Background

Keeping Controlled Unclassified Information (CUI) secure from prying eyes is critical to our national sovereignty and economy. Yet companies that process important government data (whether directly or as a sub-contractor in the supply chain) have only been required to “self-attest” to their conformance with relevant DFARS/NIST SP 800-171 guidance.

Unfortunately, that didn’t work very well ...
The Problem

“The U.S. is losing $600 billion a year to our adversaries in exfiltrations, data rights, & R&D loss. If we were able to institute good cyber hygiene and reduce that by 10%, think of the amount of money that we could save to truly reinvest back into our partners in the industrial base that we need to stay on the competitive edge...”

KATIE ARRINGTON, FORMER SPECIAL ASSISTANT FOR CYBERSECURITY TO ASSISTANT SECRETARY OF DEFENSE FOR ACQUISITION
The Solution

CMMC will require each organization to “prove” they are fully compliant by a combination of:

1) Entering a score in SPRS
2) A Senior Official signing an attestation of conformance
3) Undergoing a C3PAO certification assessment

---

CMMC V2 Level 2: 110 Security Requirements Across 14 Security Domains

<table>
<thead>
<tr>
<th>Access Control</th>
<th>Media Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness &amp; Training</td>
<td>Personnel Security</td>
</tr>
<tr>
<td>Audit &amp; Accountability</td>
<td>Physical Protection</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Identification &amp; Authentication</td>
<td>Security Assessment</td>
</tr>
<tr>
<td>incident Response</td>
<td>System/Communications Protection</td>
</tr>
<tr>
<td>Maintenance</td>
<td>System &amp; Information Integrity</td>
</tr>
</tbody>
</table>
That's Where We Fit In...

Pivot Point Security Has “Been There & Done That” for $3B+ of Manufacturers & Suppliers...

We Have Been Helping Firms Prove They Are Secure & Compliant For Over 20 Years... It's What We Do
This isn't our first rodeo.

Our confidence comes from our experience and all that we are trusted to protect...

CMMC/800-171 for $3B+ Manufacturers

The World's Barcodes

In Car Technology for 275M+ Vehicles

100+ ISO 27001 Certifications

200+ Government Entities
Lean on Our Proven Process to Achieve CMMC Certification

1. Establish Targets, Objectives, & Resources
2. Risk Assessment
3. Categorization, Scoping & Control Assessment
4. Risk Remediation & POAMs
5. System Security Plan
6. "Soak" Phase
7. CMMC Readiness Assessment
8. Certify
9. Govern & Evolve

Can't Bid (Panic) — Can Bid (Calm)
Step #1: Establish Targets, Objectives, & Resources

Establish CMMC Level, Time-Frame, & Resourcing

Ask yourself these questions:

What CMMC Level do I need?
You may need to consult with an upstream agency or prime contractor for guidance. If you are uncertain, CMMC Level 2 achieves full 800-171 conformance and is likely your target.

When do I need to get certified by?
<6 months (if you are not 800-171 compliant already) will be a challenge.

What personnel, expertise, & financial resources do I need to get certified?
Most importantly, do you have the internal expertise and bandwidth to achieve DFARS 7012/7019/7020 or 7021 compliance in your target time frame?
CMMC “Cyber Hygiene” Certification Levels

Gain a Better Understanding of What the CMMC Level You Need Entails

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designed to protect Federal Contract Information (FCI)</td>
<td>Designed to protect Controlled Unclassified Information (CUI)</td>
<td>Designed to protect Controlled Unclassified Information (CUI) in high priority programs</td>
</tr>
</tbody>
</table>
Step #2: Scoping & Control Maturity Assessment

Understand Where Controlled Unclassified Information (CUI) Controls are Required & How to Segregate/Protect Each Asset Type

Review relevant artifacts (e.g., existing policies, network diagrams) and conduct scoping interviews to understand how your CUI flows to, within, and from your organization. At the same time assess the maturity of CMMC relevant controls. Use this information to categorize and classify your assets and establish the scope of your CMMC SSP.
Step #3: Risk Assessment

Know (& Prove to the CMMC Assessor) That All Key Risks to CUI are Understood and Effectively Managed

Establishing a repeatable methodology for, and conducting a Risk Assessment no less than annually, is a CMMC requirement. Leverage the results of the Scoping/Control Maturity Assessment to identify control implementation gaps that are leaving you at an “unacceptable” level of risk and/or non-compliant with CMMC.
Step #4: Risk Remediation & POAMs

Build & Execute the Risk Treatment Plan That Will Lead to Successful CMMC Certification

Leverage the Risk Assessment to determine and identify/document the control implementation gaps that need to be addressed for you to move you to your target state into an actionable Risk Treatment Plan.
Roles of Users and Number of Each Type:

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Number of Administrators Privileged Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>3</td>
</tr>
</tbody>
</table>

Description of Information: Engineering, Inc. processes, stores, and transmits Technical Information, DoD Critical Infrastructure Security Information, Propulsion Information, and Unclassified Controlled Nuclear Information.

