July 12, 2023

To: Finance and Administration Committee

From: Darrell E. Johnson, Chief Executive Officer

Janet Sutter, Executive Director
Internal Audit Department

Subject: Performance Audit of the Orange County Transportation Authority's Cybersecurity Program

Overview

On behalf of the Internal Audit Department, the firm BCA Watson Rice LLP, has completed an audit of the Orange County Transportation Authority's Cybersecurity Program. The audit found that the Orange County Transportation Authority's Cybersecurity Program was performing adequately across most of the National Institute of Standards and Technology Cybersecurity Framework. However, BCA Watson Rice LLP identified five areas of improvement to further enhance the program.

Recommendation

Direct staff to implement five recommendations provided in the performance audit of the Orange County Transportation Authority's Cybersecurity Program.

Background

The Orange County Transportation Authority (OCTA) Cybersecurity Office within the Information Systems Department, of the Finance and Administration Division, is responsible for the Cybersecurity Program. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a voluntary framework primarily intended for organizations like OCTA to better manage and reduce cybersecurity risk. This framework provides an extensive set of cybersecurity best practices and standards designed around five core functions: Identify, Protect, Detect, Respond, and Recover. These five functions contain 23 control categories and 108 subcategories.

Internal Audit engaged BCA Watson Rice LLP, to conduct the audit to supplement audit resources and to provide expertise in the area of information technology audits. The purpose of the audit was to provide comprehensive and strategic recommendations to improve OCTA's cybersecurity posture, aligning it with industry best practices for improved efficiency and cost-effectiveness.

Discussion

The audit scrutinized OCTA's Cybersecurity Program according to these five functions and their corresponding categories. Each function was systematically assessed to identify gaps, deficiencies, and areas for improvement. Overall, the audit found the Cybersecurity Program was performing adequately across the majority of the NIST CSF five functions, 23 control categories, and 108 subcategories. However, five recommendations have been made to further enhance the program, as follows:

BCA Watson Rice LLP (auditors), found that current asset management processes do not fully enable the Cybersecurity Office to identify, track, and protect all hardware, software, and data assets against cybersecurity threats. Specifically, the auditors noted that a policy for asset inventory does not exist and that not all external and internal systems are fully cataloged and visible to the Cybersecurity Office. The auditors recommended OCTA adopt and implement an asset management policy that governs asset management and associated activities. Management agreed and responded that a policy will be developed, and an asset management system implemented.

The audit also noted that newly discovered vulnerabilities are not always mitigated or documented as “accepted risks” in a timely manner, in accordance with OCTA’s Cybersecurity Vulnerability Remediation Policy. The auditors recommended OCTA implement a comprehensive vulnerability management program that includes identifying, assessing, prioritizing, remediating, and/or documenting vulnerabilities as “accepted risks” in a timely manner. Management agreed and indicated that the current Vulnerability Policy will be enhanced and all issues will be remediated or documented as “accepted risks” in a timely manner going forward.

Auditors also reported that OCTA’s protection and recover functions relating to business continuity and disaster recovery could be strengthened. OCTA’s Business Impact Analysis (BIA) has not been formally updated since July 2016, and a full backup and recovery fail-over of all critical systems has not been tested. In addition, the Cybersecurity Office has not played a material role in the Continuity of Operations Recover (COOP) and Disaster Recovery Plan (DRP) process. The auditors recommended that OCTA update the BIA with direct input from the Cybersecurity Office and use results to inform the development, implementation, and maintenance of an updated COOP and DRP, and that the DRP plan be tested annually. Management responded they are currently working with the Security and Emergency Preparedness Department to review and update the COOP. Management plans to create playbooks to further improve the business continuity and disaster recovery processes to ensure business requirements are met.

The auditors also found that the data protection and privacy program could be strengthened by adopting a comprehensive policy, designating an individual to define and communicate data and privacy requirements, and performance of user access reviews at least every 90 days for all internal employees and third-party contractors that have OCTA user accounts and/or access to internal resources. Management committed to implementing a comprehensive data protection and privacy program for all protected data and to designate the cybersecurity manager as the individual responsible to define and communicate data and privacy requirements. In addition, management agreed to implement user access reviews at least every 90 days.

