Evaluation of Cybersecurity Maturity Model Certification (CMMC) Readiness at the

Colorado State University System

Colorado State University System

Evaluation of Cybersecurity Maturity Model Certification (CMMC) Readiness

Public Report

May 2024

Report Number 2350P-IT

Eide Bailly LLC

EideBailly®

CPAs & BUSINESS ADVISORS

THE MISSION OF THE OFFICE OF THE STATE AUDITOR
IS TO IMPROVE GOVERNMENT
FOR THE PEOPLE OF COLORADO

LEGISLATIVE AUDIT COMMITTEE

Representative Lisa Frizell Chair	Representative Andrew Boesenecker Vice Chair
Representative Gabe Evans	Senator Dafna Michaelson Jenet
Senator Rhonda Fields	Senator Rod Pelton
Representative William Lindstedt	Senator Kevin Van Winkle

OFFICE OF THE STATE AUDITOR

Kerri L. Hunter, CPA, CFE	State Auditor
Matt Devlin, MS, CISA, CISM	Chief IT Auditor
Cindi Radke, CISA	Contract Monitor
Eide Bailly LLP	Contractor

REPORT NUMBER 2350P-IT

EideBailly

CPAs & BUSINESS ADVISORS

May 23, 2024

Members of the Legislative Audit Committee:

This report contains the results of the Evaluation of Cybersecurity Maturity Model Certification (CMMC) Readiness at the Colorado State University System. The evaluation was conducted pursuant to Section 2-3-103, C.R.S, which authorizes the State Auditor to conduct performance, financial, and information technology audits of all departments, institutions, and agencies of the state government. The report presents our findings, conclusions, and recommendations, and the responses of the Colorado State University.

We conducted this performance evaluation in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate 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 evaluation objectives.

During our evaluation work, we identified certain matters that were considered sensitive to protecting state information technology assets. Accordingly, these matters are not included in this report but were reported to the Colorado State University's management in a separate confidential report dated May 22, 2024.

E. Anders Erickson
Principal, Risk Advisory Services
Eide Bailly, LLC

CONTENTS

REPORT HIGHLIGHTS

Evaluation of Cybersecurity Maturity Model Certification (CMMC) Readiness at the Colorado State University System
IT Performance Evaluation, May 2024 – Report Number 2350P-IT

EVALUATION CONCERNS

The Cybersecurity Maturity Model Certification (CMMC) is a program being developed by the United States Department of Defense (DoD) to enhance the cybersecurity practices within the Defense Industrial Base (DIB). The DIB includes the organizations, facilities, and resources that support the research, development, design, production, delivery, and maintenance of military weapons systems, subsystems, and components. The primary purpose of the CMMC is to ensure that organizations in the DIB sector adequately protect sensitive information and data related to national security. While the DoD is conducting a prolonged implementation and rollout of CMMC, the security standards that form the foundation of the CMMC are built upon preexisting contractual requirements. Accordingly, the DoD expects organizations in the DIB to already be complying with the minimum-security standards established by CMMC.

Colorado State University (CSU) is a member of DIB through research contracts it maintains with the DoD. In the context of our evaluation, these contracts facilitate the following two functions: (1) they provide CSU employees and students with access to sensitive national security data and information, and (2) they require CSU to adhere to Federal and DoD regulations for the protection of sensitive data and information. This report identifies the following primary concerns:

- At the time of our evaluation, CSU had not established the security practices necessary to ensure compliance with minimum information technology (IT) security standards required by and agreed to in its current contracts with the DoD.
- The lack of a strong, centralized authority for IT security at CSU could significantly hinder the University's ability to meet minimum DoD requirements for information security and ultimately obtain and maintain Cybersecurity Maturity Model Certification.

Additional concerns were identified related to the University's compliance with specific technical and programmatic federal and DoD regulations for the protection of sensitive data and information, which will ultimately become requirements of CMMC. Due to the sensitive nature of these concerns, the details have been included in a separate, confidential report, as Findings 2 and 3.

BACKGROUND

The Colorado State University System:

- The CSU System is composed of three campuses: CSU Fort Collins, CSU Pueblo, and CSU Global.
- Each of the three campuses and the CSU System is responsible for maintaining its own IT program, policies, and procedures.
- CSU Fort Collins is the only member of the CSU System that currently maintains contracts with the DoD. Accordingly, our evaluation focused on the activities and programs at that campus.