ENVIRONMENT

Inc. designs and manufactures motion control components for the Defense industry, and manufacturing take place in both our Boca Raton, FL and Needham, MA facilities. Our company also hosts servers that process and store CUI in AWS Govcloud.

Step #5: System Security Plan (SSP)

Document “How” Your CMMC Compliant Systems Protects CUI

CMMC requires that you develop an SSP that “provides an overview of the security requirements of the system, describes the controls in place for meeting those requirements and delineates responsibilities and expected behavior of all individuals who access the system.”
Step #6: “Soak” Phase

SPRS & Time to Build The Evidence for Your C3PAO Assessment or Self Attestation

With your SSP documented, your controls in place, and POAM’s for those controls that still are in progress, you are ready to get a score in SPRS to meet your DFARS 252.204.7019/7020 requirement. As you work through POAM’s you will update your score in SPRS to reflect your current status.

A CMMC assessor will be looking for at least two forms of objective evidence that each of the 110 practices is operated in a “persistent and habitual” manner.
Step #7: CMMC Readiness Assessment

Document “How” Your CMMC Compliant Systems Protects CUI

Ensuring you have what you need for a successful CMMC certification assessment or your self attestation is best done by validating your readiness via a readiness assessment. Just make sure the person (inside your organization or outside) is objective enough to audit the environment and is either an accredited Registered Practitioner (RP), Certified CMMC Professional (CCP), or CMMC Certified Assessor (CCA).
### Control Objective

- Individual access authorizations are verified.
- Access is controlled to areas based on requirements.
- Keys, combinations, and other physical means of access control are used.
- When lost, or when individuals are transferred, combinations are changed.
- When compromised, or when individual combinations are changed, that individual is credited.
- Visitors are issued a physical token (e.g., ID cards) that identifies them as not on-site personnel.
- Must be surrendered before leaving the facility, and expires through automated or visual means.

### Reasonably-Expected CMMI Maturity Level

- As part of the Business Continuity Plan (BCP) for work sites.
- Plan addresses maintaining adequate systems and procedures at alternate work sites.
- Plan addresses the effectiveness of security controls at alternate work sites.
- Plan addresses the approved means for communicating with information security personnel in case of security incidents.

---

**Step #8: Attest or Get Certified**

Submit Your Attestation or Engage a C3PAO

Once the cybersecurity program has been implemented, and appropriately documented, it is CMMC Assessment and self attestation ready.
Step #9: Govern & Evolve

Maintain Your Attestation/Certification via Continuous Monitoring & Continuous Improvement

Once you attest and/or are certified you will be required to provide ongoing (yet to be formally documented) evidence that you are maintaining compliance with CMMC.
Beware of these CMMC “Gotcha's”

MDM
CUI on mobile devices must be encrypted.

Appropriate Encryption
File sharing & email need to be encrypted.

Multi Factor Authentication
Access to CUI must be via MFA even on your local network.

Logging with Alerting
Extensive audit logs need to be captured, reviewed, and alerted on.

Manage Supply Chain Risk
Managing the risk of using third parties and cloud services is integral to managing your risk.

Required Controls That Often Cause Heartburn (& May Require Significant Time & Budget)
What Would Non-Compliance With CMMC Look Like For You?

What would happen to your customer count and sales numbers if you could no longer win new DoD contracts?
What Would Non-Compliance With CMMC Look Like For You?

What about the Whistleblower act and the False Claims Act?
Are disgruntled employees a compliance risk to your organization?
Would a DIBCAC audit have civil liability implications?
If You Follow Our Proven Process, Successful CMMC Should Feel Like This...

Get excited!
You can continue to bid on and win DoD projects.

Get Even More Excited!
Not all firms that currently compete with you for DoD contracts will be successful in their CMMC pursuit, leaving you with more room to grow.

Get even more & more excited!
Reading the writing on the wall, other government agencies are considering the CMMC as their de facto standard to bid on federal contracts. You will be primed to find additional federal contract work outside of the DoD.

Life is Risky... Working with us to achieve CMMC Compliance/Certification isn’t!
CMMC Information Straight from the Source

EP#1 KATIE ARRINGTON – CMMC: WHAT YOU NEED TO KNOW ABOUT DOD CYBERSECURITY REGULATION

EP#10 STUART ITKIN – EXOSTAR AND THEIR ROLE IN YOUR CMMC CERTIFICATION

EP#22 BEN TCHOBINEH – CMMC TRAINING & ASSESSMENTS: ROLLOUT, CERTIFICATION & COMPETITION

EP#21 SANJEEV VERMA – CMMC COMPLIANCE DOESN’T HAVE TO BE HARD (OR PRICEY)

EP#17 THOMAS PRICE – CMMC CERTIFICATION AUDITS—CAN YOU LEVERAGE ISO 27001?

EP#71 GEORGE PEREZDIAZ & CALEB LEIDY - CMMC 2.0 IS HERE!
Any questions? Reach out!

📞 609-581-4600
✉️ info@pivotpointsecurity.com