Lastly, the auditors recommended that third-party security management could be strengthened. OCTA has third-party consultants working with OCTA's data that are not subject to the same training as OCTA employees and are not required to acknowledge OCTA information technology and cybersecurity policies. Also, access reviews of these third-party consultants are not currently conducted. Management agreed and proposed additional security queries of vendors on a periodic basis, as well as development and implementation of a process to ensure all consultants working with OCTA data received cybersecurity training and follow the same policy requirements as OCTA employees.

Summary

An audit of OCTA's Cybersecurity Program has been completed by the firm of BCA Watson Rice LLP. The detailed audit scope and results are included in the audit report at Attachment A.

Attachment

A. Orange County Transportation Authority, Performance Audit of OCTA’s Cybersecurity Program, May 31, 2023, Final Report

Approved by:

Janet Sutter
Executive Director, Internal Audit
714-560-5591

ATTACHMENT A

ORANGE COUNTY TRANSPORTATION AUTHORITY

Performance Audit of OCTA's Cybersecurity Program

May 31, 2023

FINAL REPORT

Prepared by:
BCA Watson Rice LLP
Certified Public Accountants and Advisors

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report summarizes the outcomes of the comprehensive audit of OCTA's Cybersecurity Program. The intent of this audit was to evaluate the adequacy and effectiveness of OCTA's existing cybersecurity framework, policies, procedures, and controls. In addition, it aimed to assess the applicability and strength of these controls against possible cybersecurity threats. The goal of this audit was to provide comprehensive and strategic recommendations to improve OCTA's cybersecurity posture, aligning it with industry best practices for improved efficiency and cost-effectiveness.

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) was adopted as a benchmark during the audit. The NIST CSF is a voluntary framework primarily intended for organizations like OCTA to better manage and reduce cybersecurity risk. This framework provides an extensive set of cybersecurity best practices and standards designed around five core functions: Identify, Protect, Detect, Respond, and Recover. These five functions contain 23 control categories and 108 subcategories. Ultimately, these functions offer a high-level, strategic view of an organization's management of cybersecurity risk.

1. **Identify:** This function involves developing an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. It establishes the prioritization and scope of cybersecurity activities. Key program activities include:

    - Conducting a comprehensive asset inventory, including all physical and software assets.
    - Understanding the organization's mission, objectives, stakeholders, and supply chain.
    - Implementing cybersecurity governance policies and processes, with clear lines of responsibility.
    - Conducting regular risk assessments to identify and prioritize potential vulnerabilities and threats.
    - Developing a risk management strategy to address identified risks.

2. **Protect:** The function that develops and implements the appropriate safeguards to ensure delivery of critical infrastructure services. It supports the ability to limit or contain the impact of a potential cybersecurity event. Key program activities include:

    - Implementing strong access control policies and processes.
    - Providing regular cybersecurity awareness and training for all employees.
    - Ensuring data is protected through techniques like encryption and secure backup procedures.
    - Establishing information protection processes and procedures to protect systems and information.
    - Deploying protective technologies like firewalls, intrusion detection systems, and antivirus software.

3. **Detect:** This function is about developing and implementing the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner. This facilitates swift response and recovery activities. Key program activities include:

   - Implementing processes to detect and report anomalies and events that may indicate a cybersecurity event.
   - Continuously monitoring networks and systems to detect potential cybersecurity events.
   - Regularly conducting security assessments to identify vulnerabilities and verify the effectiveness of protective measures.

4. **Respond:** This function is concerned with developing and implementing appropriate activities to act regarding a detected cybersecurity incident. The objective of this function is to limit the impact of the event. Key program activities include:

   - Having a well-prepared incident response plan that outlines steps to take in the event of a cybersecurity incident.
   - Having communication plans that detail how to coordinate with internal teams and external stakeholders during and after an event.
   - Having processes in place to analyze events, understand their impact, and contain them.
   - Ensuring there are processes for improving the organization's response activities based on lessons learned from past events and ongoing monitoring.