KEY FACTS AND FINDINGS

- CSU had not established a centralized governing authority responsible for establishing uniform standards for IT security across all colleges and departments.
- CSU had not identified key leadership and programmatic roles who will be responsible for oversight, facilitation, and monitoring of CMMC.
- CSU had not established a formal training program to educate appropriate personnel on policies and procedures for identifying and handling of sensitive DoD information.

Additional key facts and findings were identified related to the University's compliance with specific technical and programmatic Federal and DoD regulations for the protection of sensitive data and information, which will ultimately become requirements of CMMC. Due to the sensitive nature of these concerns, the details have been included in a separate, confidential report, as Findings 2 and 3.

The box below provides a count of the total recommendations made from this evaluation, including those in both the public report and the associated confidential report. This box also provides a count of the number of recommendations with which CSU management agreed, partially agreed, or disagreed.

Recommendations Made

16

Responses

Agree: **16**

Partially Agree: **0**

Disagree: **0**

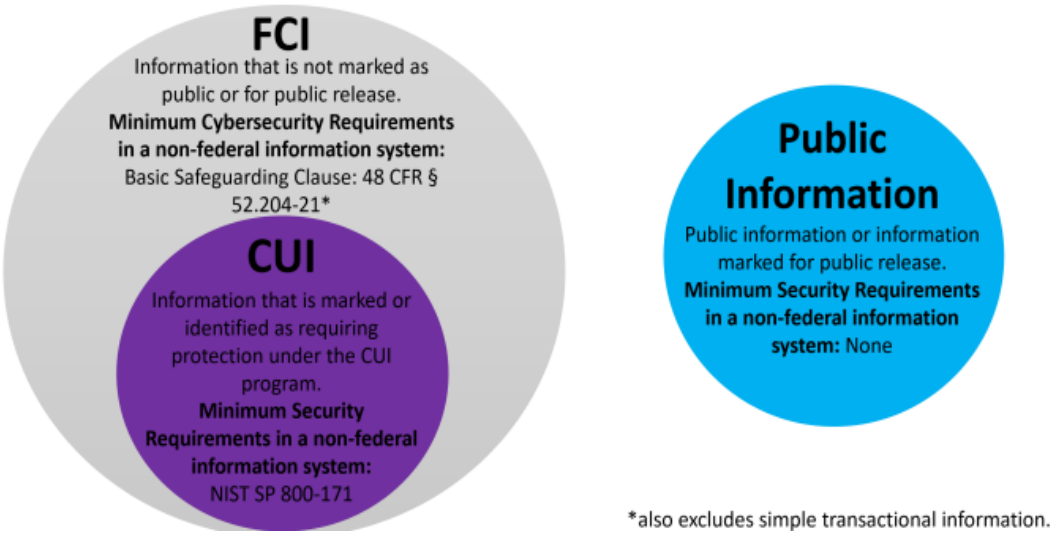
CHAPTER 1

OVERVIEW

The Cybersecurity Maturity Model Certification (CMMC) is a comprehensive framework developed by the United States Department of Defense (DoD) to enhance and standardize cybersecurity practices across the Defense Industrial Base (DIB). The DIB includes the organizations, facilities, and resources that support the research, development, design, production, delivery, and maintenance of military weapons systems, subsystems, and components. Introduced to safeguard sensitive information and address evolving cyber threats, CMMC establishes a set of cybersecurity standards that defense contractors and suppliers must meet to qualify for DoD contracts. The cybersecurity maturity model comprises varying maturity levels, ranging from basic cyber hygiene practices to advanced capabilities, each corresponding to increasing levels of security practices and processes. By requiring CMMC, the DoD aims to fortify the overall cybersecurity posture of its supply chain, ensuring that contractors handling sensitive information and data related to national security adhere to robust cybersecurity measures. CMMC aims to protect two types of sensitive data and information:

- **Federal Contract Information (FCI)**: Information provided by or generated for the federal government under a contract, excluding publicly available data.
- **Controlled Unclassified Information (CUI)**: Information handled using safeguarding or dissemination controls as required by law or regulation.

The diagram below delineates the fundamental distinctions among FCI, CUI, and Public Information.



Source: National Archives, FCI and CUI, what is the difference? CUI Program Blog June 2020

The majority of organizations seeking compliance with CMMC will fall into Level 1 or Level 2. As detailed in the table below, the differences between CMMC Level 1 and Level 2 lie in the range of security practices required, the type of assessment conducted, and the sensitivity of information being handled.

