U.S. Consumer Product Safety Commission
OFFICE OF INSPECTOR GENERAL

Evaluation of the CPSC's Management of Cloud Computing, Shared Services, & Third-Party Systems

January 31, 2024

24-A-01

VISION STATEMENT

We are agents of positive change striving for continuous improvements in our agency's management and program operations, as well as within the Office of Inspector General.

STATEMENT OF PRINCIPLES

We will:

Work with the Commission and the Congress to improve program management.

Maximize the positive impact and ensure the independence and objectivity of our audits, investigations, and other reviews.

Use our investigations and other reviews to increase government integrity and recommend improved systems to prevent fraud, waste, and abuse.

Be innovative, question existing procedures, and suggest improvements.

Build relationships with program managers based on a shared commitment to improving program operations and effectiveness.

Strive to continually improve the quality and usefulness of our products.

Work together to address government-wide issues.

January 31, 2024

TO: Alexander Hoehn-Saric, Chair
Peter A. Feldman, Commissioner
Richard L. Trumka Jr., Commissioner
Mary T. Boyle, Commissioner

FROM: Christopher W. Dentel, Inspector General

Christopher W. Dentel

Digitally signed by Christopher W. Dentel
Date: 2024.01.31 15:14:13 -05'00'

SUBJECT: Evaluation of the CPSC's Management of Cloud Computing, Shared Services, & Third-Party Systems

We retained the services of Williams, Adley, & Co.-DC LLP (Williams Adley), an independent public accounting firm, to conduct an evaluation to assess the Consumer Product Safety Commission's (CPSC) management of its cloud systems, shared services, and third-party systems, from a legal, internal control, and contractual perspective. Under a contract monitored by the OIG, Williams Adley issued a report to document the results of its evaluation. The contract required that the evaluation be performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation* (QSIE). We reviewed the resulting report and related documentation and made relevant inquires to the contractors. Our review was not intended to enable us to express, and we do not express, an opinion on the matters contained in the report. Williams Adley is responsible for the attached report. However, our review disclosed no instances where Williams Adley did not comply, in all material respects, with CIGIE's QSIE.

Williams Adley found that the CPSC utilizes cloud computing, shared services, and third-party systems to support its mission and operations. They identified three findings. The first finding is that the CPSC has not defined or implemented an Information Technology (IT) modernization plan. The second finding is that the CPSC has not developed, and effectively maintained, an up-to-date and accurate inventory of its cloud, shared services, and third-party systems. The third finding is that the CPSC has not properly authorized some of its cloud computing, shared services, and third-party systems for use and operation.

Williams Adley's report contains 6 recommendations that the CPSC must address to improve the CPSC's management of its cloud systems, shared services, and third-party systems.

Should you have any questions, please contact me.

Table of Contents

Abbreviations and Short Titles 2
EXECUTIVE SUMMARY 3
What We Found 3
What We Recommend 3
1. OBJECTIVE 4
2. BACKGROUND 4
3. ASSESSMENT RESULTS 5
4. CONSOLIDATED LIST OF RECOMMENDATIONS 8
Appendix A: Objective, Scope and Methodology 9
A.1 Objective 9
A.2 Scope 9
A.3 Methodology 9
Appendix B: Management Responses 11

Abbreviations and Short Titles

CPSC	U.S. Consumer Product Safety Commission
EXIT	Office of Information and Technology Services
IT	Information Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
Williams Adley	Williams, Adley, & Co.-DC LLP

EXECUTIVE SUMMARY

The U.S. Consumer Product Safety Commission (CPSC) Office of Inspector General (OIG) retained Williams, Adley, & Co.-DC LLP (defined as "Williams Adley," "we," and "our" in this report), an independent public accounting firm, to perform the independent evaluation of the effectiveness of CPSC's management of cloud computing, shared services, and third-party systems in accordance with established requirements. This report documents the results of the evaluation.

What We Found

Williams Adley found that the CPSC utilizes cloud computing, shared services, and third-party systems to support its mission and operations. During our evaluation, we identified three findings. The first finding is that the CPSC has not defined or implemented an Information Technology (IT) modernization plan. The second finding is that the CPSC has not developed, and effectively maintained, an up-to-date and accurate inventory of its cloud, shared services, and third-party systems. The third finding is that the CPSC has not properly authorized some of its cloud computing, shared services, and third-party systems for use and operation. Lastly, we did not identify any findings related to contracts associated with cloud computing, shared services, and third-party systems.

In commenting on a draft version of this report, management provided responses, which are presented in Appendix B. We did not evaluate management's response and, accordingly, we express no opinion on the responses.

