengthen the Postal Service's cybersecurity posture, protect its network, and support the Postal Service business. The CISO leadership works in coordination with other organizational units, such as the Business Services Organization, Human Resources (HR), Finance, and Supply Management to conduct contract worker oversight, external recruitment, and financial resource and budget management.

Workforce Planning Best Practices

Workforce planning is the process used to analyze an organization's workforce and determine actions needed to ensure its staff can support current and future business objectives. According to industry best practices, effective workforce planning includes managing immediate staffing needs; as well as considering internal and external factors such as workforce aging, labor/skill availability, and market trends to develop strategies and tactics to proactively manage talent. Workforce planning processes include, but are not limited to, recruitment, training and development, succession planning, performance evaluation, and contract staffing.[5] Further, a workforce plan should align with the organization's strategic plan and identify actions to overcome barriers to accomplish business goals.[6]

Finding Summary

The CISO workforce is stable, and the CISO has defined job roles and responsibilities that align with industry standards and began monitoring some workforce related metrics. However, we could not determine whether the CISO is adequately staffed because the CISO leadership had not established necessary elements of an effective workforce planning process to ensure personnel are qualified to meet the organization's mission and goals. While the CISO identified the goal of "recruiting, investing in, developing, and retaining a skilled cybersecurity workforce" as a desired outcome associated with accomplishing its five-year strategic plan, the plan

[4] *USPS CISO Cybersecurity Strategic Plan FY 2023-2027.*
[5] Hewertson, R.B. *6 Steps to Implementing a Workforce Planning Change Process.* https://blog.shrm.org
[6] *Workforce Planning Guide*, U.S. Office of Personnel Management, November 2022.

did not include specific actions to accomplish this strategy, resulting in initiatives that appear reactive in nature rather than proactive in planning for future needs.

Finding #1: Corporate Information Security Office Workforce Planning

The CISO workforce remained stable from October 2022 through July 2023, the CISO's position descriptions aligned with industry standards, and the CISO leadership began monitoring some workforce related metrics. However, we found that the CISO leadership did not document key components of a workforce plan to ensure ongoing initiatives aligned to strategic goals.

> "The CISO employee turnover rate from October 2022 through July 2023 was lower than the national average."

CISO Workforce, Position Descriptions, and Metrics

According to workforce data provided by HR, the CISO employee turnover rate from October 2022 through July 2023 was 2.8 percent. This is lower than the national average during the same timeframe, which peaked at 3.9 percent. This is also an improvement from recent years, where CISO turnover was 19.5 percent in FY 2021 and 7 percent in FY 2022. The national averages in FYs 2021 and 2022 were 4.1 percent and 4.2 percent, respectively.

In addition, the CISO maintains defined categories for employee roles in which employee job descriptions are grouped. These categories outline expectations, competencies, and recommended certifications for personnel across all CISO functional areas. We reviewed CISO job descriptions within these categories and determined they were aligned with industry standards.

Furthermore, the CISO conducted a skills assessment[7] for all CISO employees and contractors in summer 2022, which identified the top five skills with gaps, skills recommended for training, and skills in which staff felt proficient, but the program manager felt needed improvement. (see Figure 2.) The CISO recommended internal and external training as a strategy to improve the identified skills gaps and the results of this assessment contributed to the development of the job categories highlighted above that align positions with required competencies.

We also found HR maintains a dashboard[8] for workforce staffing data that provides various reports in areas such as recruitment, retention, and separation metrics; attrition rates; and results of employee stay[9] and exit interviews, which are available to all components across the Postal Service.[10] During our audit, the CISO began incorporating some of this workforce data into their on-going monitoring activities. For example, the CISO leadership stated they began using HR dashboard data to track employee turnover during the first quarter of FY 2023 and vacancies as of March 2023. The CISO leadership stated they monitor employee turnover rates to ensure they remain stable and track vacancy data to analyze the time taken to fill open positions.

[7] The skills assessment included a survey of 225 staff across all five CISO portfolios. Staff completed a self-assessment for skills deemed high value. Program managers reviewed these self-assessments and provided their input based on whether they thought the staff member needed to improve in a skill.
[8] This dashboard allows data filtering and analysis for individual Postal Service organizational units.
[9] Stay interviews are one-on-one conversations between an employee and their manager on topics that are most concerning to the employee.
[10] Exit interviews are ways for employers to learn why employees are ending their time with the agency.

Figure 2. CISO's Summer 2022 Skills Assessment Results

Top Five Skills Gaps

- Skill in preparing justifications and business cases for recommendations on cybersecurity initiatives.
- Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
- Knowledge of understanding cybersecurity trends and threats.
- Skill in utilizing time management to meet deadlines and milestones.
- Skill in anticipating potential obstacles and risks to a plan and developing alternative solutions.

