INFORMATION TECHNOLOGY
COLORADO STATE UNIVERSITY SYSTEM

April 1, 2025

Kerri L. Hunter, CPA, CFE
State Auditor
Colorado Office of the State Auditor
1525 Sherman St., 7th Floor
Denver, CO 80203

Dear Auditor Hunter:

In response to your request, we have prepared the attached updated status report on the implementation status of audit recommendations contained in the Evaluation of Cybersecurity Maturity Model Certification (CMMC) Readiness at the Colorado State University System. The report provides a brief explanation of the actions taken by the Colorado State University System to implement each recommendation.

In the wake of the audit recommendations from Eide Bailly, the CSU System Board of Governors issued a resolution on June 7, 2024, charging the CSU System Vice President for Information Technology "to develop a plan to improve and modernize IT and cybersecurity" and authorized the Chancellor "to take any necessary actions to assist with the implementation". Elements of this charge include:

- Develop a plan to improve and modernize IT and cybersecurity in order to obtain and maintain CMMC by updating CSU's infrastructure, personnel structure, policies, standardization practices, and enforcement related to its IT environment.

- Establish a centralized authority for IT security at CSU.

- Modernize CSU's IT infrastructure (such as directories, e-mail, networks, servers, and digital storage), as well as its endpoint management (including Windows, Mac, and Linux).

- Modernize the structure and allocation of resources, such as employees and budget, and update technology standards and procurement, as well as workflows and processes.

A 6-month planning effort with broad stakeholder engagement was completed in December 2024. The CSU System Chancellor, and CSU Ft. Collins President, approved the plan to implement the elements of the resolution in a phased, 3-year initiative focusing on CMMC compliance in Phase 1 (to meet the October 1, 2025 anticipated CMMC 2.0 deadline) and leveraging moves to a more consolidated and cloud-forward approach to IT at CSU.

During the planning phase, external experts (including EAB, Trebuchet Group, Summit Security Group, and Vantage Technology Group) were engaged to assist in developing elements of the plan and pursuing a thorough review and rewrite of all security policies for the CSU System. The primary policy (CSU System IT Security Policy) was drafted following national best practices, has been reviewed by a group of stakeholders from both Fort Collins and Pueblo campuses, and will be put forward to the Board of Governors for adoption, anticipated to be May 1, 2025. Additional derived Standards and supporting Procedure documents are being developed in the first phase of the implementation. Notably, these Standards include formal specification and guidance for treatment of FCI and CUI.

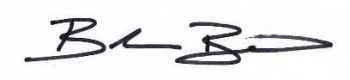
As a key element in the plan, CSU is entering into a strategic partnership with Microsoft, providing cybersecurity compliance assistance, implementation resources for both a cloud migration and "Modern Desktop" management, as well as staff upskilling support and a Student Security Operations Center.

In the status response for the 16 recommendations, the following abbreviations are used:

- **OVPR:** CSU's Office of the Vice President for Research
- **DoIT:** CSU's Division of IT
- **UCSD Sherlock:** The secure enclave maintained by the University of California, San Diego
- **M365 GCC:** Microsoft's Government Community Cloud (similar to commercial M365 services, but geared toward collaboration support for CUI and other regulated data requiring more advanced security controls)

If you have any questions about this status report and the Colorado State University System's efforts to implement the audit recommendations, please contact Brandon Bernier at 970-491-7448 or Brandon Bernier.

Sincerely,



Brandon Bernier
Vice President for IT & Chief Information Officer
Colorado State University System

Evaluation Recommendation Status Report

Evaluation Name:	Evaluation of Cybersecurity Maturity Model Certification (CMMC) Readiness at the Colorado State University System – Public Report
Evaluation Number:	2350P-IT
Agency:	Colorado State University
Date of Status Report:	April 1, 2025

Section I: Summary

Rec. Number	Response from Audit Report	Original Implementation Date	Current Implementation Status	Current Implementation Date
1A	Agree	December 2024	Partially Implemented	May 2025
1B	Agree	April 2024	Partially Implemented	May 2025
1C	Agree	April 2024	Partially Implemented	May 2025
1D	Agree	December 2024	Implemented	February 2025
1E	Agree	December 2024	Implemented	April 2025