What We Recommend

We made six recommendations that the CPSC must address to improve the CPSC's management of its cloud systems, shared services, and third-party systems.

Tony Wang,
Cybersecurity Risk Services, Partner
Williams, Adley &. Co.-DC LLP

WILLIAMS ADLEY
Confidence Earned

1. OBJECTIVE

The objective of this independent evaluation was to assess the CPSC's management of its cloud systems, shared services, and third-party systems, from a legal, internal control, and contractual perspective.

2. BACKGROUND

Over the past few years, the federal government has encouraged agencies to move to a consumption-based IT services model (e.g., pay only for amount used) and away from the traditional on-premises agency-owned IT services model to improve IT security and lower costs. The following concepts support this move.

Cloud Computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud model is delivered through three service models (Software as a Service, Platform as a Service, and Infrastructure as a Service).

Shared Services

Shared services are the provision of consolidated capabilities or functions (services and information systems) that are common across multiple organizations or agencies. Shared services support efficiency by reducing duplication and lowering costs through consistent delivery of standardized capabilities or functions in ways that make the most of innovative processes and commercial solutions.

Third-Party Systems

A third-party system is a service provider external to an organization that provides a service or technology as part of a contract. In the IT space, a third-party system typically provides a technology used to store, process, and/or transmit data that enhances an organization's operational efficiency.

Federal Cloud Computing Strategy[1]

The impetus for this move came from the *Federal Cloud Computing Strategy* also known as "Cloud Smart" released by the Office of Management and Budget (OMB) in 2018 which provides a high-level strategy that was developed to drive cloud computing, shared services, and third-party system adoption in federal agencies based on recommendations detailed in the American Technology Council's *Report to the President on Federal IT Modernization* [2] published in 2017.

The "Cloud Smart" initiative which states that the federal government should move IT processing power to the cloud. The related OMB strategy document does not provide specific guidance on

[1] https://cloud.cio.gov/strategy/
[2] https://www.cio.gov/assets/resources/Report-to-the-President-on-IT-Modernization-Final.pdf

how to accomplish cloud adoption but recommends that the process be determined by each independent federal agency.

3. ASSESSMENT RESULTS

Finding 1: Ineffective IT Modernization Planning

In order to comply with the *Federal Cloud Computing Strategy* and to properly manage and plan for the adoption of cloud systems, shared services, and third-party systems, an agency should develop an IT modernization plan. However, the CPSC has not developed and implemented an IT modernization plan. Specifically, the CPSC has not completed basic tasks to enable the CPSC to make an effective and cost-effective plan to address its IT modernization concerns. The CPSC has not:

- defined its current state by inventorying its legacy systems
- calculated the costs associated with the operation and maintenance of those legacy systems
- calculated the cost and level of effort associated with modernizing these systems;
- identified potential cost saving opportunities that may be gained through modernization
- documented its target state

Furthermore, the CPSC has not planned an approach or begun the process to transition its mission critical applications to a cloud-based environment. Neither has the CPSC evaluated all of its mission critical and non-mission critical legacy applications for transitioning to the cloud as required within its *Cloud Management Strategy*.

Based on inquiries with CPSC management, including Office of Information and Technology Services (EXIT) personnel, it was noted that EXIT currently does not have the appropriate mix of staff with the relevant skills and abilities to modernize its systems. EXIT staff are in the process of enhancing their technical capabilities and capacity to support planning and modernizing efforts; however, they have not yet developed a plan. Without a plan to modernize the agency's IT systems, management cannot effectively identify opportunities to improve operations, save resources, and improve security to meet future priorities.

It is critical for a small agency with limited resources to proactively plan for the future and consider the most cost-effective way forward. Furthermore, legacy systems may operate with known security vulnerabilities that are either technically difficult, or prohibitively expensive to address.

Recommendations:

1. Develop and implement an IT modernization plan. This plan should:
    i. document an inventory of all legacy systems in operation at the CPSC
    ii. identify the cost associated with the operations and maintenance of the legacy systems in operation in the current environment at the CPSC
    iii. identify the resources necessary to modernize each CPSC legacy system (e.g., migrating to a Commercial-Off-The-Shelf solution or shared services solution, moving

to a cloud environment, etc.)

iv. analyze potential opportunities to save money, improve operations, and improve security through modernizing the CPSC's legacy systems

2. Develop and establish a process to monitor the implementation of the IT modernization plan by documenting the objectives, goals, tasks, milestones, metrics, and funding sources associated with management's modernization efforts.