Top Skills Recommended for Training

- Skill in managing day to day activities of externally sourced resources.
- Knowledge of understanding cybersecurity trends and threats.
- Skill in applying knowledge of privacy regulations, unified customer experience, behavior analytics and security considerations while designing Identity and Access Management solutions.
- Skill in preparing and presenting briefings.
- Skill in recognizing and categorizing types of vulnerabilities and associated attacks.

Skills Misalignment Between Staff and Program Managers

- Skill in anticipating potential obstacles and risks to a plan and developing alternative solutions.
- Excellent oral and written communication skills.
- Skill in analyzing security findings, issues, and plans.
- Skill in discerning the protection needs (i.e., security controls) of information systems and networks.
- Skill in translating technical findings to non-technical employees.

Source: USPS CISO, Skills Assessment Key Findings.

Workforce Plan

While CISO's position descriptions met industry standards, the CISO leadership has not documented a workforce plan that aligns the workforce with the CISO's strategic goals. In FY 2022, the Postal Service identified several strategic risks that could affect its cybersecurity workforce, to include:

> "While CISO's position descriptions met industry standards, the CISO leadership has not documented a workforce plan that aligns the workforce with the CISO's strategic goals."

- **Talent and Staff Bench Strength Risk** – the risk that the talent pool is not deep enough to absorb staff departures.
- **Benefits and Compensation Risk** – the risk that pay and benefit policies are not flexible enough to retain high achieving staff and lack some of the benefits of private companies or other government agencies.
- **Cybersecurity Risk** – the risk that the company fails to adequately protect the confidentiality, integrity, and availability of the Postal Service's information (data or programs), which may result in unauthorized knowledge and use of confidential information.
- **Information Technology Infrastructure/ System Failure Risk** – the risk of not having the information technology personnel infrastructure needed to effectively support current and future business needs.

A documented workforce plan should identify strategies to mitigate these risks.

During our audit, we found references to a 2017 CISO Workforce Plan in several Postal Service documents.

However, the current CISO leadership could not locate a copy of this plan and has not leveraged previously established strategies. As a result, the CISO does not have a documented workforce plan that:

- Provides recruitment and retention strategies to attract and retain qualified talent. While the CISO and HR leadership coordinated on several recruitment and retention initiatives to attract cybersecurity talent, resulting in low turnover rates over the past nine months, having documented strategies that can be replicated and built upon would provide assurance to the organization that its efforts align to its strategic plan.
- Defines roles and responsibilities for the coordination of the workforce strategies documented in the plan, including continuity of duties during staffing changes and coordination with other organizational units.
- Defines a process for periodic reviews and updates.

> “Although CISO made efforts to identify skills gaps and provided recommendations to improve these skills, there is no documented methodology for performing a thorough workforce analysis to monitor progress toward addressing these gaps.”

Although CISO made efforts to identify skills gaps and provided recommendations to improve these skills, there is no documented methodology for performing a thorough workforce analysis to monitor progress toward addressing these gaps. Further, CISO was unable to provide evidence of additional skills assessments performed that could provide insight into the progress made in closing these gaps. For example, the CISO leadership stated a previous CISO hired a consultant to conduct a workforce skills assessment but could not find or provide this assessment during our review.

We also found the CISO leadership does not track progress toward addressing key CISO skills gaps for its employees and contractors. For example, the skills assessment conducted across all CISO employees and contractors identified gaps in recognizing and categorizing types of vulnerabilities and associated attacks as well as knowledge of understanding cybersecurity trends and threats. CISO management recommended internal and external training to address these gaps. The CISO leadership stated that they provide reimbursement for certification exams, but do not follow up to determine whether the employees passed or failed. Additionally, the CISO leadership does not track employee training pursued independently by the employees. Further, contractor training and certifications are not monitored or tracked. Without this information, the CISO leadership is limited in their ability to monitor progress made toward employees and contractors understanding vulnerability gaps, cybersecurity trends, and threats.

The CISO leadership did not believe there was a need for formal documentation of a workforce plan and stated that workforce planning information is documented in current strategic planning and budgeting activities. While the strategic plan outlines the goal of “recruiting, investing in, and retaining a skilled cybersecurity workforce,” it lacks a concrete plan for achieving this goal. Additionally, the CISO leadership stated that they have the ability to determine when to continue or end workforce initiatives.