Comparison Between CMMC Level 1 and Level 2

	Level 1	Level 2
Focus	Basic cyber hygiene	Advanced cyber hygiene
Required Practices	17	110
Assessment Type	Self-Assessment	Self-Assessment and Third-party Assessment
Required For	Organizations handling FCI	Organizations handling CUI

Source: Eide Bailly analysis of the CMMC Self-Assessment Guides – Level 1 and Level 2, as well as 32 Code of Federal Regulations (CFR) Part 170

Note that both CMMC Level 1 and Level 2 require organizations to conduct a self-assessment, the results of which will be reported to the DoD. In addition, organizations seeking CMMC Level 2 will eventually be required to undergo an independent assessment by a CMMC Certified Third-Party Assessor Organization to verify their compliance level.

The DoD has indicated that contract awards will be contingent upon achieving the required CMMC level, and the DoD will enforce CMMC requirements through the inclusion of specific regulatory clauses in its contracts with DIB organizations. These include clauses from the following regulations:

- The *Federal Acquisition Regulation (FAR)* is a set of rules and regulations, maintained jointly by the DoD and two other federal agencies, governing the acquisition of supplies and services by federal executive agencies in the United States. It applies when these agencies use appropriated funds for procurement. The FAR includes requirements for the protection of FCI and is referenced in DoD contracts to enforce CMMC Level 1.
- The *Defense Federal Acquisition Regulation Supplement (DFARS)* is administered by the DoD and serves as an extension to the FAR. It contains specific requirements, policies, and deviations related to defense-related acquisitions. The DFARS includes requirements for the protection of CUI and is referenced in DoD contracts to enforce CMMC Level 2.

CMMC Readiness Evaluation

In preparation for CMMC, an organization may choose to conduct a readiness evaluation, which fulfills the following objectives:

- Serves as a proactive measure to assess the organization's current cybersecurity posture and preparations to comply with the evolving cybersecurity standards mandated by the DoD.
- Enables the identification of potential gaps or deficiencies in the organization's cybersecurity practices, helping to mitigate risks and enhance overall security measures.
- Allows the organization to align its cybersecurity practices with the specific requirements outlined in the CMMC framework, ensuring preparedness for future DoD contracts.

By undergoing this assessment, organizations not only demonstrate their commitment to cybersecurity but also position themselves competitively in the DIB, showcasing a robust and compliant cybersecurity infrastructure.

Colorado State University Fort Collins

Colorado State University (CSU) Fort Collins is currently the sole campus within the Colorado State University System holding DoD contracts. Within CSU Fort Collins, there are IT and research organizations that were crucial to our evaluation and will play key roles in CSU's CMMC certification.

Information Technology Organizations

The *Division of Information Technology (DoIT)* serves as the central IT organization for CSU. The Division is responsible for delivering enterprise services for the CSU System and campus-focused technology services for the Fort Collins and Pueblo campuses. Examples of the services provided by DoIT include Communication & Collaboration, Desktop & Mobile Computing, Infrastructure & Network, Research Computing, Information Security, and Teaching & Learning.

In addition to DoIT, various colleges and departments across CSU Fort Collins fund and maintain their own separate IT departments. These IT departments maintain autonomy over their respective IT personnel, infrastructure, and systems. While CSU has implemented organization-wide IT policies, it places the responsibility on colleges and departments to ensure compliance with all relevant laws and regulations.

Research Organizations

The *CSU Office of the Vice President (VP) for Research* (Office) serves as the University's central hub, providing strategic leadership, resources, and support for facilitating research across the CSU System. Within the Office, other divisions or departments also reside that were crucial to our evaluation including the following:

- The *Division of Research IT Strategy & Operations* provides services for the research community that enable and assist CSU research, instruction, and diversity. Since July 2023, personnel within this group have taken lead roles in promoting and coordinating the University's preparations for CMMC.
- The *Division of Research Administration & Operations* includes the *Office of Sponsored Programs (OSP)* department, which is responsible for overseeing the research award lifecycle at CSU Fort Collins. As the primary coordinating office for externally funded research activities, the OSP represents the University for those involved in sponsored activities, including its contracts with the DoD.
- The *Division of Research Integrity & Compliance* aids researchers, staff, and oversight committees in the following areas (1) protection of human participants in research, (2) protection of the use of animals in research, teaching, and demonstration, (3) oversight of activities involving potentially biologically hazardous materials, (4) responsible conduct of research, (5) conflict of interest and conflict of commitment, and (6) quality assurance standards in research and manufacturing activities. The *Secure & Global Research Office* resides within the Division of Research Integrity & Compliance and aids investigators in navigating federal regulations related to export controls, controlled unclassified information, classified research, and common access cards.