Finding 2: Ineffective Cloud Computing, Shared Services, and Third-Party System Inventory

In order to effectively establish and monitor cloud computing, shared services, and third-party systems programs, it is critical to accurately identify and track those information systems. Without an accurate and complete inventory comprising all information systems, the CPSC may not be able to ensure that the appropriate controls are in place to protect the information systems and their data, and it makes transitioning to consumption-based services far more challenging.

The CPSC did not maintain an accurate, up-to-date, and complete inventory of its cloud, shared services, and third-party systems. Specifically, the inventory provided was incomplete, mislabeled, and miscategorized many of the data elements. Further, while the CPSC has defined processes for handling new cloud implementation requests within its primary commercial cloud, the CPSC has not yet defined a process for handling new cloud implementations that are outside of that cloud environment. Moreover, the CPSC has not yet defined policies and procedures to maintain a complete and accurate cloud computing, shared services, and third-party systems inventory.

According to the CPSC personnel, the inventory is not accurate or complete because the CPSC does not have the dedicated resources necessary to maintain the inventory for transitioning to a consumption-based service model.

Recommendation:

3. Establish and implement a policy and procedure to manage the cloud computing, shared services, and third-party system inventory necessary for transitioning to a consumption-based service model.

Finding 3: Cloud Computing, Shared Services, and Third-Party Management Systems Authorization to Operate and Use are not fully supported

An information system must undergo an assessment of its information security controls to ensure effectiveness prior to being authorized for use and operation. This process includes identifying information security risks to the system and designing and implementing controls to mitigate these risks. The process also includes continuously monitoring the implementation of the controls designed to mitigate information security risk. These controls must be documented by management and tested by an independent assessment team. Upon completion of this independent assessment, the information security weaknesses identified should be accepted by the agency, remediated immediately, or management should develop a remediation plan to address and monitor these issues. An authorizing official should then review the assessment

results and remediation efforts to determine whether to accept the risks posed by the system and formally authorize the system for use and operation.

However, the CPSC has not established and implemented a policy or procedure to support the use and authorization of cloud, shared services, and third-party systems. In addition:

- the CPSC did not develop the appropriate security documentation [e.g. System Security Plan, Security Assessment Report, etc.] to support its decision to authorize one cloud system to operate.
- the CPSC was unable to provide evidence that two third-party systems were authorized for operation or use.
- the CPSC was unable to provide evidence that it performed a periodic review of the vendor security documentation (e.g., FedRAMP, Service Organization Control Two reports) for its cloud systems.
- the CPSC was unable to provide evidence that the customer responsibility matrices for its cloud, shared services, and third-party systems were collected and reviewed to identify and implement CPSC responsibilities.

The CPSC has not dedicated the resources necessary to establish and implement a formal process that ensures security controls are adequately designed and implemented for the operation and use of external services (e.g., cloud, shared services, and third-party systems). Additionally, the CPSC has not developed explicit guidance and processes to identify and address information security risks and integrate those risks into the broader agency-wide enterprise risk management program.

Without a clear understanding of its information security environment (both internal and external) and an organization-wide view of risks, the CPSC is not able to identify, assess, and respond to those risks in an effective manner, which in turn, exposes the agency to targeted attacks and environmental disruptions. This also gives rise to the inefficient use of resources as efforts are spent in a reactive manner to address issues as they surface, instead of proactively preventing and addressing the weaknesses.

Recommendations:

4. The CPSC should develop and implement policies and procedures to periodically review security packages from external service providers (such as those hosting cloud, shared services, and third-party systems) to ensure that the risks posed by the external service provider are within the CPSC's risk appetite and tolerance.
5. The CPSC should review the external service provider's customer responsibility matrices, select, tailor, implement the relevant security controls from those matrices and then document (and periodically reassess) those controls to support the ongoing authorization to operate and use decision.
6. The CPSC should revisit the scope section of its security assessment policies and procedures to ensure that they include appropriate consideration for third-party systems.

