



Scoping CUI the Right Way

The Foundation of an Efficient CMMC Strategy

Presented by:



Dr. Mike Crandall
CEO
Digital Beachhead



Johnathan Dean
Compliance Success Partner
RainTech



Scoping CUI the Right Way

The Foundation of an Efficient CMMC Strategy

Isn't CMMC Dead?!?!

- On 13 July 26 the DoW CIO suspended CMMC Phase 2 which was to begin 10 Nov 26
- CMMC Phase 1 is still active and will continue while a 60-day CMMC program review takes place
- DoW CIO RFI (Questions on CMMC program) responses were due 14 Aug 26 at Noon EST
- DoW will enforce cybersecurity requirements with self-assessments and select government led assessments
- False Claim Act lawsuits will continue for organizations that misrepresent compliance scoring in SPRS
- Program of Actions and Milestones (POA&M) MUST be closed out within 180 days



Scoping CUI the Right Way

The Foundation of an Efficient CMMC Strategy

Information directly from DoW CIO

- The language has softened from “suspended” to “paused” during discussion at the BlackHat conference
- Only 147 RFI responses as of 5 Aug 26 – was expected 600+
- The concern and mandate of the SECDEF is speed of manufacturing/production – resilience!
- OT equipment is not as secure as it needs to be, and the IA of CIA needs more coverage from the DIB
- Assessments do not equal security, but compliance does drive funding for cybersecurity tools
- DC3 reports significant increase in reported breaches; 81% self attested at NIST 800-171 scores of 102 or greater
- Solicitations will provide competitive advantages to those who already have been certified
 - DoW CIO Quote: "They will not be penalized for doing the right things, and their efforts will not be in vain".
- When asked if an OSC needs to “willfully” misrepresent their score in SPRS the DoW CIO stated something to the effect of if you say you are 110 and it turns out you are not then that is “willful”.



Scoping CUI the Right Way

The Foundation of an Efficient CMMC Strategy

Now back to our previous scheduled presentation

- Scoping the boundary of your assessment is a critical first step in an organization's compliance journey
- The DoW CIO website: <https://dodcio.defense.gov/cmmc/Resources-Documentation/> has valuable links to include scoping guidance and self assessment guides
- Scoping is the act of determining what is “in” and “out” of the scope of the assessment
 - This is important as it identifies where CUI is stored, transmitted or processed within your environment
 - Over scoping could add complexity, cost drivers and potential pitfalls during an assessment
 - Under scoping could result in a false scoring during assessment potentially lowering score during DIBCAC assessment
- Scoping correctly provides an accurate assessment boundary and provides a more accurate assessment scoring which can lower overall costs, limit compliance workload and speed assessment timelines



Scoping CUI the Right Way

The Foundation of an Efficient CMMC Strategy

Scoping - First Steps

- Start by understanding your current environment – Take a Cyber Inventory
 - Hardware – Endpoints (Laptops, PCs, Phones, etc), Infrastructure (Switches, Routers, APs), VoIP
 - Software – Internal, Cloud Based, Phone Apps
 - Internal connections and connectivity – I like to say if you can “ping” it then it may be in scope
 - External connections – remote access (MSP, Telework, Service Providers), Finance, CRM, Cloud, etc
 - People / Users – General Users, CUI Users, Administrators / Privileged Users, External Users
 - External Service Providers – MSP, Security Suites, SEIM/ SOC, O365/Google, Cloud Service Providers
 - Data Storage Locations to include Backups
 - CAGE Code and High Level Organization (HLO)

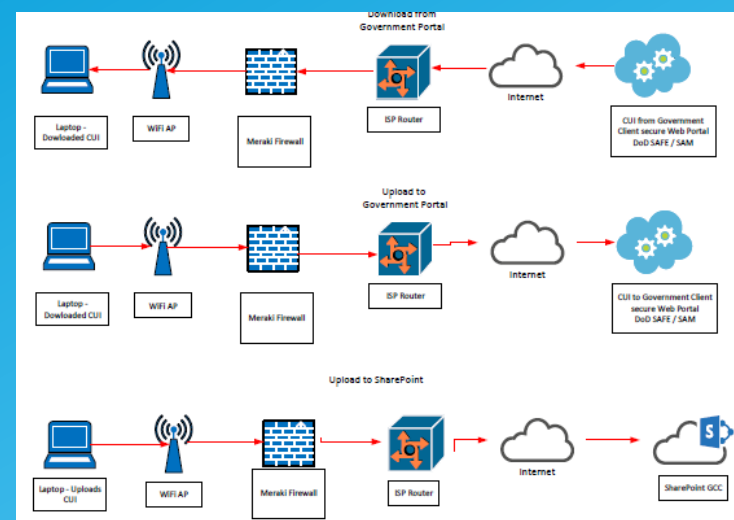


Scoping CUI the Right Way

The Foundation of an Efficient CMMC Strategy

Scoping - How does your CUI Flow

- The next scoping task is determining how your CUI flows into, out of and within your environment
- What sources of inbound CUI do you have?
 - DoD SAFE or other secure portal
 - eMAIL
 - SFTP
 - USB or other removable media
- How do you transfer CUI data out bound? (same as inbound?)
- How does CUI move within your environment?
 - Sharepoint
 - eMail
 - OneDrive (or other shared drive)
 - USB or other removable media