In 2015, the OIG issued a report highlighting deficiencies with the CISO’s employee-to-contractor staffing ratio, pay bands, and training for cybersecurity staff that limited its ability to perform critical functions to protect the Postal Service network.[11] Although we did not identify a staffing challenge from October 2022 through July 2023,

[11] *U.S. Postal Service Cybersecurity Functions*, Report Number IT-AR-15-008, dated July 17, 2015.

having a documented workforce plan will help identify recruitment and retention measures if the stability of the workforce begins to decline. A documented plan and strategy will provide the CISO with agreed-upon actions to mitigate unforeseen challenges.

According to best practices,[12] an organization should establish and maintain a strategic workforce plan to guide its workforce practices and activities. U.S. Office of Personnel Management guidance states that workforce planning should align human capital needs directly to the agency's strategic plan, identify current and future staffing gaps, and use data to make workforce decisions and recommendations. A workforce plan is generally long term (2-3 years) in focus and includes a workforce analysis along with the intended actions for areas such as position classification, position management, workforce design, recruiting, and hiring. Skills gap assessments are just one element of a workforce analysis. These assessments should also include a review of whether an agency has enough individuals to complete its work and a review of staff demographics, such as years of service, retirement eligibility, and the impact key staff turnover will have in the organization's ability to deliver key services.[13] In addition, best practices state the workforce plan should identify groups responsible for different strategic workforce planning activities and a schedule to periodically review and revise the plan.[14]

Without a formal workforce plan that addresses the CISO strategic priorities and immediate and long-term staffing needs, the CISO risks not adequately preparing for changes to future skills requirements and talent availability. Further, without formally documenting workforce plan responsibilities, performance goals, and expectations for periodic review and updates, the CISO risks inconsistent execution of workforce activities, particularly in times of transition between management.

Recommendation #1

We recommend the **Vice President, Chief Information Security Officer**, in coordination with the **Vice President, Organization Development**, establish and document a workforce plan that describes key recruitment, retention, and performance measurement activities. At a minimum, the plan should address strategic priorities, include workforce goals and objectives, identify stakeholder roles and responsibilities, and define a process for periodic review and updates.

Recommendation #2

We recommend the **Vice President, Chief Information Security Officer**, develop a process to track employee and contractor training and certifications to monitor progress toward addressing the skills gaps identified in periodic skills assessments.

Management's Comments

Management disagreed with the finding and recommendations 1 and 2.

Regarding the finding, management stated they disagree with the OIG's conclusion that, despite low turnover, the CISO does not have a workforce plan. Additionally, management stated in terms of recruitment and retention, the CISO workforce remained stable with low turnover in FY 2023, compared to previous years. Management further stated that their current recruitment and retention strategies are effective and the OIG provided no information to support its conclusion. Therefore, management asserts that the OIG should have concluded that the CISO was adequately staffed and the OIG's conclusion that the CISO does not have a workforce plan is unrelated to the audit objective and planned assessment methods.

Regarding recommendation 1, management stated the OIG did not identify any deficiencies in CISO staffing in this audit. Management further stated that establishing and documenting a workforce plan would add to the workload of the CISO leadership with no discernable benefit. Management stated that there does not appear to be a need to develop a documentation-based plan as it would be too high level and not impact or change current processes.

[12] Curtis, B., Hefley, W.E., & Miller, S.A. (July 2009). People Capability Maturity Model (P-CMM) Version 2.0, Second Edition. Carnegie Mellon University Software Engineering Institute. https://doi.org/

[13] *Workforce Planning Guide*, U.S. Office of Personnel Management, November 2022.

[14] Curtis, B., Hefley, W.E., & Miller, S.A. (July 2009). People Capability Maturity Model (P-CMM) Version 2.0, Second Edition. Carnegie Mellon University Software Engineering Institute. https://doi.org/

Regarding recommendation 2, management stated the OIG did not identify any deficiencies in CISO staffing. Management further stated that developing a process to track employee and contractor training and certifications to monitor progress toward addressing the skill gaps identified in periodic skills assessments would add to the workload of the CISO leadership with no discernable benefit.

See Appendix B for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management comments nonresponsive to the recommendations in the report and will pursue concurrence through the formal audit resolution process.

Regarding finding 1, we identified that the CISO leadership ensured its workforce remained stable during FY 2023, defined job roles and responsibilities that aligned with industry standards, and began monitoring some workforce related metrics. However, as stated in the report, the CISO workforce turnover rates fluctuated significantly compared to national averages for FYs 2021 and 2022. Additionally, the CISO leadership does not track progress toward addressing key skills gaps for its employees and contractors. A documented workforce plan should identify strategies to mitigate these risks.

Regarding recommendation 1, we could not determine whether CISO was adequately staffed because the CISO leadership had not established necessary elements of an effective workforce planning process to ensure personnel are qualified to meet the organization's mission and strategic goals. Without a formal workforce plan that addresses the CISO strategic priorities and immediate and long-term staffing needs, the CISO risks not adequately preparing for changes to future skills requirements and talent availability.