Principal Investigators

In addition to the groups outlined above, the University's Principal Investigators (PIs) play an essential role in the protection of sensitive data and information related to national security. These individuals, who can be found within any college or division of the University, are often referred to as the faculty, investigator, or project director on a research contract. They are identified by CSU or the contract awarding organization as having the level of authority and responsibility to direct the sponsored project or program. It is important to note that PIs may not report directly to the research department, but their oversight is crucial for ensuring expenditures are in accordance with sponsor and University regulations, policies, and procedures and they are responsible for regulatory compliance, effort reporting, and technical reporting back to the sponsor.

Evaluation Objectives, Scope, and Methodology

We conducted this performance evaluation pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct performance, financial, and information technology audits of all departments, institutions, and agencies of the state government. Our evaluation work was performed from July 2023 through April 2024, and we appreciate the cooperation and assistance provided by the University's management and staff.

We conducted this performance evaluation in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate 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 evaluation objectives.

The key objectives of the evaluation include the following: (1) determine whether the CSU System is adequately prepared for the CMMC requirements and has aligned and/or enhanced its cybersecurity posture, in accordance with applicable standards, as it relates to protecting sensitive information and data related to national security received from the DoD, and (2) assess the CSU System's cybersecurity posture, as outlined in applicable standards, in order to determine whether the State has taken sufficient steps to help ensure that the State will not lose current and future DOD funding, or be in breach of DOD contracts.

To accomplish our evaluation objectives, we performed numerous evaluation activities and utilized various sampling techniques. These activities and sampling techniques are outlined in each individual finding within the report.

As required by auditing standards, we planned our evaluation work to assess the effectiveness of those internal controls that were significant to our evaluation objectives. Details about the evaluation work supporting our findings and conclusions, including any deficiencies in internal control that were significant to our evaluation objectives, are described in the remainder of this report. Any details, including any deficiencies that could expose the University's overall cybersecurity posture are included in a separate, confidential report. Specifically, Findings 2 and 3 are included in a separate, confidential report, and address deficiencies we identified in the areas of specific controls related to CMMC Level 1 and Level 2 compliance.

The scope and methodology of this CMMC Readiness Evaluation utilized the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* to assess the effectiveness of CSU's cybersecurity practices. The CMMC combines various cybersecurity standards and best practices, which map and align to NIST SP 800-171. Our evaluation focused on CSU's compliance with the security functions and practices as outlined in the NIST 800-171 and required by CMMC. The table below presents the security domains that make up the NIST 800-171 and identifies whether each security domain is included in the requirements for CMMC Level 1 or Level 2.

Security Domain	Level 1	Level 2
Access Control	✓	✓
Awareness and Training		✓
Audit and Accountability		✓
Configuration Management		✓
Incident Response		✓
Identification and Authentication	✓	✓
Maintenance		✓
Media Protection	✓	✓
Physical Protection	✓	✓
Personnel Security		✓
Risk Assessment		✓
Security Assessment		✓
System and Communications Protection	✓	✓
System and Information Integrity	✓	✓

A draft of this report was reviewed by CSU. Obtaining the views of responsible officials is an important part of ensuring that the report is accurate, complete, and objective. We, along with the Colorado Office of the State Auditor (OSA), were responsible for determining whether and how to revise the report, if appropriate, based on CSU's comments. The written responses to the recommendations and the related implementation dates were the sole responsibility of CSU.

CHAPTER 2
PUBLIC FINDINGS AND INFORMATION

Finding 1: CMMC Program Management

For many institutions, a successful Cybersecurity Maturity Model Certification (CMMC) requires organization-wide changes to IT operations and practices. It is critical that institutions like the Colorado State University System (CSU or University) tackle CMMC with a unified approach, or they risk failure or mismanagement of resources. Accordingly, it would be prudent for institutions to consider CMMC and the changes it necessitates as an organization-wide program and grant the program the necessary components for successful implementation. These components should include the establishment of authority, roles and responsibilities, awareness and training programs, and compliance monitoring.