Section II: Narrative Detail

Recommendation 1A	
The Colorado State University System (CSU) should improve program management controls and ensure compliance with Cybersecurity Maturity Model Certification (CMMC) requirements by: Establishing a unified governance structure. This should include appointing a central authority responsible for defining and enforcing uniform IT security standards across all campuses, ensuring consistent measures are implemented, and mitigating the risk of security threats.	
Current Implementation Status	Partially Implemented
Current Implementation Date	May 2025
Status Update Narrative	The formal IT Governance model has been finalized, with cybersecurity represented both as an input for new projects and an advisory when new projects are referred to executive leadership. The CSU System Chief Information Security Officer (CISO) has been formally identified in the new System-wide IT Security Policy as the central authority responsible for defining and enforcing IT security standards, ensuring consistent measures are implemented, and mitigating the risk of security threats. The new policy has been submitted for approval at the May 1-2 Board of Governors meeting; estimating completion and public posting of the policy May 15, 2025.

Recommendation 1B	
The Colorado State University System (CSU) should improve program management controls and ensure compliance with Cybersecurity Maturity Model Certification (CMMC) requirements by: Identifying the senior official who will be responsible for ensuring compliance with CMMC Program requirements and who will submit the annual CMMC affirmation.	
Current Implementation Status	Partially Implemented
Current Implementation Date	May 2025
Status Update Narrative	The CSU System CISO has been identified in the new System-wide IT Security Policy as the senior official responsible for ensuring compliance with security regulations generally. Specific responsibility is assigned to the CISO to ensure and affirm CMMC compliance in the Advanced Cybersecurity Protection Standard – CUI. Since the policy has been submitted for approval at the May 1-2 Board of Governors meeting, this recommendation has been listed as In Progress; estimating completion and public posting by May 15, 2025.

Recommendation 1C	
The Colorado State University System (CSU) should improve program management controls and ensure compliance with Cybersecurity Maturity Model Certification (CMMC) requirements by: Identifying an individual who will be responsible for accessing and submitting reports through the Department of Defense's Supplier Performance Risk System.	
Current Implementation Status	Partially Implemented
Current Implementation Date	May 2025
Status Update Narrative	The CSU Senior Director for Research IT will access and submit reports through the Department of Defense's Supplier Performance Risk System (SPRS), as clarified in the Roles & Responsibilities section of the final Advanced Cybersecurity Protection Standard – CUI. Since the authority to enforce new standards is in the new CSU System-wide IT Security Policy, which has been submitted for approval at the May 1-2 Board of Governors meeting, this recommendation has been listed as In Progress; estimating completion and public posting by May 15, 2025.

Recommendation 1D	
The Colorado State University System (CSU) should improve program management controls and ensure compliance with Cybersecurity Maturity Model Certification (CMMC) requirements by: Establishing a formal training program to educate appropriate personnel on policies and procedures for identifying and handling FCI and CUI. *This topic is also discussed more extensively in the confidential report within recommendations 2.C and 3.E.*	
Current Implementation Status	Implemented
Current Implementation Date	February 2025
Status Update Narrative	The OVPR has developed, and has begun administering, a training program covering both Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). All personnel currently engaged in projects with CUI have taken the training; moving forward, training will be first administered when a new CUI project or user is on-boarded, and then annually afterwards.

Recommendation 1E	
The Colorado State University System (CSU) should improve program management controls and ensure compliance with Cybersecurity Maturity Model Certification (CMMC) requirements by: Establishing a formal, post-award procedure to ensure that appropriate controls are in place to ensure compliance with CMMC related Federal Acquisition Regulations and Defense Federal Acquisition Regulation Supplement.	
Current Implementation Status	Implemented
Current Implementation Date	April 2025
Status Update Narrative	A post-award procedure has been established by the OVPR to ensure appropriate controls for CMMC. The procedure, in place since November 2024, is shared among the Office for Secure and Global Research, the Senior Research Administrator in the Office of Sponsored Programs and the Principal Investigator for each project. Touch points begin with the setup of a Technology Control Plan at project initiation (before release of funds), combined with annual review of requirements and re-affirmation of compliance at annual renewal in the Kuali Research system. A Procedure describing this process was updated for clarity and published, removing “draft” status, in March 2025, with additional communication from the VP for Research in April 2025.