Regarding recommendation 2, the CISO identified significant skills gaps for its employees and contractors. However, the decentralized and reactive approaches employed by management place the organization at risk of not having the skills to meet its strategic needs.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. All recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

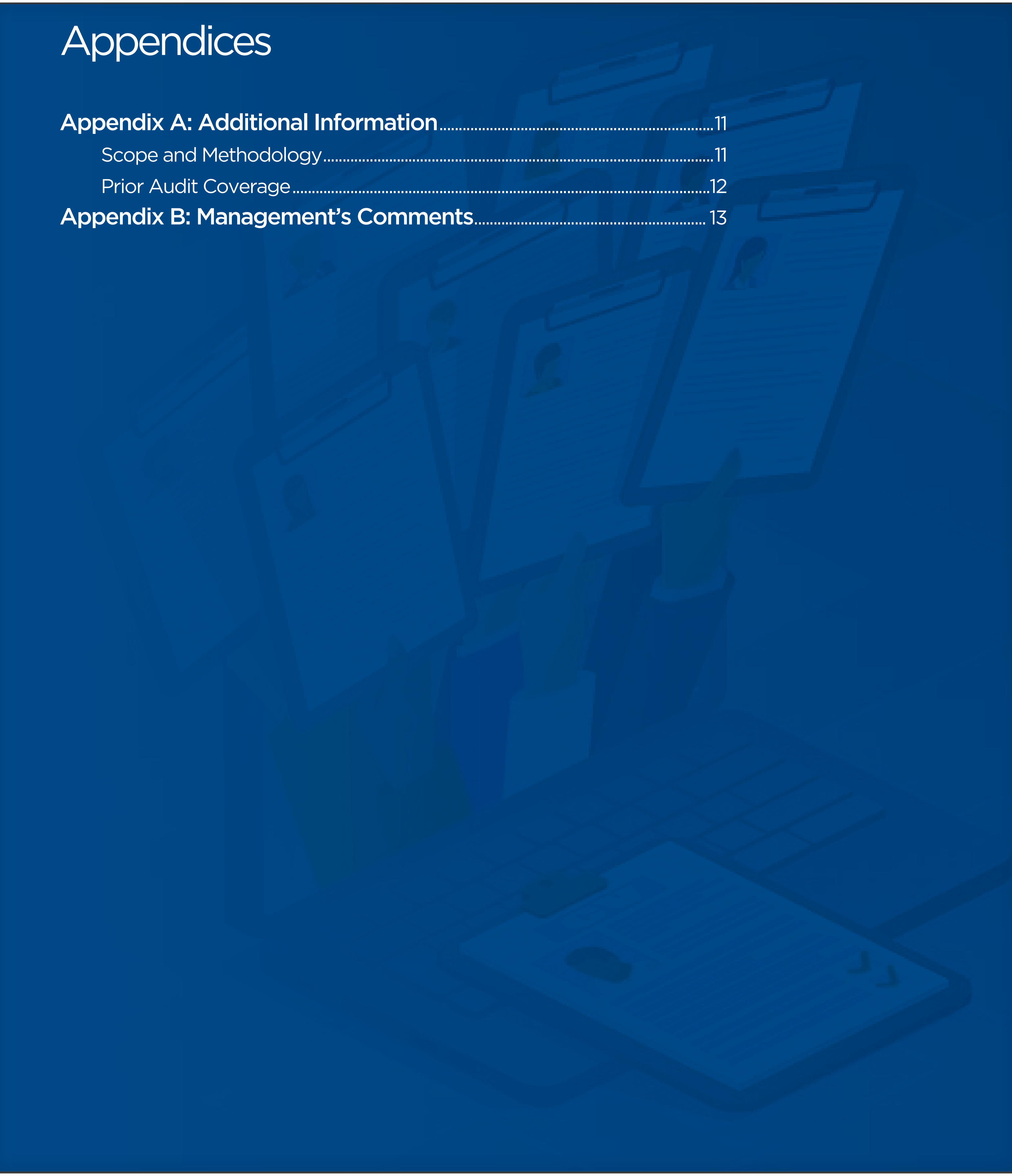
Appendices

Appendix A: Additional Information 11

Scope and Methodology 11

Prior Audit Coverage 12

Appendix B: Management's Comments 13



Appendix A: Additional Information

Scope and Methodology

The scope of our audit included an analysis of the CISO resources from FY 2021 through FY 2023. To accomplish our objective, the audit team:

- Reviewed CISO workforce policies, procedures, regulations, laws, studies, and best practices to gain an understanding of the requirements related to recruitment, retention, and performance measurements.
- Reviewed the CISO structure, CISO positions, and its summer 2022 skills assessment.
- Analyzed employee and contractor data.
- Interviewed personnel to gain an understanding of the components of the CISO workforce, and the oversight and management of contract employees.