5. **Recover:** The function that develops and implements appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. Key program activities include:

   - A recovery plan that includes detailed steps for returning to normal operations after an event.
   - Communication plans for coordinating recovery activities with internal teams and external partners.
   - Processes for improvement to ensure that recovery planning is updated based on lessons learned from past events and ongoing monitoring.

The audit scrutinized OCTA's cybersecurity program according to these five functions and their corresponding categories. Each function was systematically assessed to identify gaps, deficiencies, and areas for improvement.

Overall, our audit found that OCTA’s Cybersecurity Program was performing adequately across the vast majority of the NIST CSF five functions, 23 control categories, and 108 subcategories. However, we also discovered areas requiring improvement. The findings, described below, have resulted in detailed recommendations, designed to enhance OCTA's cybersecurity capabilities, efficiency, and resilience.

The objective of these recommendations is not just to achieve compliance with NIST CSF but to build a cybersecurity program that is robust, responsive, and adaptable given OCTA's specific business context, assets, and industry-specific evolving threat landscape. By embracing these changes, OCTA will not only be better positioned to protect its digital assets but also be equipped to respond effectively and recover swiftly in the event of a cybersecurity incident.

The remainder of this page is intentionally left blank

INTRODUCTION AND BACKGROUND

OCTA engaged BCAWR to conduct a performance audit to determine the adequacy and effectiveness of its Cybersecurity Program. A performance audit often identifies risks, cost savings, best practices, efficiencies, business process improvements, gaps, vulnerabilities, or overlaps in services, or compliance considerations with internal controls or other rules and regulations.

It was determined at the beginning of the audit that OCTA used the NIST CSF as guidance for their Cybersecurity program, which serves as criteria for measuring controls and identifying control gaps and vulnerabilities. Thus, BCAWR used the NIST Cybersecurity Framework, including the supplemental NIST 800-82 family of controls (Guide to Industrial Control Systems) as criteria for this audit.

By design, the NIST framework provides a holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate—contributing to systems that are more resilient in the face of cyber-attacks and other threats. Testing an organization against a framework affords an opportunity to explore areas to strengthen protocol and begin a risk-based approach toward designing and adopting the most appropriate security control framework for OCTA operations.

BCAWR affirms that it is independent of OCTA and conducted the performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) and relevant best practices. GAGAS requires that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. BCAWR believes that the evidence obtained provides a reasonable basis for our findings and recommendations.

The results of this performance audit, as detailed below, identify areas in need of improvement when measured against the NIST CSF.

The remainder of this page is intentionally left blank.

METHODOLOGY

This section contains the methodology used to assess OCTA's CSP based on the scope and objectives of this audit:

AUDIT STEPS	TESTING METHODOLOGY
Survey and High-level Risk Assessment (RA)	We requested and reviewed all relevant and existing OCTA CSP documentation. During the survey phase, our engagement team confirmed our understanding of how the OCTA CSP operates. We deployed our Cybersecurity Questionnaire and obtained responses from the Cybersecurity Office. We leveraged the results of our high-level RA to target our testing to achieve the objectives of this audit. We observed, where possible, activities related to the CSP operations and overall governance process.
Inquiries and Meetings	We made inquiries of management and corroborated responses with appropriate operations personnel. We also conducted inquiries of personnel responsible for carrying out distinct aspects of the CSP and corroborated responses with other personnel and documentation. Our inquiries included interviews and meetings with OCTA's CSP key stakeholders and OCTA's top management personnel.
Examinations and Walk-Throughs	We inspected CSP documents and other related documentation to determine the adequacy and appropriateness of OCTA's CSP. We also determined whether the CSP development process was conducted in accordance with specific control policies and procedures, and any established industry standards. Our examination process involved reviewing and analyzing the CSP-related documents.
Substantive Testing	We conducted substantive testing of OCTA's CSP, using our OCTA-approved Detailed Work Plan.
Reporting	We prepared a draft report and conducted an Exit Conference with OCTA before obtaining Management's Response to our findings and finalizing the Audit Report.

DETAILED AUDIT RESULTS

Finding No. 1: Current asset management processes do not fully enable the Cybersecurity Office to identify, track, and protect all hardware, software, and data assets against cybersecurity threats.

