Luke is a Senior Manager at Echelon and brings over 12 years of professional experience to our clients. He is an experienced management consultant with an extensive background in the development and implementation of Cybersecurity, Governance, Risk, & Compliance (GRC), Third Party Risk Management (TPRM), and Business Continuity strategies. Luke has consulted with numerous clients in the financial services, insurance, manufacturing, and healthcare industries, and has a proven track record of delivering successful projects while maintaining a customer-focused approach.

He has helped many clients identify and mitigate organizational risks, compliance gaps, and audit findings by aligning with best-practice frameworks (NIST 800-171, NIST CSF, ISO 27001, HIPAA, PCI, SOC2, and HITRUST CSF). Luke has also created and implemented strategies for organizations to implement Integrated Risk and Compliance processes, procedures, and technology solutions and is well-versed in Lean Six Sigma best practices along with their application to drive process improvement using data analytics.
We take on your toughest cybersecurity, technology risk and compliance challenges so that you can focus on running your business.

**Comprehensive Cybersecurity Strategy**
Establish and execute long-term cyber strategy. Mobilize a multidisciplinary team of cybersecurity and technology risk experts.

**Offensive Security and Testing**
Develop an informed perspective of the current state of your cybersecurity and technology risk posture.

**Defensive Security**
Engineer solutions to address critical risk areas and establish processes that drive sustained improvement and raise your cybersecurity maturity.

**Audits, Assessments and Compliance**
Navigate the complexity of cybersecurity standards, frameworks and regulations.
THE AGENDA

▪ What is CMMC?
  > CMMC-Accreditation Body (AB)
  > CUI/FCI
  > DoD Internal Review

▪ CMMC 2.0
  > Framework Changes
    ▪ Model
    ▪ Assessments
    ▪ Implementation

▪ What’s Next
  > Observations
  > Concerns
  > Action Items
WHAT IS CMMC?
Enough is enough we need to protect our data!

China J-10

United States F-16
DOD CYBER ACQUISITION HISTORY

2007
- Defense Industrial Base cybersecurity program was initiated.

Executive Order 13556, establishing the need to protect Controlled Unclassified Information.

2010

2016
- DoD issues DFARS 252.204-7012 “Safeguarding Covered Defense Information and Cyber Incident Reporting” clause and NIST 800-171 r2.

CMMC development begins, NIST 800-171 r2 draft released.

2019
- CMMC v1.0 Released.

2020

DOD CYBER ACQUISITION HISTORY
The initial CMMC Standard was released in January 2020.

The CMMC program was created to help improve cyber security protection standards for companies in the Department of Defense supply chain.

Contractors and Subcontractors

The Department of Defense partnered with CMMC Accreditation Body (CMMC-AB), to organize the CMMC certification and partner ecosystem.
The CMMC’s main mission is to protect the processing, storage, or transmission, of the below types of data:

**Controlled Unclassified Information**

CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

**Federal Contract Information**

FCI is information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as that on public websites) or simple transactional information, such as that necessary to process payments.
Definitions you need to know...

**OSC** - Organization Seeking Certification

**RPO and RPs** – Registered provider organization. RPOs in the CMMC ecosystem provide advice, consulting, and recommendations to their clients.

**C3PAO** – Certified third-party assessment organizations. Organizations who are authorized to perform the certification assessment on behalf of the Department of Defense.

**SPRS System** - Supplier Performance Risk System is the source where DIB (Defense Industrial Base) companies submit their self-attestations.
Internal Review Goals

- Safeguarding sensitive information to enable and protect the warfighter
- Dynamically enhancing DIB cybersecurity to meet evolving threats
- Ensuring accountability while minimizing barriers to compliance with DoD requirements
- Contributing towards instilling a collaborative culture of cybersecurity and cyber resilience
- Maintaining public trust through high professional and ethical standards

In March 2021, the Department of Defense initiated an internal review of CMMC’s implementation.
CMMC 2.0
As a result of the 9-month internal review performed by the Department of Defense, the department released CMMC model 2.0:
CMMC 2.0 MODEL

CMMC 1.0
- 5 increasingly progressive levels from Basic to Advanced
- Levels 2 and 4 intended as transition stages between Levels 1, 3, and 5

CMMC 2.0
- 3 increasingly progressive levels:
  - Foundational / Level 1 (same as previous level 1)
  - Advanced / Level 2 (previous level 3)
  - Expert / Level 3 (previous level 5)

Requirements at Each Level

CMMC 1.0
- Requirements include cybersecurity standards and maturity processes at each level
- Cybersecurity standards consist of certain requirements from NIST SP 800-171 as well as CMMC-unique standards

CMMC 2.0
- Eliminates all maturity processes
- Eliminates all CMMC unique security practices:
  - Advanced / Level 2 will mirror NIST SP 800-171 (110 security practices)
  - Expert / Level 3 will be based on a subset of NIST SP 800-172 requirements
CMMC 2.0 ASSESSMENTS

CMMC 1.0
- Required all DoD contractors to undergo third-party assessments for CMMC compliance

CMMC 2.0
- Allows the majority of contractors, associated with Foundational/ Level 1 and a subset of Advanced/Level 2 programs, to perform annual self-assessments
- A portion of the Advanced/Level 2 programs will require triennial third-party assessments
- Expert / Level 3 programs will require triennial assessments conducted by government officials