We conducted this performance audit from October 2022 through September 2023 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on August 30, 2023, and included their comments where appropriate.

In planning and conducting the audit, we obtained an understanding of the CISO workforce internal control structure to help determine the nature, timing, and extent of our audit procedures. We reviewed the management controls for overseeing the program and mitigating associated risks. Additionally, we assessed the internal control components and underlying principles, and we determined that the following five components were significant to our audit objective: control environment, risk assessment, control activities, information and communication, and monitoring.

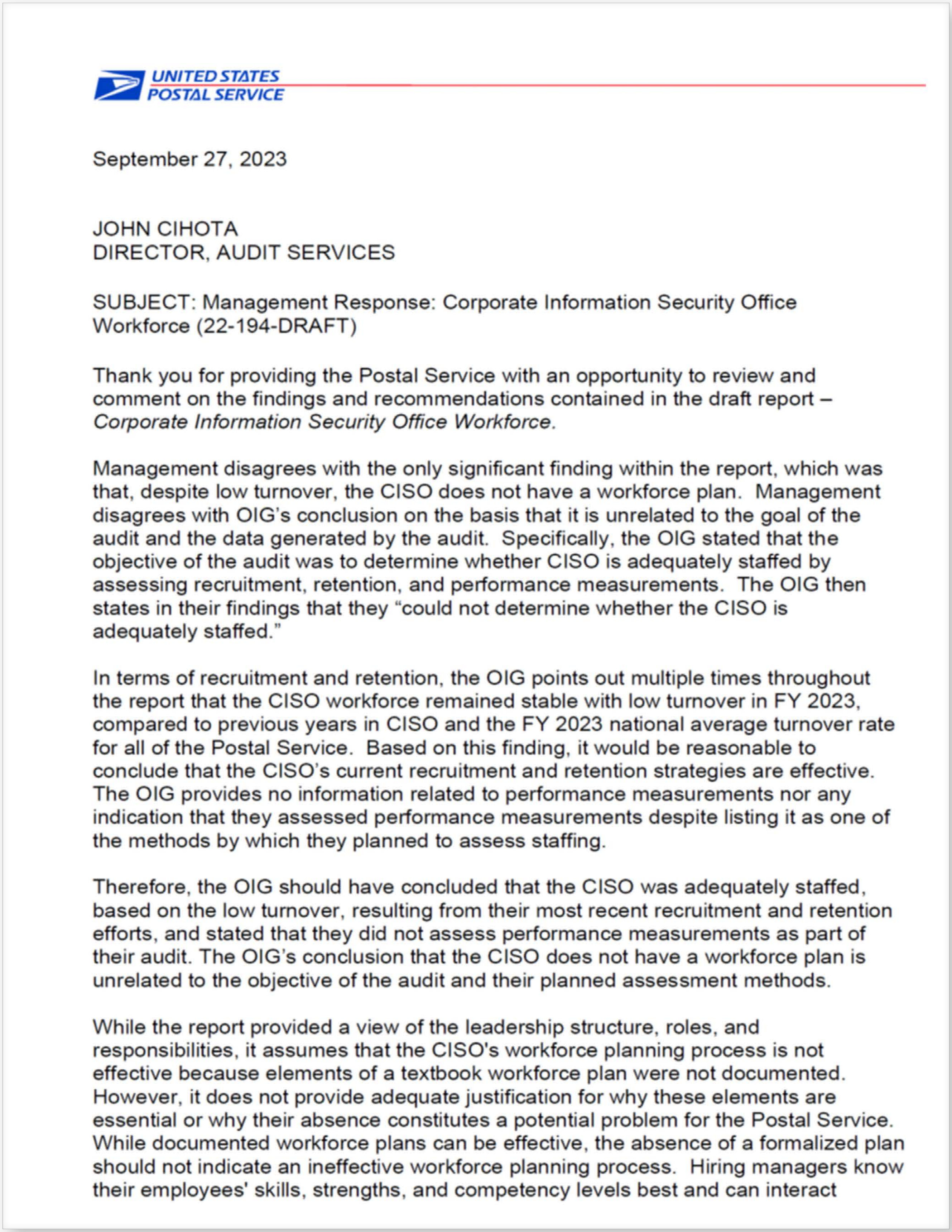
We developed audit work to ensure that we assessed these controls. Based on the work performed, we identified internal control deficiencies related to control activities and monitoring that were significant within the context of our objectives. Our recommendations, if implemented, should correct the weaknesses we identified.