The University comprises three campuses (Fort Collins, Pueblo, and Global), each serving unique roles and missions. Presently, only Colorado State University – Fort Collins (CSU-Fort Collins) holds active contracts with the Department of Defense (DoD). The Office of the Vice President for Research at Colorado State University – Fort Collins oversees the management of ongoing DoD contracts. Principal Investigators (PIs) are faculty members within the University who are accountable for conducting the research and executing the projects. They are typically the primary contacts with the DoD and report to their respective colleges within the University.

The CMMC requires CSU to identify a senior-level official who has responsibility for ensuring compliance with CMMC Program requirements. This individual will also be responsible for submitting the annual affirmation to the DoD confirming the organization's continuing compliance with the specified CMMC security requirements.

The Federal Acquisition Regulations (FARs) and Defense Federal Acquisition Regulation Supplement (DFARS), upon which the CMMC is built, state that to be considered for an award with the DoD, CSU is required to implement the National Institutes of Standards and Technology's (NIST) Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, and have a current assessment, "…for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order." This assessment cannot be more than three years old. The DFARS then defines requirements for CSU to submit the results of their assessment showing compliance with NIST SP 800-171 through the Supplier Performance Risk System (SPRS), an online procurement analysis tool maintained by the DoD to assess contractor risk.

CSU's contracts with the DoD provide CSU researchers with access to a variety of potentially sensitive information that include both Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). Accordingly, the identification and protection of both types of information throughout the University is critical to meeting the requirements outlined by the CMMC. The University relies upon its PIs to ensure the information obtained or created in connection with these DoD contracts is handled in accordance with federal regulations and contractual requirements. Since the breadth of individuals involved in this research cannot be limited to a specific college or office, it is critical that the

University adopt a broad approach for educating relevant personnel on the identification and protection of sensitive information.

Residing within the CSU-Fort Collins's Office of VP for Research is the Office of Sponsored Programs (OSP). The OSP is responsible for overseeing the research award lifecycle at CSU Fort Collins. As the primary coordinating office for externally-funded research activities, the OSP represents the University for those involved in sponsored activities. The OSP has established extensive procedures and practices for pre-award activities, which include Proposal & Budget Development, Proposal Review & Submission, and Award Receipt & Negotiation. Once a contract has been executed, the OSP performs contract monitoring procedures; however, these procedures are primarily focused on financial management. OSP relies upon a contract's designated PI to oversee compliance with any other requirements of the contract, including requirements for the identification and protection of sensitive information.

What work was performed and what was the purpose?

To conduct our assessment and support our conclusions, we conducted interviews with CSU administrative staff at the Fort Collins, Pueblo, and Global campuses. We also interviewed research personnel at the Fort Collins campus that had contracts with the DoD. The purpose of these interviews was to understand the policies and practices in place for managing information security and research. Specifically, we:

- Evaluated applicable institutions' policies and procedures related to data security, awareness and training, and sponsored programs.
- Examined the current trainings provided to researchers and support personnel.
- Analyzed the CSU Fort Collins contract award lifecycle managed by the OSP.
- Assessed the ability of researchers and supporting staff to identify FCI and CUI, in accordance with federal standards and their understanding of measures for the protection of such information.

The purpose of the work performed was to evaluate CSU's design and implementation of control activities related to the overall implementation and management of program and activities critical to the CMMC.

What problems did the work identify and how were the results measured?

We identified the following problems with the program management activities CSU has established to prepare for and comply with the requirements of the CMMC:

1. **CSU had not established a centralized governing authority responsible for establishing uniform standards for information technology (IT) security across all colleges and departments.** The CSU Division of IT (DoIT) provides standards and assistance to the University at large, and some colleges and departments look to DoIT for guidance and support. However, governance and oversight for IT security is currently distributed across various IT teams within the University's colleges and departments. A significant portion of these colleges and departments are overseen by internal resources, independent of DoIT.

Section 24-37.5-404.5(2)(c), C.R.S., states that each institution of higher education, in coordination with the department of higher education, shall develop an information security program. The information security program shall provide information security for the communication and information resources that support the operations and assets of the institution of higher education. The information security program shall include (summarized): periodic risk assessments, ensuring adequate security for communication and information resources, providing awareness training for employees, administrators, and users, conducting annual testing and evaluation of security effectiveness, establishing a process for detecting and responding to security incidents, and developing plans for the continuity of operations in the event of a security incident.

Standards for Internal Control in the Federal Government (Green Book) that are published by the U.S. Government Accountability Office and considered a leading industry internal control framework, states in Principle 14.3 that management should communicate quality information down and across reporting lines to enable personnel to perform key roles in achieving objectives, addressing risks, and supporting the internal control system. In these communications, management should assign the internal control responsibilities for key roles.