CMMC 1.0
- DoD reviewed CMMC-AB Conflict of Interest policies

CMMC 2.0
- DoD will approve CMMC-AB’s Conflict of Interest policies
## CMMC 2.0 Implementation

<table>
<thead>
<tr>
<th>Plan of Actions and Milestones (POA&amp;Ms)</th>
<th>CMMC 1.0</th>
<th>CMMC 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No allowance for POA&amp;Ms</td>
<td>Allows the use of POA&amp;Ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Highest weighted requirements cannot be on POA&amp;M list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DoD will establish a minimum score requirement to support certification with POA&amp;Ms</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Waivers</th>
<th>CMMC 1.0</th>
<th>CMMC 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No allowance for waivers</td>
<td>Applied to entire CMMC requirement, not individual cybersecurity practices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Allowed on a very limited basis in select mission critical instances, upon senior leadership approval</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DoD program office submits a justification package that includes specified timeline and associated risk mitigation plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Timelines imposed on a case-by-case basis to achieve CMMC compliance</td>
</tr>
</tbody>
</table>
NIST SP 800-171 & 800-172 OVERVIEW

**NIST 800-171**
- Required for Level 2 Certification
- 110 Controls across 14 Practices
- Aimed to protect confidentiality of CUI
- NIST 800-171A – Assessment Methodology

**NIST 800-172**
- Required for Level 3 Certification
- 110 Controls across 14 Practices + 35 enhanced requirements
- Aimed to address Advanced Persistent Threats (APT) to ensure that at-risk data is secured on non-federal systems
- APT – adversary with sophisticated levels of expertise and significant resources
- NIST 800-172A – Assessment Methodology
WHAT NOW?

OBSERVATIONS / CONCERNS / ACTION ITEMS
1) Framework Overhaul Brings Simplicity
   ▪ Reduction of CMMC Levels from 5 to 3
   ▪ Elimination of the maturity processes
   ▪ Back to ‘basics’ of NIST 800-171, elimination of CMMC practices
   ▪ Protection of CUI magnified, protection of FCI seems subordinate

2) Who Does the Assessment Has Widely Changed
   ▪ Contractors seeking Level 1 (only FCI) will be able to self-assess
   ▪ Role of C3PAO is fairly diminished
   ▪ DoD led assessments will occur at the new Level 3

3) CMMC-AB
   ▪ CMMC-AB is not going away
   ▪ DoD website states, “CMMC-AB will accredit CMMC Third Party Assessment Organizations (C3PAOs) and the CMMC Assessors and Instructors Certification Organization (CAICO)”
1) CMMC 2.0 is What CMMC 1.0 Should Have Been
   ▪ We are basically back to where we were in 2016
   ▪ CMMC 2.0 would have been a good starting point
   ▪ Now we are 9-24 months away from it going into effect

2) Fluidity and Confusion
   ▪ Level 2 programs (those with CUI) were bifurcated during the initial release of CMMC 2.0, whereby some require triennial third-party audits, and the rest will require annual self-assessments. Now all Level 2 requires C3PAO assessments
   ▪ Level 3 programs will require triennial assessments conducted by government officials

3) Relaxed Requirements
   ▪ The maturity requirements for security processes no longer exist in CMMC 2.0, maturity requirements were necessary to build security into repeatable processes not just a checkmark on a piece of paper
   ▪ POAMs are also back, allowing contractors to kick the can down the road where they are non-compliant, good news for companies but bad for DoD cybersecurity?
1) Can’t Stop, Won’t Stop!
   - CMMC 1.0 is gone and so are the old practices. Turn the focus to NIST 800-171, it is the future
   - This is not going away, it is just taking more time
   - Use this extra time to spread out budget and effort

2) Take Advantage of Resources Available
   - DoD Project Spectrum (https://www.projectspectrum.io/) gives plenty of great resources to small and medium sizes businesses to help become compliant
   - Training videos, tool reviews, readiness checklists, etc.

3) Be Proactive, Certify Now.
   - If your organizations handles CUI and you feel you have done a lot to meet the requirements, certify now
   - Voluntarily achieve certification ahead of the requirement timeline, it just may be a strategic advantage for your business
WHY SHOULD YOU START NOW?
CMMC 2.0 (NIST 800-171) Compliance Takes Time & Money

- The process for becoming compliant with the standards set forth in NIST 800-171 may take a significant amount of time to implement depending on the size and complexity of your organization
- You can also spread the budget out over a longer period of time to better absorb the impact
- DoD has expressed intent to expedite the process, resulting in CMMC 2.0 potentially being implemented before the end of 2022
  - Once CMMC 2.0 goes into effect, all contracts will require awardees to be compliant with CMMC 2.0 at the time of award

Cybersecurity Changes Require Culture Change

- The CMMC standards demand buy-in from all the different business functions in your organization. They must all live and breathe your organizational cybersecurity standards.

Reduce Likelihood of a Disastrous Computer Incident

- The controls that your organization implements will instill counter measures that will derail a cyber criminal’s efforts to exploit your environment.

Potential Financial Incentives

- The Department of Defense is looking at opportunities to provide incentives for contractors who voluntarily obtain a CMMC 2.0 Level 2 Certification’s in the interim period
Questions?
Cyber Intelligence Weekly

A weekly newsletter sharing some of the major developments on the future of cybersecurity that you must know about!

By Dan Desko
Cybersecurity Leader | IT Risk Enthusiast | Board Advisor...

Published weekly
2,254 subscribers
Speaker Contact Information

- Luke.Wawrzeniak@echeloncyber.com