We assessed the reliability of computer-generated data by analyzing and reviewing the raw data, comparing automated and manual data to supporting documents or systems, and interviewing personnel knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

Report Title	Objective	Report Number	Final Report Date	Monetary Impact (in millions)
Postal Service's Non-Career Employee Turnover Follow-Up	Assess the Postal Service's ongoing actions to reduce non-career employee turnover rates.	22-180-R23	4/18/2023	$52.1
Contractor – Labor Qualifications	Determine whether costs incurred by the Postal Service, as they relate to contractor employee labor qualifications for paid invoices, conform to contract requirements.	22-160-R23	3/24/2023	$5.9
U.S. Postal Service Knowledge Continuity	Determine whether the Postal Service ensured that it did not lose critical knowledge when employees transferred within or left the organization (due to retirement, resignation, reduction in force, or other reason).	21-255-R22	5/27/2022	$0
First-Line Supervisor Recruitment and Retention	Assess whether the Postal Service is effectively hiring and retaining first-line supervisors.	19SMG008HR000-R20	4/13/2020	$16.4
Effectiveness of the Postal Service's Efforts to Reduce Non-Career Employee Turnover	Assess the Postal Service's effectiveness in reducing non-career employee turnover and evaluate underlying reasons for non-career employee turnover.	19POG001SAT000-R20	2/12/2020	$13.7

Appendix B: Management's Comments



UNITED STATES POSTAL SERVICE

September 27, 2023

JOHN CIHOTA
DIRECTOR, AUDIT SERVICES

SUBJECT: Management Response: Corporate Information Security Office Workforce (22-194-DRAFT)

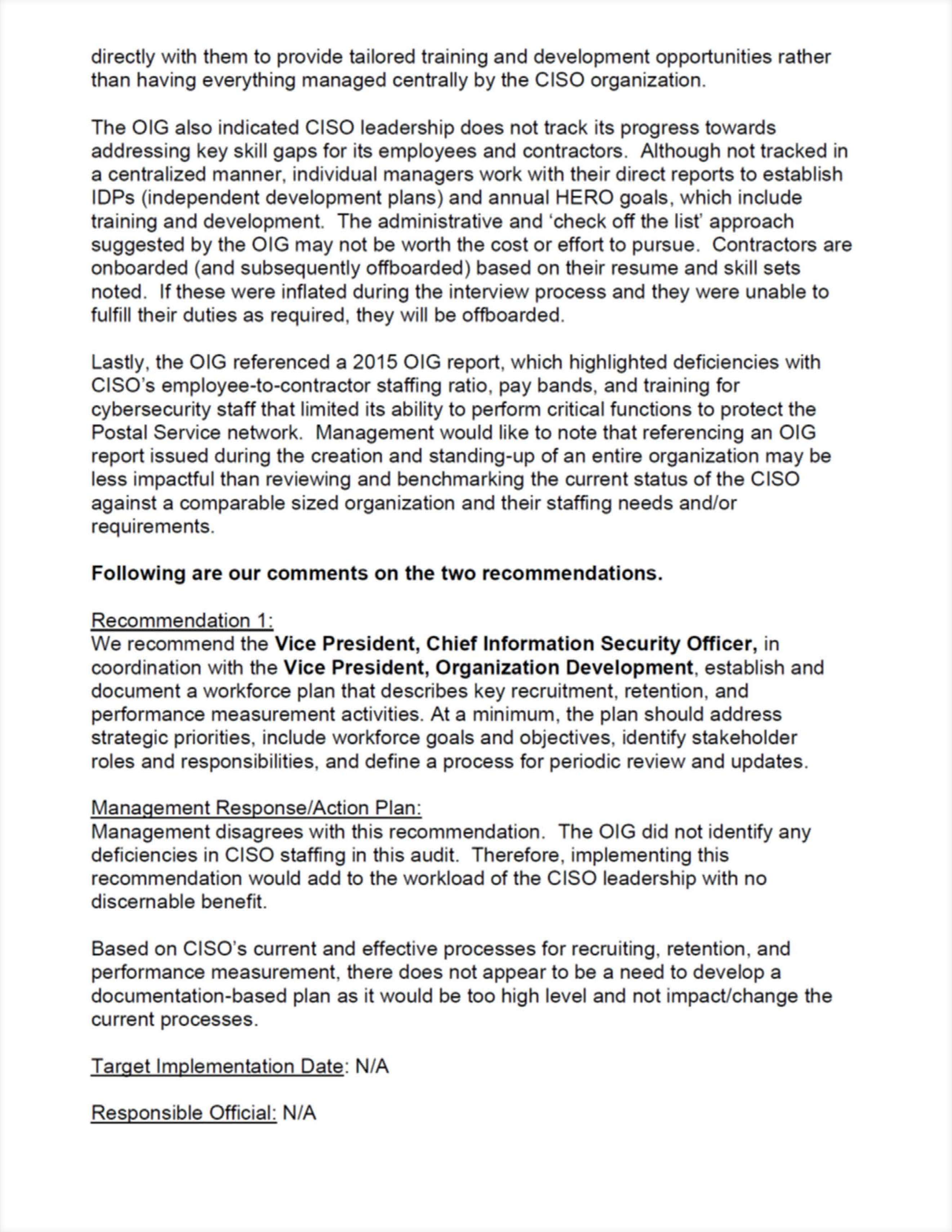
Thank you for providing the Postal Service with an opportunity to review and comment on the findings and recommendations contained in the draft report – *Corporate Information Security Office Workforce*.

