Cross Collaboration Between ATE Projects and Centers in Developing Interactive Student Activities

Corrinne Sande
Principal Investigator (PI) and Director
Whatcom Community College, Bellingham, WA
Director of Computer Science and Information Systems

Dr. John Sands
Director and PI – National Center for Systems Security and Information Assurance (CSSIA)

Michael Qaissaunee
PI – E-MATE 2.0 Project

This material was developed with funding from the National Science Foundation under Grants #1601612 and #1500375

E-MATE 2.0
Building Capacity for Interactive Teaching and Learning

NSF
Funding & Vision

Content development

Scheduling & Logistics

Interacts (E-MATEs)
This workshop was made possible by funding from the National Science Foundation.

CMMC Orientation Training

Developed and produced by:

NSSCIA
National Support Center for Systems Security and Information Assurance
What is the CMMC?

- **Cybersecurity Maturity Model Certification**
- Will encompass multiple maturity levels that ranges from “**Basic Cybersecurity Hygiene**” to “**Advanced/Progressive**”.
- Intent: incorporate CMMC into Defense Federal Acquisition Regulation Supplement (DFARS) and use as a requirement for contract award.
- DOD planning to migrate to the new CMMC framework this year.
- Created by the Office of Under Secretary of Defense for acquisition and sustainment to protect **Unclassified Controlled Information (CUI)**.
- Applies to Defense Industrial Base (DIB) supply chain.

*The DoD defines process maturity as “the extent of institutionalization of practices within an organization.”

The most recent CMMC model framework is Version 1.02 (March 2020).
Purpose of CMMC

• Enhance and improve the cybersecurity posture of the Defense Industrial Base (DIB).

• Serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene and protect controlled unclassified information (CUI) that resides on the Department’s industry partners’ networks.
Who does the CMMC directly effect?

• CMMC applies to **all DOD contractors** and **subcontractors that are servicing DOD contracts**.
  • Includes **full-time**, **part-time**, and **temporary contractors** that may be in scope of servicing the DOD contract.

**Note:** **subcontractors may not have to meet the same level of CMMC requirement as the prime.**
  – The CMMC maturity level for a subcontractor will be based on the type of work and service they are doing to support the contract.
Who tracks progress and status?

- The **CMMC Accreditation Body**, in partnership with DOD, will have a central CMMC marketplace, and only DOD will have access to all defense industrial base companies’ certification.
- The marketplace will also include all the firms that are CMMC Third-Party Assessor Organizations (C3PAOs).
- Per the DOD, the results of a CMMC assessment and companies’ certification level will not be made public; "the only information that will be publicly available is that your company has a CMMC certification."
CMMC Model Framework

The CMMC model has five defined levels, each with a corresponding set of practices and processes.

• **Level One** - ~80% of current contractors will just need level one of the CMMC model for most contracts. (need to demonstrate just practice)

• **Level Two** - will not be required; a transitional level to level three.

• **Level Three** - requires an organization to accomplish all 800-171 requirements and 20 additional practices.
  • This will allow access to CUI.

• **Level Four and Five** - reserved for DoD special programs; consist of proactive and progress practices.

  Contractors must meet both associated practices and processes to achieve each specific CMMC level.
• Defines cybersecurity practices at the highest level by **domains**.

• Each domain is segmented by **capabilities**.

• **Capabilities** identify contractor achievements that ensure cybersecurity within each domain.

• Demonstrate compliance with required capabilities by showing adherence to **practices and processes** mapped across the five maturity levels of CMMC.

• **Practices** measure the technical activities necessary to achieve compliance with a given capability requirement; **processes** will measure the maturity of a company’s process.
What is a CMMC Practice?
A security or CMMC practice is an action or activity that results in improving the security of an information asset.
• There are 173 practices mapped across the five CMMC maturity levels.
• They are accumulative.

Example:
• Ensuring doors are locked, passwords are properly implemented, materials are properly labeled.
What is a CMMC Process?

A **process** is a series or set of activities that interact to produce a result; it may occur once-only or be recurrent or periodic.

As it applies to CMMC the processes are the activities and actions that enable an organization's capabilities.

There are 5 levels of practices.
The CMMC model consists of **17 domains**. Many of these CMMC domains originated from the Federal Information Processing Standards (FIPS) 200 security-related areas and the NIST SP 800-171 control families. The current CMMC model also includes Asset Management (AM), Recovery (RE), and Situational Awareness (SA) domains.
The pyramid diagram illustrates the levels of processes and practices in cyber hygiene.

- **Level 1**: Basic Cyber Hygiene
  - Performed

- **Level 2**: Intermediate Cyber Hygiene
  - Documented

- **Level 3**: Good Cyber Hygiene
  - Managed

- **Level 4**: Proactive
  - Reviewed

- **Level 5**: Advanced/Progressive
  - Optimising

The numbers 171, 156, 130, and 72 likely represent the number of entities or cases at each level.
A capability is the ability to perform or achieve certain actions or outcomes. With CMMC, capability represents performing or achieving certain actions/outcomes in terms of proving a specific level of maturity in the organizations ability to protect information and the systems that host information.
Examples of capabilities include:
- Identify and document assets
- Control remote system access
- Detect and report events
Process Maturity Levels

<table>
<thead>
<tr>
<th>Process Maturity Level</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ML 1: Performed</td>
<td>There are no maturity processes assessed at ML 1. A Level 1 organization performs Level 1 practices but does not exhibit process institutionalization.</td>
</tr>
</tbody>
</table>

- Performance
- Documented
- Managed
- Reviewed
- Optimized
<table>
<thead>
<tr>
<th>Process Maturity Level</th>
<th>Processes</th>
</tr>
</thead>
</table>
| ML 3: Managed         | 1. Review [DOMAIN NAME] activities for adherence to policy and practices.  
                         2. Provide adequate resources to meet the plan for [DOMAIN NAME] activities. |

Process Maturity Levels

- Optimized
- Performance
- Reviewed
- Documented
- Managed
Process Maturity Levels

<table>
<thead>
<tr>
<th>Process Maturity Level</th>
<th>Processes</th>
</tr>
</thead>
</table>
<pre><code>                    | 2. Review the status and results of [DOMAIN NAME] activities with higher level management and resolve issues. |
</code></pre>
<p>| Documented             |           |
| Managed                |           |
| Reviewed               |           |
| Performance            |           |
| Optimized              |           |</p>
Process Maturity Levels

<table>
<thead>
<tr>
<th>Process Maturity Level</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLS: Optimized</td>
<td>1. Standardize a documented approach for [DOMAIN NAME] across all applicable organizational units.</td>
</tr>
<tr>
<td></td>
<td>2. Share identified improvements to [DOMAIN NAME] activities across the organization.</td>
</tr>
</tbody>
</table>

- Optimized
- Performance
- Reviewed
- Documented
- Managed
These online interactive lessons are provided as a resource for faculty and teachers to incorporate into their cybersecurity classes. They are designed to help students grasp difficult concepts by interacting with the content, navigating through pages, selecting options, completing activities, and answering questions. Self-assessments are often provided, either at the end of an interactive lesson or on a separate web page.

The interactive lessons on NCyTE.net have been developed through funding from National Science Foundation grants to Brookdale Community College in Lincroft, New Jersey, and Whatcom Community College in Bellingham, Washington.
Cross Collaboration Between ATE Projects and Centers in Developing Interactive Student Activities

Corrinne Sande
CSande@whatcom.edu

Dr. John Sands
sands@morainevalley.edu

Michael Qaissaunee
mqaissaunee@brookdalecc.edu

This material was developed with funding from the National Science Foundation under Grants #1601612 and #1500375