In our tests, interviews, and document reviews we noted the following:

- External and internal systems are not fully cataloged.
- No asset inventory nor asset management policy exists for technology assets.
- The Cybersecurity Office does not have full visibility within the OCTA network to effectively identify and report vulnerabilities. Some of these areas include onboard vehicle systems, radio networks, third-party controlled systems connected to the OCTA network (e.g., fueling stations, mechanical, and other support infrastructure), third-party Software as a Service (SaaS) environments, Payment Card Industry (PCI) environments, physical security (Closed Circuit Television (CCTV)/video management systems and Lenel for physical badge access), disaster recovery site, telecom network, and Internet of Things (IoT) devices.
- OCTA's data is not fully inventoried and classified based on criticality and business value.

OCTA has cataloged some of its internal systems; however, a comprehensive catalog does not exist. In addition, there is no policy requiring an inventory/catalog of internal systems.

NIST's Asset Management standard requires that organizations identify and manage their systems and data consistent with their relative importance (see Appendix for detailed criteria).

Internal systems and the data they process are related. The Cybersecurity Office should have full visibility of all critical systems and data to conduct effective monitoring to protect the systems and the data they process.

Recommendation:

OCTA should identify and catalog all hardware, software, and data assets and fully implement a comprehensive asset management program. We recommend that this program be consistent with the NIST Cybersecurity Framework and include asset identification, asset management, asset tracking, asset valuation, risk management, access control, configuration management, and maintenance and monitoring.

OCTA should draft and adopt an asset management policy that governs the asset management program and its associated activities.

Management Response:

Management agrees with these recommendations. Upon reviewing the findings and considering our current asset inventory practices, we concur with the assessment that our reliance on manual spreadsheets for asset inventory (hardware/software) is not optimal and may introduce potential risks and limitations. We recognize the importance of implementing a more robust and efficient asset management program to strengthen our cybersecurity posture. Therefore, we commit to taking the necessary steps to address this recommendation.

Information Systems currently has a line item within the fiscal year 2023-24 budget for the replacement of the Help Desk Call Tracking system. An asset management module will be included with this new software. The budget line item includes both the software and professional services for implementation.

An asset management policy will also be developed and finalized as part of the asset management software implementation.

Finding No. 2: Newly discovered vulnerabilities are often not mitigated or documented as "accepted risks" in a timely manner.

In our tests, interviews, and document reviews we noted the following:

- Some critical and high vulnerabilities in the OCTA network were discovered over 90 days ago. Though many of these vulnerabilities are not on critical systems, some are on internet-facing systems that are critical in nature and should be prioritized.
- Newly identified vulnerabilities are not mitigated or documented as "accepted risks" in a manner consistent with OCTA's Cybersecurity Vulnerability Remediation Policy. Policy states that critical vulnerabilities should be remediated within 24 or 48 hours depending on the nature of the vulnerability.
- OCTA has not established a baseline security standard for internet-facing systems.

NIST CSF standards state that an organization should perform activities to prevent the expansion of an event, mitigate its effects, and resolve the incident (see Appendix for detailed criteria).

The timely remediation of vulnerabilities and the required analysis to evaluate the true nature of the risk of each vulnerability is not prioritized. Though many of these vulnerabilities are related to noncritical systems, according to best practices and internal policy, they must all be evaluated individually. Monitoring software sometimes produces false positives, consequently, the reports from monitoring software should be evaluated carefully to eliminate false positives.

Recommendation:

To minimize cybersecurity risk, maintain compliance with internal policies and industry regulations, and reduce the likelihood of successful attacks, we recommend OCTA implement a comprehensive vulnerability management program that includes identifying, assessing, prioritizing, remediating, and/or documenting vulnerabilities as "accepted risks" in a timely manner, following the NIST Cybersecurity Framework guidelines. The key steps in the program include identifying, assessing, prioritizing, remediating, documenting, monitoring, and reviewing/improving.

We also recommend OCTA prioritize the identification and remediation of critical and high vulnerabilities for internet-facing systems.