Management disagrees with the only significant finding within the report, which was that, despite low turnover, the CISO does not have a workforce plan. Management disagrees with OIG's conclusion on the basis that it is unrelated to the goal of the audit and the data generated by the audit. Specifically, the OIG stated that the objective of the audit was to determine whether CISO is adequately staffed by assessing recruitment, retention, and performance measurements. The OIG then states in their findings that they "could not determine whether the CISO is adequately staffed."

In terms of recruitment and retention, the OIG points out multiple times throughout the report that the CISO workforce remained stable with low turnover in FY 2023, compared to previous years in CISO and the FY 2023 national average turnover rate for all of the Postal Service. Based on this finding, it would be reasonable to conclude that the CISO's current recruitment and retention strategies are effective. The OIG provides no information related to performance measurements nor any indication that they assessed performance measurements despite listing it as one of the methods by which they planned to assess staffing.

Therefore, the OIG should have concluded that the CISO was adequately staffed, based on the low turnover, resulting from their most recent recruitment and retention efforts, and stated that they did not assess performance measurements as part of their audit. The OIG's conclusion that the CISO does not have a workforce plan is unrelated to the objective of the audit and their planned assessment methods.

While the report provided a view of the leadership structure, roles, and responsibilities, it assumes that the CISO's workforce planning process is not effective because elements of a textbook workforce plan were not documented. However, it does not provide adequate justification for why these elements are essential or why their absence constitutes a potential problem for the Postal Service. While documented workforce plans can be effective, the absence of a formalized plan should not indicate an ineffective workforce planning process. Hiring managers know their employees' skills, strengths, and competency levels best and can interact



directly with them to provide tailored training and development opportunities rather than having everything managed centrally by the CISO organization.

The OIG also indicated CISO leadership does not track its progress towards addressing key skill gaps for its employees and contractors. Although not tracked in a centralized manner, individual managers work with their direct reports to establish IDPs (independent development plans) and annual HERO goals, which include training and development. The administrative and 'check off the list' approach suggested by the OIG may not be worth the cost or effort to pursue. Contractors are onboarded (and subsequently offboarded) based on their resume and skill sets noted. If these were inflated during the interview process and they were unable to fulfill their duties as required, they will be offboarded.

Lastly, the OIG referenced a 2015 OIG report, which highlighted deficiencies with CISO's employee-to-contractor staffing ratio, pay bands, and training for cybersecurity staff that limited its ability to perform critical functions to protect the Postal Service network. Management would like to note that referencing an OIG report issued during the creation and standing-up of an entire organization may be less impactful than reviewing and benchmarking the current status of the CISO against a comparable sized organization and their staffing needs and/or requirements.

Following are our comments on the two recommendations.

