SOUTHERN CONNECTICUT STATE UNIVERSITY

Cybersecurity Maturity Model Certification

Example of a Reading Chapter from Module 3: Securing Sensitive Data

Excerpt from Module 3 Chapter

By Greg McVerry

Who took the caked marked CUI from the fridge? CMMC and Data Ownership

We have all felt the rage. You go into the fridge to grab the ooey-gooey chocolate volcano cake you brought from home, and the empty shelf laughs at you with an eerie cackle. Despite the fact that you had carefully labelled the treat, someone did not know who owned the cake, and took it for themselves.

Almost all of the guidance on Cybersecurity Maturity Model Certification (CMMC) tells you to start with determining where and how Controlled Unclassified Information (CUI) flows through your system. In other words, you begin the certification process by figuring out who decides the in-office lunch policy, and what can go in the fridge.

In addition, many clients will tell you that they are unsure of whether or not they will be sending you CUI, but still require you to have a system that supports CUI for the sake of future contracts.

Start with deciding who's in charge.

CMMC and Data Ownership

To understand the team your company brings to table, and how CUI is best managed within that team, we turn to the National Institute of Standards and Technology's Special Publication 800-18 (NIST SP 800-18). This document, which acts as a guide for developing security plans for federal information systems, begins by outlining where the buck stops in the context of CUI.

The first question NIST SP 800-18 asks is this: what is Management Operation?

In order for your cybersecurity plans and practices to adequately reflect the protection of vital resources, a senior management official must authorize your system. The authorization of a system to process certain kinds of information, granted by a management official, provides an important quality control. By manually authorizing processing within a system, the manager acknowledges and accepts its associated risks.

Therefore, before you can begin to determine how you want CUI to flow through your personnel and systems, you have to know who will act as this senior management official. In other words, you have to decide who will sign the dotted line.

Roles and Responsibilities

Management authorization should be based on an assessment of management, operational, and technical controls.

1. Security Officer
2. Information Systems Owner
3. Information Owner

According to NIST, you begin by appointing a Chief Information Officer (CIO).

The CIO is the agency official responsible for developing and maintaining an organization-wide information security program. This individual has several responsibilities for system security planning.

Most small manufacturers do not have a CIO. It is likely that they employ a Managed Service Provider, or that their CEO takes on the position. Sometimes companies choose a random, yet convenient employee for the job; Deborah in accounting, for example, because of her years of experience managing a WordPress site for her GoBots collection. But usually, it's just you. Which means take on the following responsibilities:

- The CIO chooses the senior agency information security officer (probably also you, an MSP, or Deborah)
- Develop all the security procedures and policies (likely a copy and paste exercise from SANS templates)
- Do all of the cybersecurity stuff
- Do all of the cybersecurity training stuff.

The Information Systems Owner (ISO), according to NIST, keeps all of your wifi and printers going. This is also, most likely, just you. The ISO is responsible for the overall procurement, development, integration, and modification—plus the operation and maintenance—of the information system. This means that they are required to:

- Write the system security plan
- Maintain and monitor the system security plan
- Ensure employees attend cybersecurity training
- Update the system security plan
- Help with implementing practices and processes.

In the context of CUI, the information owner is most often the Department of Defense, except in the case of Intellectual Property. But in terms of your company, you need to know who:

- Establishes the roles and rules
- Helps with security
- Decides who gets access to sensitive information.

NIST SP 800-18 lists a few other positions, but we have already described three jobs past the typical organization's headcount (Deborah quit when saw she had to do government-level controls on private sector budgets).

It is important to note that NIST wrote the guide to developing security plans for the government, not for your small business. Just remember that you do need to decide who acts as the authorizing agent. Ask yourself, who:

- Decides our System Security Plan (SSP) is good to go
- Authorizes the information system
- Denies access to the information system.

When you begin your CMMC journey, it is crucial for you to determine who gets to play boss of the SSP, the information system, and all of the people involved. If you fail to do this, your chocolate lava cake will undoubtedly be taken from the fridge without your permission.

Example of a Participating Task from Module One: Introduction to CMMC

Module One – Participating Task Description & Rubric

Create a one-page flyer explaining the CMMC program for a manufacturing defense contractor and a flyer for a Manage Service Provider.

OR

Develop a blog post or company memo defining Cybersecurity Maturity Model Certification.

Based on the information in Module One regarding Federal Contract Information (FCI), Controlled Unclassified Information (CUI), and the CMMC and its history, you will create two different one page flyers or a blog post to convey this information to two different groups:

- Manufacturing Defense Contractor
- Managed Service Provider

You can use Microsoft Word or blog post to develop these flyers. Throughout the creation process, consider the most important pieces of information for these two groups.

Please review the scoring rubric below to ensure that you include all the necessary information within the participating task.

Participating Task Rubric

3 points	**2 points**	**1 point**
The CMMC origin, levels, practices, and processes are all described as they pertain to a Manufacturing Defense Contractor and a Managed service provider. Depictions of information are clear, concise, and pertinent to target groups.	Some of the relevant CMMC origins, levels, practices, and processes are missing, have inaccurate information, or are not described as they apply to a Manufacturing Defense Contractor and a Managed Service Provider in 1-3 components.	The CMMC origin, levels, practices, and/or processes have more than 3 inaccuracies or missing components. The information is not tailored to the needs of the two target groups.

Example of a Reading Task from Module Two: History of CMMC

Module Two – Reading Task

While you are reading President Biden's Executive Order, "Deliver Uncompromised" by Nissen, et al. (2018) and watching the module videos, complete the following Semantic Feature Analysis.

The purpose of this activity is to synthesize the Module Two Materials, as well as to support your performance task at the end of the module.

The table below is a Semantic Feature Analysis chart. Its purpose is to explore how concepts are related to each other, and to make connections between essential concepts. To complete the chart, please add the date and purpose of each term in the first two columns. In the remaining columns, you will indicate how the concepts in Column A align to the areas listed in the grey columns. Place a "+" in the matrix when the concepts align. Place a "—" in the matrix if they do not.

Column A	Date	Purpose	All Contractors	Defense Contractors	Federal Contract Information (FCI)	Controlled Unclassified Information (CUI)
Federal Information Security Modernization Act (FISMA)						
Risk Management Framework (RMF)						
FedRAMP						
FAR Clause 52.204-21						
DFARS Clause 252.204-7012						
National Institute of Standards and Technology (NIST) SP 800-171						
National Institute of Standards and Technology (NIST) SP 800-172						