Management Response:

Management agrees with these recommendations. The IS department will define/enhance our Vulnerability Management Program and prioritize the identification and remediation of critical and high vulnerabilities, especially those affecting internet-facing systems. Projects are currently planned to create a Patch Management and Vulnerability Identification and Remediation Program and Policy.

Some of the identified vulnerabilities are due to other older applications in use that do not support the latest version of the identified application. In these cases, a written exception is submitted to the Cybersecurity Manager and approved by the Chief Information Officer (CIO). Information Systems is working to upgrade those systems as quickly as possible so that they can support the newer version of the identified application.

Our endpoints are protected by multiple layers of security, including SecureWorks and Microsoft Defender. In the event of compromise, SecureWorks provides investigation, forensics, and analysis and we have procedures to isolate individual systems. These security services greatly reduce active risk to our environment. The Information Systems department will work to remediate or document these issues as "accepted risks" for as many of these items as possible within the 90-day window identified in the audit finding.

Finding No. 3: The Protect and Recover functions of the Cybersecurity program relating to business continuity and disaster recovery can be strengthened.

In our tests, interviews, and document reviews we noted the following:

- The Business Impact Analysis (BIA) defines critical systems and recovery times and has not been formally updated since July 2016.
- At the time of this audit, a full backup and recovery fail-over of all critical systems has not been tested or scheduled.
- Cybersecurity has not played a material role in the Continuity of Operations (COOP) and Disaster Recovery Plan (DRP) processes in recent years.

NIST CFS standards state that security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of information systems and assets (see Appendix for detailed criteria).

During our review, it was discovered that the BIA was developed by OCTA's Security and Emergency Preparedness group. A more collaborative effort, including OCTA Information Technology (IT) Department and Cybersecurity Office, will help ensure all critical IT and cybersecurity elements are included in the BIA and resulting COOP and DRP.

Recommendation:

The prerequisite to effective COOP and DRP plans is a comprehensive BIA. We recommend that OCTA update its BIA with direct input from the Cybersecurity Office and the business units. This newly developed BIA can then inform the development, implementation, and maintenance of an updated COOP and DRP plan and their associated processes and procedures that align with the NIST Cybersecurity Framework. This includes identifying critical assets and processes, establishing recovery objectives, developing response and recovery strategies, testing, updating plans regularly, and training employees on their roles and responsibilities during an incident. We also recommend that the DRP plan be tested annually and include data restoration and critical system recovery tests.

Management Response:

Management agrees with these recommendations. The BIA and COOP play a critical role in defining and providing guidance to all divisions. Information Systems is currently working with our Security and Emergency Preparedness department to review and update the COOP and participate in the update of the BIA once initiated.

Each year, Information Systems conducts an incident response tabletop exercise to test our overall cybersecurity posture and to validate our readiness to respond to a cyber-attack that could prompt an Authority-wide response. This year we're taking this exercise a step further by testing the efficacy of our incident response procedures to include restoring the targeted information systems from a backup. Following this exercise, Information Systems also plans to create playbooks to include recovery updates, associated processes, and approvals to further improve our business continuity and disaster recovery processes to ensure we can meet business requirements.

Finding No. 4: The Data Protection and Privacy Program can be strengthened.

In our tests, interviews, and document reviews we noted the following:

- FA-IS-900.09DATACLASS - Data Classification Security Policy is not currently adopted or in production. The policy was rescinded in 2021.
- Limited deployment of Multi-Factor Authentication (MFA). Aside from O365, MFA is primarily only available to privileged user accounts.
- Currently, management and staff perform annual user access reviews, but these are incomplete and lack sufficient follow-up, deviating from best practices. In organizations like OCTA, quarterly access control reviews are usually conducted to confirm validity of users.
- The Cybersecurity Office has not implemented an Insider Threat Program. An Insider Threat Program is an internal strategy that organizations develop to prevent, detect, and respond to harmful actions by its employees, contractors, or other insiders. This includes threats to the organization's information systems, data, or other assets through malicious intent or negligence. The program typically incorporates cybersecurity measures, employee training, behavior monitoring, and incident response protocols.
- Personnel with privileged accounts and access to sensitive data are not required to sign confidentiality agreements.