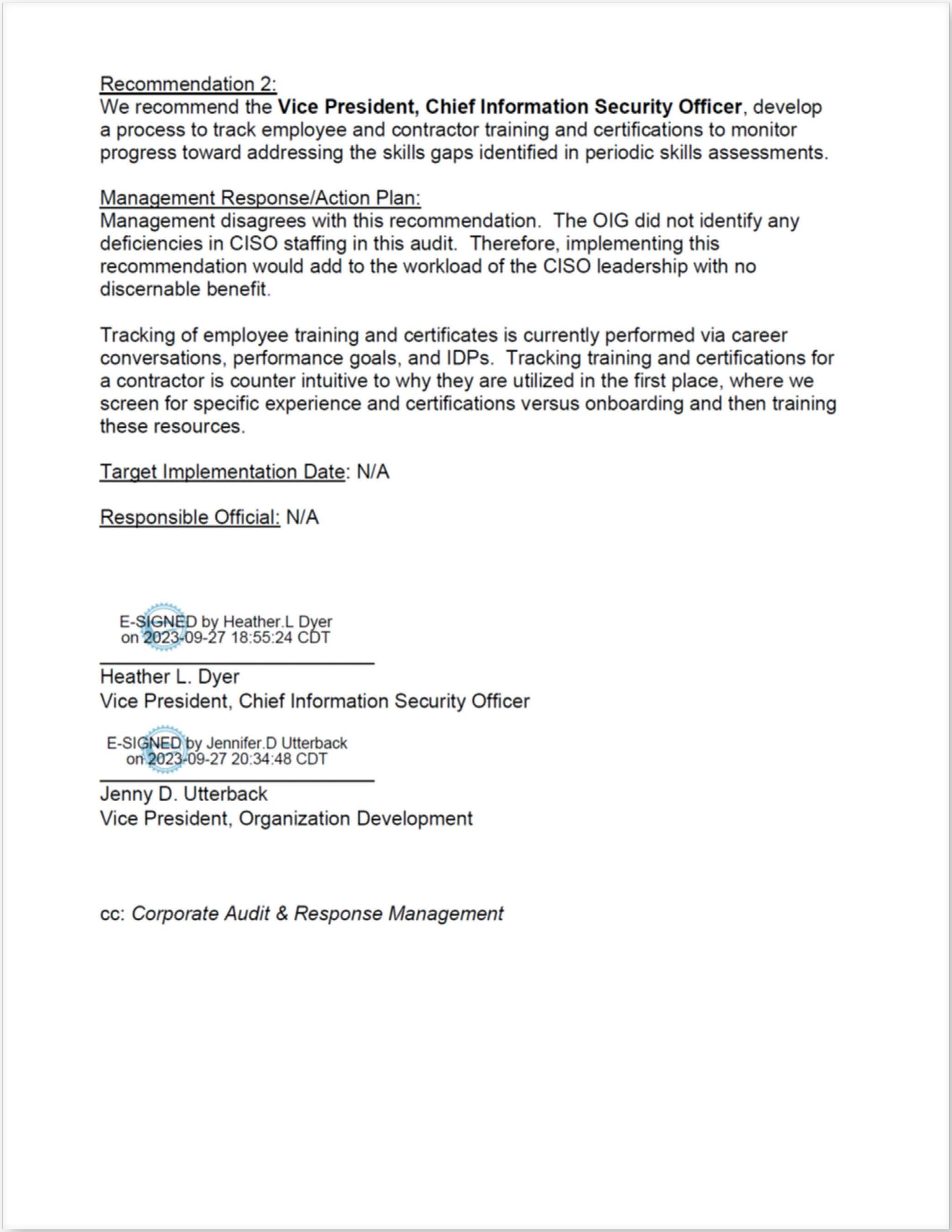
Recommendation 1:
We recommend the **Vice President, Chief Information Security Officer,** in coordination with the **Vice President, Organization Development**, establish and document a workforce plan that describes key recruitment, retention, and performance measurement activities. At a minimum, the plan should address strategic priorities, include workforce goals and objectives, identify stakeholder roles and responsibilities, and define a process for periodic review and updates.

Management Response/Action Plan:
Management disagrees with this recommendation. The OIG did not identify any deficiencies in CISO staffing in this audit. Therefore, implementing this recommendation would add to the workload of the CISO leadership with no discernable benefit.

Based on CISO's current and effective processes for recruiting, retention, and performance measurement, there does not appear to be a need to develop a documentation-based plan as it would be too high level and not impact/change the current processes.

Target Implementation Date: N/A

Responsible Official: N/A



Recommendation 2:
We recommend the **Vice President, Chief Information Security Officer**, develop a process to track employee and contractor training and certifications to monitor progress toward addressing the skills gaps identified in periodic skills assessments.

Management Response/Action Plan:
Management disagrees with this recommendation. The OIG did not identify any deficiencies in CISO staffing in this audit. Therefore, implementing this recommendation would add to the workload of the CISO leadership with no discernable benefit.

Tracking of employee training and certificates is currently performed via career conversations, performance goals, and IDPs. Tracking training and certifications for a contractor is counter intuitive to why they are utilized in the first place, where we screen for specific experience and certifications versus onboarding and then training these resources.

Target Implementation Date: N/A

Responsible Official: N/A

E-SIGNED by Heather.L Dyer
on 2023-09-27 18:55:24 CDT

Heather L. Dyer
Vice President, Chief Information Security Officer

E-SIGNED by Jennifer.D Utterback
on 2023-09-27 20:34:48 CDT

Jenny D. Utterback
Vice President, Organization Development

cc: *Corporate Audit & Response Management*

Contact us via our Hotline and FOIA forms. Follow us on social networks. Stay informed.

1735 North Lynn Street, Arlington, VA 22209-2020
(703) 248-2100

For media inquiries, please email press@uspsoig.gov
or call (703) 248-2100