NIST Cybersecurity Framework Governance ID.GV-3, states that legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are to be understood and managed.

Control Objectives for Information and Related Technology (COBIT) 5 MEA03.01, Identify External Compliance Requirements, states that on a continuous basis, the entity should identify and monitor for changes in local and international laws, regulations and other external requirements that must be complied with from an IT perspective.

2. CSU had not identified the senior official who will be responsible for ensuring the University's compliance with CMMC Program requirements and who will submit the annual CMMC affirmation to the DoD confirming the organization's continuing compliance with the specified CMMC security requirements.

When the CMMC was initially announced by the DoD in 2021, CSU placed responsibility for meeting the requirements of this new initiative under the DoIT. In 2023, the University transitioned this responsibility from DoIT to the Office for the Vice President of Research. At the time of our assessment, a senior official responsible for ensuring CSU's compliance with CMMC Program requirements had not been identified.

32 Code of Federal Regulations (CFR) Part 170 (DRAFT), released by the DoD's Office of the Department of Defense Chief Information Officer (CIO) states, "A senior official from the prime contractor and any applicable subcontractor will be required to annually affirm continuing compliance with the specified security requirements."

32 CFR Part 170 (DRAFT), released by the DoD's Office of the Department of Defense Chief Information Officer (CIO) states, "All CMMC affirmations shall be submitted by the Organization Seeking Assessment (OSA) senior official who is responsible for ensuring OSA compliance with CMMC Program requirements."

Green Book Principle 3.06 states that, to achieve the entity's objectives, management should assign responsibility and delegate authority to key roles throughout the entity.

3. **CSU had not identified an individual who will be responsible for accessing and submitting reports through the DoD's Supplier Performance Risk System (SPRS).**

   DFARS 252.204-7019 states that contractors (i.e., CSU), "…shall verify that summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) are posted in the Supplier Performance Risk System (SPRS) for all covered contractor information systems relevant to the [contractor]."

   Green Book Principle 3.06 states that, to achieve the entity's objectives, management should assign responsibility and delegate authority to key roles throughout the entity.

4. **CSU had not established a formal training program to educate appropriate personnel on policies and procedures for identifying and handling FCI and CUI.**

   NIST SP 800-171 Control 3.2.2 states organizations, or CSU, should ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

   Green Book Principle 4.05 states that management should enable individuals to develop competencies appropriate for key roles, reinforce standards of conduct, and tailor training based on the needs of the role.

   Federal Information System Controls Audit Manual (FISCAM) Control SM-3.1 states that management should ensure that employees—including data owners, system users, data processing personnel, and security management personnel—have the expertise to carry out their information security responsibilities.

   NIST Cyber Security Framework Practice AT-1 states that all users should be informed and trained on their security responsibilities.

   NIST SP 800-53, Security and Privacy Controls for Information Systems and Organization, Control AT-2a states that organizations should provide security and privacy literacy training to system users (including managers, senior executives, and contractors).

5. **CSU had not established formal, post-award procedures to ensure that appropriate controls are in place to guarantee compliance with Federal Acquisition Regulations (FARs) and DFARS related to CMMC.**

   During interviews with OSP management, they explained that it is the responsibility of PIs to ensure they comply with any regulatory requirements outlined in their contracts with the DoD. However, when we questioned PIs about the monitoring of compliance with the requirements stipulated in their DoD contracts, the PIs stated that they were under the impression that this was the responsibility of the OSP.

Green Book Principle 3.06 states that, to achieve the entity's objectives, management should assign responsibility and delegate authority to key roles throughout the entity.

32 CFR Part 170 (DRAFT), released by the DoD's Office of the Department of Defense Chief Information Officer (CIO) states that monitoring of compliance with the terms of a contract with the DoD is the responsibility of the contractor (i.e., CSU), with the government contracting officer.

Why did the problems occur?

We identified the following causes for the problems identified:

CSU explained that the absence of defined roles in response to CMMC requirements was due to ambiguities in the timing and expectations of these requirements from DoD. Additionally, they explained that the lack of assigned responsibility for accessing SPRS stemmed from the departure of the previously designated individual in August 2023 with no replacement appointed. Furthermore, CSU attributed the deficiency in formal, post-award procedures for ensuring compliance with DoD requirements to understaffing and insufficient resources. However, it is important to note that most of the issues identified in this finding are based upon requirements and regulations that have existed independent of the CMMC and should have already been met by CSU.