- Of OCTA's three PCI environments, two are fully PCI DSS (Data Security Standard) compliant, while one is missing some controls and is thus non-compliant.
- OCTA does not have a designated individual responsible for data privacy or data classification. Defining data privacy and data classification requirements informs the data protection mechanisms and controls necessary to protect data sets at the appropriate level. Formally designating a data privacy lead is a best practice. This individual would be responsible for all data privacy matters at OCTA, including issues related to employees' and customers' personally identifiable information (PII) and personal health information (PHI).

NIST CSF standards state that the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy (see Appendix for detailed criteria).

Inadequate data protection measures may result in unauthorized access, disclosure, or theft of sensitive data, leading to data breaches or leaks. Data breaches or privacy violations can lead to a loss of trust among customers and stakeholders, damaging an organization's reputation and potentially leading to a loss of business. Non-compliance with data protection and privacy regulations can result in significant fines, penalties, and legal consequences. Data breaches and regulatory fines can have a direct financial impact on the organization, including costs related to incident response, remediation, customer notifications, and potential lawsuits. Data breaches or loss of data can lead to disruptions in operations, impacting the organization's ability to deliver services and potentially causing financial and reputational harm. Inadequate personal data protection can result in identity theft or fraud, affecting customers, employees, or other individuals whose data is compromised. A weak data protection program may make the organization more susceptible to cyberattacks, such as ransomware, phishing, or advanced persistent threats, resulting in further data breaches and negative consequences.

Recommendation:

We recommend that OCTA implement a comprehensive Data Protection and Privacy Program aligned with NIST, which can help mitigate risks and minimize potential negative consequences associated with weak or inadequate data protection measures. A Data Protection and Privacy Program is an organized set of activities, policies, and procedures designed to protect sensitive data from unauthorized access and ensure compliance with data protection regulations and privacy standards, aiming to minimize risks associated with data breaches, leaks, or loss. Key components of a Data Protection and Privacy Program include data governance, data classification, access control, data encryption, data retention and disposal, data privacy compliance, incident response and breach management, training and awareness, risk assessment and management, monitoring and auditing, and vendor and third-party management.

OCTA should also designate a directly responsible individual to define and communicate the Authority's data and privacy requirements. These requirements should be captured in an updated Data Classification Policy.

Lastly, OCTA should perform user access reviews at least every 90 days for all internal employees and third-party contractors with OCTA user accounts and access to internal resources.

Management Response:

Management agrees with these recommendations. As a public agency, OCTA's data is available to the public via a public records request. OCTA will implement a comprehensive Data Protection and Privacy Program aligned with NIST for all protected data. Our data is currently encrypted both in transit and at rest. OCTA also has a robust records retention program in place for physical records including classification of documents and automated notification of when those documents reach end of life and need to be destroyed. OCTA currently has contracts in place with SecureWorks and Microsoft to assist with incident response and breach management. Cybersecurity utilizes KnowBe4 for security awareness training that covers a wide variety of training including how to protect data.

Management will designate the Cybersecurity manager as the individual that is directly responsible to define and communicate the OCTA's protected data and privacy requirements. These requirements will be captured in an updated Data Classification Policy.

Management agrees that user access reviews should be performed at least every 90 days for all internal employees and third-party contractors with OCTA user accounts and access to internal resources and will comply. However, we may reduce the frequency from 90 days to every six months at a future date if it appears that changes are minimal.

Finding No. 5: Third-Party Security Management can be strengthened.

During our review, we discovered that OCTA has third-party contractors/consultants working with OCTA's data that are not required to obtain training like the training received by OCTA's employees before being given access to OCTA's data. Further, we noted the following:

- Third-party contractors are not required to acknowledge OCTA's cybersecurity and IT policies.
- Access reviews for third-party contractors are not conducted.

NIST CSF standards state that an organization should establish priorities, constraints, risk tolerances, and assumptions and use them to support risk decisions associated with managing the risks associated with suppliers. The organization should establish and implement the processes to identify, assess and manage the risks associated with suppliers (see Appendix for detailed criteria).