4. CONSOLIDATED LIST OF RECOMMENDATIONS

Recommendations
1. Develop and implement an IT modernization plan. This plan should: i. document an inventory of all legacy systems in operation at the CPSC ii. identify the cost associated with the operations and maintenance of the legacy systems in operation in the current environment at the CPSC iii. identify the resources necessary to modernize each CPSC legacy system (e.g., migrating to a Commercial-Off-The-Shelf solution or shared services solution, moving to a cloud environment, etc.) iv. analyze potential opportunities to save money, improve operations, and improve security through modernizing the CPSC's legacy systems 2. Develop and establish a process to monitor the implementation of the IT modernization plan by documenting the objectives, goals, tasks, milestones, metrics, and funding sources associated with management's modernization efforts. 3. Establish and implement a policy and procedure to manage the cloud computing, shared services, and third-party system inventory necessary for transitioning to a consumption-based service model. 4. The CPSC should develop and implement policies and procedures to periodically review security packages from external service providers (such as those hosting cloud, shared services, and third-party systems) to ensure that the risks posed by the external service provider are within the CPSC's risk appetite and tolerance. 5. The CPSC should review the external service provider's customer responsibility matrices, select, tailor, implement the relevant security controls from those matrices and then document (and periodically reassess) those controls to support the ongoing authorization to operate and use decision. 6. The CPSC should revisit the scope section of its security assessment policies and procedures to ensure that they include appropriate consideration for third-party systems.

Appendix A: Objective, Scope and Methodology

A.1 Objective

The objective of this independent evaluation was to assess the CPSC's management of its cloud systems, shared services, and third-party systems, from a legal, internal control, and contractual perspective.

A.2 Scope

This evaluation covered the period of July 1, 2022, to June 30, 2023. The evaluation included selecting a representative subset of the CPSC's cloud, shared services, and third-party systems.

A.3 Methodology

We performed this evaluation from August through December 2023, and conducted this evaluation in accordance with Council of Inspectors General on Integrity and Efficiency, *Quality Standards for Inspection and Evaluation*. Those standards require that we obtain sufficient evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objectives.

To perform this evaluation, we interviewed CPSC senior management and employees to evaluate relevant managerial effectiveness and operational controls in accordance with federal guidance. We obtained evidence to support Williams Adley's conclusions and recommendations, tested effectiveness of established or defined controls, conducted sampling where applicable, and collected and reviewed written documents to supplement observations and interviews. We delivered Notices of Findings and Recommendations that support this report to CPSC management.

Our assessment from an internal control perspective included reviewing the CPSC policies and procedures that guide the management of cloud computing, shared services, and third-party systems including the use of an IT modernization plan and the completeness and accuracy of the CPSC's cloud computing, shared services, and third-party inventory. We assessed the CPSC's management of cloud computing, shared services, and third-party systems, from a legal and contractual perspective by reviewing the CPSC's associated contracts and assessing the inclusion of applicable Federal Acquisition Regulation clauses.

Sampling Methodology

With respect to the sampling methodology employed, standards indicate that either a statistical or judgmental sample can yield sufficient and appropriate evidence. Based on professional judgement, Williams Adley did not use statistical sampling during this evaluation. Williams Adley employed another type of sample permitted by standards—namely, a non-statistical sample known as a judgmental sample. A judgmental sample is a sample selected by using discretionary criteria rather than criteria based on the laws of probability. In this evaluation, Williams Adley has taken great care in determining the criteria to use for sampling based on Williams Adley's judgement of risk.

Williams Adley acknowledges that it is possible that the information security deficiencies identified in this report may not be as prevalent or may not exist in other information systems that were not tested.

Evaluation, testing, and analysis were performed in consideration with guidance from the following:

- Council of Inspectors General on Integrity and Efficiency, *Quality Standards for Inspection and Evaluation*
- OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (Revised)
- OMB Memoranda
- OMB, *Federal Information Technology Operating Plan*
- OMB, *Federal Cloud Computing Strategy*
- Chief Information Officer's Council, *Application Rationalization Playbook*
- Chief Acquisition Officer's Council and Chief Information Officer's Council, *Creating Effective Cloud Computing Contracts for the Federal Government*
- National Institute of Standards and Technology Federal Information Processing Standards Publications and Special Publications
- Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
- President's Management Agenda, *Cross-Agency- Priorities, IT Modernization and Sharing Quality Services*
- American Technical Council, *Report to the President on IT Modernization*
- Government Accountability Office, *Standards for Internal Control in the Federal Government*
- Government Accountability Office, *Information Technology: Agencies Need to Continue Addressing Critical Legacy Systems*
- CPSC's 2024 Presidential Performance Budget
- CPSC Strategies, Policies, Standards, Guides, and Standard Operating Procedures

Appendix B: Management Responses

United States
Consumer Product Safety Commission

Memorandum

TO: Office of Inspector General (OIG) **DATE:** January 19, 2024

FROM: Bryan Burnett, Chief Information Officer (EXIT)

Digitally signed by BRYAN BURNETT
DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=BRYAN BURNETT, 0.9.2342.19200300.100.1.1=61001000009719
Date: 2024.01.19 20:33:13 -05'00'

SUBJECT: Evaluation of the CPSC's Management of Cloud Computing, Shared Services, and Third-Party Systems Management Response

---

Management appreciates the work conducted by the OIG and its auditors in this assessment of the CPSC's management of its cloud systems, shared services, and third-party systems.