Why do these problems matter?

The lack of a cohesive governance structure for information security not only has implications for the University's compliance with IT security standards but also increases the risk of inconsistent security measures across campuses, leaving certain areas more susceptible to threats. Moreover, the decentralized nature of resource allocation may lead to inefficiencies and hinder alignment with comprehensive IT security compliance standards across all operational sites.

The official responsible for leading and managing CSU's engagement in the CMMC assessment holds critical importance due to their role as the decision-making authority for the Organization Seeking Assessment (OSA) in this context. This individual not only guides the OSA through the intricacies of the assessment process, but also makes pivotal decisions that impact the University's compliance posture. In addition, their leadership ensures a cohesive and strategic approach to meet CMMC requirements, facilitating effective communication, coordination, and implementation of cybersecurity measures.

Implementing a formal training program for personnel on the identification and handling of FCI and CUI is crucial for organizational cybersecurity. Such a program ensures that employees are well-informed about the specific policies and procedures related to FCI and CUI, reducing the risk of inadvertent mishandling or unauthorized disclosure of sensitive information. This proactive approach not only enhances compliance with security standards, but also reinforces a culture of cybersecurity awareness and responsibility throughout the University, ultimately mitigating the potential impact of security breaches and contributing to the overall resilience of the organization's information infrastructure.

By implementing robust post-award measures, the University can ensure their practices align with the specific cybersecurity requirements outlined in FARs and DFARS, as well as adhere to the standards set

forth by CMMC. These procedures would provide a systematic framework for monitoring and enforcing the required controls after securing a government contract.

Recommendation No. 1:

The Colorado State University System (CSU) should improve program management controls and ensure compliance with Cybersecurity Maturity Model Certification (CMMC) requirements by:

A. 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.

B. Identifying the senior official who will be responsible for ensuring compliance with CMMC Program requirements and who will submit the annual CMMC affirmation.

C. Identifying an individual who will be responsible for accessing and submitting reports through the Department of Defense's Supplier Performance Risk System.

D. 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.*

E. 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.

Agency Responses:

Recommendation No. 1:

A. **Agree. Implementation Date: December 2024.**
A formal IT governance model is under development and will be implemented. A central authority responsible for defining and enforcing uniform IT security standards across all campuses will be appointed within the formal IT governance model.

B. **Agree. Implementation Date: April 2024.**
The CSU System Chief Information Security Officer (CISO) has been identified as the senior official responsible for ensuring compliance with CMMC requirements and will submit the annual CMMC affirmation.

C. **Agree. Implementation Date: April 2024.**
The CSU Senior Director for Research IT will assess and submit reports through the Department of Defense’s Supplier Performance Risk System (SPRS).

D. **Agree. Implementation Date: December 2024.**
An awareness training program for researchers is in development. The Office of the Vice President for Research will ensure it includes information about safeguarding Controlled Unclassified Information (CUI) and Federal Contract Information (FCI).

E. **Agree. Implementation Date: December 2024.**
CSU's Office of the Vice President for Research will establish a post-award procedure to ensure appropriate controls.

Glossary

Access Control

The implementation of policies and measures to regulate and restrict access to systems, networks, and data, ensuring that only authorized entities can interact with specific resources.

Awareness and Training

The process of educating and informing individuals within an organization about security policies, procedures, and best practices to enhance their understanding and promote a security-conscious culture.

Audit and Accountability

The systematic collection, analysis, and recording of security-related activities to provide a comprehensive record for monitoring and investigating security incidents.

Certified Third-Party Assessor Organization

An accredited entity authorized to assess and verify the cybersecurity posture of organizations, typically for compliance with specific standards or regulations.

College

A specialized academic unit or division within the larger university structure. These colleges are often organized based on academic disciplines or fields of study, and they may house multiple departments or schools related to a specific subject area.

Configuration Management

The disciplined process of planning, identifying, and controlling changes to hardware, software, and system configurations to maintain security and operational integrity.

Control Family

A group of security controls within a framework or standard that addresses specific aspects of information security.

Controlled Unclassified Information (CUI)

Information that requires safeguarding or dissemination controls, as designated by federal laws, regulations, or government policies.

Cyber Hygiene

Best practices and habits individuals and organizations adopt to maintain good cybersecurity, including regular software updates, secure password practices, and awareness of online threats.

Cybersecurity

The practice of protecting or defending the organization's systems, networks, programs, data, etc. from cyberattacks, whether criminal or unintentional unauthorized access.