The current environment increases the risks to OCTA's systems and information assets.

Recommendation:

To address the risks from partners/contractors and protect against potential security incidents, OCTA should adopt a comprehensive third-party risk management program that includes conducting thorough security assessments, monitoring the security posture of vendors, and ensuring compliance with internal policy, relevant regulations, and adopted industry standards.

A comprehensive third-party risk management program, based on NIST guidelines, aims to identify, assess, and mitigate the risks associated with third-party vendors. The program involves the following key components: vendor selection due diligence, regular risk assessments, the establishment of clear contract terms, oversight of security controls, continuous monitoring, the establishment of a collaborative incident management process, and regular training and awareness.

OCTA should ensure that all contractors possessing OCTA accounts and access to internal resources undergo cybersecurity awareness training that aligns with the training mandated for internal staff.

Management Response:

Management agrees with these recommendations. For vendor selection due diligence, OCTA currently includes language in our scopes of work and our contracts requiring vendors to provide detailed information on their cybersecurity programs. This information is considered when proposals are evaluated, and vendors are selected. OCTA will perform additional security queries on a periodic basis, beyond our initial review of the vendor responses.

Processes are being developed to ensure all third-party contractors, including OCTA-hired contractors and outside vendors receive the same cybersecurity training, and follow all the same policy requirements, as the OCTA administrative staff.

May 31, 2023

BCA Watson Rice, LLP

APPENDIX

Finding No. 1: Current asset management processes do not fully enable the Cybersecurity Office to identify, track, and protect all hardware, software, and data assets against cybersecurity threats.

Criteria

Function: Identify (ID)

Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

ID.AM-1: *Physical devices and systems within the organization are inventoried.*

ID.AM-2: *Software platforms and applications within the organization are inventoried.*
ID.AM-3: *Organizational communication and data flows are mapped.*

ID.AM-4: *External information systems are cataloged.*
ID.AM-5: *Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.*
ID.AM-6: *Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.*

Finding No. 2: Newly discovered vulnerabilities are often not mitigated or documented as "accepted risks" in a timely manner.

Criteria

Function: Respond (RS)

Mitigation (RS.MI): Activities are performed to prevent the expansion of an event, mitigate its effects, and resolve the incident.

RS.MI-3: *Newly identified vulnerabilities are mitigated or documented as accepted risks.*

OCTA's Cybersecurity Vulnerability Remediation Policy:

- *i. Critical-level vulnerabilities found on systems will be addressed within 15 calendar days of initial detection.*
- *ii. High-level vulnerabilities found on systems will be addressed within 30 calendar days of initial detection.*

Finding No. 3: The Protect and Recover functions of the Cybersecurity program relating to business continuity and disaster recovery can be strengthened.

Criteria

Function: Protect (PR)

Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of information systems and assets.

> ***PR.IP-9:*** *Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.*
> ***PR.IP-10:*** *Response and recovery plans are tested.*
> ***PR.IP-4:*** *Backups of information are conducted, maintained, and tested.*

Function: Recover (RC)

Improvements (RC.IM):

Recovery planning and processes are improved by incorporating lessons learned into future activities.

> ***RC.IM-1:*** *Recovery plans incorporate lessons learned.*

Communications (RC.CO):

Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

> ***RC.CO-3:*** *Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.*

Finding No. 4: The Data Protection and Privacy Program can be strengthened.

Criteria

Function: Identify (ID)

Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

> ***ID.AM-5:*** *Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.*

Category: Data Security (PR.DS): Information and records (data) are managed consistently with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

PR.DS-1: *Data-at-rest is protected.*

PR.DS-2: *Data-in-transit is protected.*

PR.DS-3: *Assets are formally managed throughout removal, transfers, and disposition.*

PR.DS-4: *Adequate capacity to ensure availability is maintained.*

PR.DS-5: *Protections against data leaks are implemented.*

Finding No. 5: Third-Party Security Management can be strengthened.

Criteria

Function: Identify (ID)

Category: Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

ID.SC-1: *Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.*

ID.RA-2: *Third-party stakeholders are identified, prioritized, and assessed.*

ID.SC-3: *Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.*

ID.SC-4: *Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.*