Management concurs with the findings and recommendations regarding improving the management of the agency's application inventory, including how the agency categorizes and performs security assessments for the applications. While the scope of this evaluation was through June 30, 2023, management will take this opportunity to briefly discuss some of the changes included in a draft update of the agency's Assessment and Authorization (A&A) Policy, which will be finalized in the first quarter of 2024. The first of these changes is the switch from Authorizations to Operate (ATO) to Authorizations to Use (ATU) for cloud-based applications. ATUs take advantage of existing security assessments and will free up agency resources to increase the number of applications that are reviewed, as per the OIG's recommendation. The ATU process also focuses on reviewing service providers' customer responsibility matrices, as the OIG suggests. Management also intends to move from Revision 4 to Revision 5 of the National Institute of Standards & Technology's (NIST's) Security and Privacy (800-53) Controls for its assessments, an effort that many federal agencies already have undertaken. Finally, management is revising the scope section of its A&A Policy to ensure that it includes appropriate consideration for third-party systems.

Management generally concurs with the findings and recommendations regarding maintaining an updated Modernization Plan. As the OIG notes, there is no single resource that documents the agency's modernization efforts. Management is committed to collecting and organizing the existing materials that support the agency's modernization efforts in a manner that improves transparency and accountability. EXIT's current focus is on improving its ability to execute

U.S. Consumer Product Safety Commission
4330 East-West Highway
Bethesda, MD 20814
cpsc.gov

National Product Testing & Evaluation Center
5 Research Place
Rockville, MD 20850

This memorandum was prepared by the CPSC staff. It has not been reviewed or approved by, and may not necessarily reflect the views of, the Commission.

Page 1 of 2

existing modernization plans, enhancing its technical capabilities, and increasing internal support for the agency's multiple in-progress modernization efforts, including:

- Compliance Regulatory Enforcement (CRE): a *cloud-based* case management system that went into production in November 2023. The services developed for CRE will serve as a common platform for future modernization efforts for the agency's legacy Integrated Field System and Dynamic Case Management systems.
- WebNEISS (National Electronic Injury Surveillance System) and Epidemiology Management Application (EMA): *cloud-based* applications that are the starting points for Epidemiology's legacy application and process modernization efforts. WebNEISS went into production in January 2024.
- International Trade Data System Risk Assessment Methodology System (ITDS/RAM): while this import surveillance application was deployed in the agency's on-premises data center, it was developed as a *cloud-ready* application. To scale the application to support ever-increasing data volumes, the Office of Import Surveillance has requested that management consider a *cloud migration* for this fiscal year.
- SAS Viya: the agency's new analytics platform went into production in September 2023. The initial deployment was in a SAS data center, with plans to move it to the *agency's commercial cloud provider* after SAS achieves the necessary FedRAMP authorization.
- cpsc.gov: the agency's primary website was previously migrated to a *commercial cloud provider*. There is a current effort to significantly enhance the website's navigation, search, and overall value proposition.
- Consumer Product Safety Risk Management System (CPSRMS): the agency's legacy implementation of a Public Database as mandated in the Consumer Product Safety Improvement Act (CPSIA) 2008, Section 212. A project to enhance the data dictionary and documentation for the application was approved during the 2023 mid-year Capital Planning and Investment Control (CPIC) process. This project will aid in the planning of a future modernization effort.

Each of these initiatives followed EXIT's Solution Development Life Cycle process, which includes a Project Request, Project Intake meeting, and Statement of Work development and review. These initiatives also were presented to the CPIC Review Board for inclusion in the agency's budget cycles and, once approved, were included in the agency's Operating Plan. In terms of monitoring, the ongoing efforts are discussed internally within EXIT on a bi-weekly basis, with Program Office and vendor leadership on a monthly basis, and with agency leadership on a quarterly basis as part of the Strategic Data Review process.

For more information on this report please contact us at CPSC-OIG@cpsc.gov

To report fraud, waste, or abuse, mismanagement, or wrongdoing at the CPSC go to OIG.CPSC.GOV or call (301) 504-7906

Office of Inspector General, CPSC, 4330 East-West Hwy., Suite 702, Bethesda, MD 20814