Cybersecurity Maturity Model Certification (CMMC)

A framework developed by the U.S. Department of Defense to ensure that contractors and suppliers within the defense industrial base meet specific cybersecurity standards and practices based on their handling of sensitive government information.

Cybersecurity Posture

The overall strength and effectiveness of an organization's cybersecurity defenses, practices, and preparedness against cyber threats.

Cybersecurity Practices

The set of strategies, protocols, and measures designed to protect computer systems, networks, and data from unauthorized access, attacks, and damage.

Defense Federal Acquisition Regulation Supplement (DFARS)

A set of regulations that extends and supplements the Federal Acquisition Regulation (FAR), specifically addressing the needs of the Department of Defense in federal acquisitions.

Defense Industrial Base (DIB)

A collective term for the companies and individuals involved in the production and maintenance of goods and services essential for national defense.

Department

an organizational unit within a college or faculty that focuses on a specific academic discipline or field of study.

Department of Defense (DoD)

The executive department of the U.S. federal government responsible for coordinating and supervising all agencies and functions related to national security and the armed forces.

Federal Acquisition Regulations (FARs)

A set of rules and guidelines governing the acquisition process for the U.S. federal government.

Federal Contract Information (FCI)

Sensitive information that is not publicly available, provided by or generated for the government under a federal contract, used for the purpose of performing that contract.

Incident Response

The organized approach to addressing and mitigating security incidents, including detecting, responding to, and recovering from events that could impact the confidentiality, integrity, or availability of information.

Identification and Authentication

The process of verifying the identity of users, systems, or devices and allowing access only to authorized entities through the use of credentials and authentication mechanisms.

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Policy

A formal document that defines required security safeguards for all aspects of information systems, information technology, IT assets and data protection.

Maintenance

The ongoing activities and procedures necessary to ensure the continued effectiveness and security of systems, including regular updates, patches, and preventive maintenance.

Media Protection

Safeguarding physical and digital media assets that store or transmit sensitive information, including policies and procedures for secure handling, storage, and disposal.

National Institute of Standards and Technology (NIST)

NIST is located within the Federal Department of Commerce and develops standards that are applicable to the federal government and can be adopted by other organizations.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171

A set of guidelines and requirements published by NIST to protect Controlled Unclassified Information (CUI) in non-federal systems and organizations.

Organization Seeking Assessment (OSA)

An entity undergoing evaluation or assessment, often related to compliance, quality, or cybersecurity.

Physical Protection

The measures and controls implemented to secure physical assets, facilities, and infrastructure from unauthorized access, damage, or compromise.

Personnel Security

Policies and practices designed to ensure the trustworthiness of individuals who have access to sensitive information or are involved in security-sensitive roles within an organization.

Post-award

The phase of a project or contract that occurs after the awarding of a contract or grant.

Principal Investigators (PIs)

Individuals who lead and are responsible for the conduct of research projects, often in academic or scientific settings.

Procedures

A set of established and documented steps or guidelines designed to govern specific activities or processes within an organization.

Program Management

The process of planning, executing, and overseeing the progress and performance of a program or project.

Risk Assessment

The systematic evaluation of potential security risks, threats, and vulnerabilities to identify, analyze, and prioritize potential impacts on an organization's assets and operations.

Security Assessment

The process of evaluating and testing the effectiveness of security controls, policies, and procedures to identify vulnerabilities and assess overall security posture.

Self-Assessment

The process by which an entity evaluates its own performance, typically in the context of compliance, cybersecurity, or quality management.

Sensitive Data or Information

Information whose loss, misuse or unauthorized access to or modification of which could adversely affect the interests or the ability of the organization to conduct day-to-day operations or the privacy of individual persons.

Standard

A set of established criteria, guidelines, or specifications used to ensure consistency, quality, or compatibility in various processes or products.

Supplier Performance Risk System (SPRS)

A government database used to assess and manage the performance and risk of government contractors.

System and Communications Protection

Measures to protect information systems, networks, and data during transmission, including encryption, access controls, and safeguards against network-based attacks.

System and Information Integrity

The implementation of measures to protect against unauthorized or malicious alterations to information systems, data, and software to ensure their accuracy and reliability.

Third-party Assessment

An evaluation conducted by an external entity, independent of the assessed organization, to assess compliance, performance, or adherence to specific standards.

University

An institution of higher education that offers undergraduate and postgraduate programs across a variety of academic disciplines.