Scoping CUI the Right Way

The Foundation of an Efficient CMMC Strategy

Scoping - Asset Types to Assign to Inventory

- CMMC has five (5) main types of categories for assets

- CUI
- Security Protection
- Contractor Risk Managed
- Specialized
- Out of Scope

- ALL assets must be categorized

- People
- Equipment
- Physical Locations

Asset Category	Asset	Asset Quantity	Asset Type
Controlled Unclassified Information	Windows 11 Devices	66	Technology
Contractor Risk Managed	Windows 11 Devices	108	None
Contractor Risk Managed	Virtual Machine - Windows Server 2016	3	Technology
Contractor Risk Managed	Virtual Machine - Windows Server 2019	6	Technology
Contractor Risk Managed	Virtual Machine - Windows Server 2022	5	Technology
Controlled Unclassified Information	Adobe Acrobat Desktop	23	Technology
Out-of-Scope	Adobe Cloud	1	Technology
Security Protection	Cisco Secure Client	37	Technology
Controlled Unclassified Information	Procore Federal	3	Technology
Controlled Unclassified Information	Autodesk Navisworks Freedom	23	Technology
Controlled Unclassified Information	Bluebeam Revu	63	Technology
Security Protection	ConnectSecure Vulnerability Scan Agent	70	Technology
Security Protection	AutoElevate	70	Technology
Security Protection	DNS Agent	70	Technology
Contractor Risk Managed	Microsoft Teams	70	Technology
Controlled Unclassified Information	Microsoft 365 Apps for Business	69	Technology
Security Protection	Local Administrator Password Solution	64	Technology
Security Protection	Microsoft Intune Management Extension	63	Technology
Controlled Unclassified Information	Microsoft OneDrive	61	Technology
Controlled Unclassified Information	NinjaRMMAgent	60	Technology
Controlled Unclassified Information	Primavera P6 Professional	27	Technology
Controlled Unclassified Information	RMS 3 Launcher	50	Technology
Security Protection	ScreenConnect Client	70	Technology
Security Protection	RainTech MSP/MSSP Staff	17	People



Scoping CUI the Right Way

The Foundation of an Efficient CMMC Strategy

Scoping - Asset Categories Explained

- CUI: Processes, Transmit or Stores CUI data (Endpoints, Mobile Devices, Servers, Cloud, etc)
- Security Protection: Providing security services in protection of CUI (Routers, Firewalls, Switches, etc)
- Contractor Risk Managed: Are within the scoped network/environment but are meant not to process, transmit or store CUI
- Specialized: Operational Technology (OT) or other asset that performs a specialized function (typically in manufacturing)
- Out of Scope: Systems that are logically or physically separated from the in scope environment



Scoping CUI the Right Way

The Foundation of an Efficient CMMC Strategy

Scoping - Build out Network Diagram

- Take everything that has been inventoried, categorized and how the data flows and build a network diagram that demonstrates at a high level
 - Need not show ALL endpoints, users etc; instead represent each asset type on the diagram
 - SHOW Out of Scope environments and how they are separated from the in scope network
 - Include connections to External Service Providers and Cloud Service Providers
 - Include connections to external systems (DoD SAFE, Federated Networks, etc)
 - Demonstrate how subnets or other logical separations are utilized
 - Include SPAs and CRMAs and all other identified assets

Make the Diagram Easy to Read
Yet have all the information needed



Scoping CUI the Right Way

The Foundation of an Efficient CMMC Strategy

Scoping - Getting it right matters

- Under scoping
 - Could cause additional expense and potential failure during formal CMMC assessment
 - Miss areas that expose areas of weakness in implementation of controls
 - Under funding for compliance security
- Over scoping
 - Could increase assessment costs and provide unneeded reviews of systems
 - Over funding for compliance security
 - Increase in implementation costs across your enterprise

Measure twice
Cut once



Scoping CUI the Right Way

The Foundation of an Efficient CMMC Strategy

Scoping - Tips, Tricks and Rules

- If you can “Ping” it then it is in scope; Out of Scope MUST BE physically or logically separated
 - Home networks and remote work can cause hurdles (VPN, ZTN, Local and/or host Firewall)
- Think about all “possible” or “potential” places CUI can be stored, sent and/or viewed
 - Mobile devices, printers, external storage, cloud systems
- In Scope External Service Providers require a Customer Responsibility Matrix
- Starting with a detailed network and data flow diagram eases scoping discussions



Scoping CUI the Right Way

The Foundation of an Efficient CMMC Strategy



Questions



Digitalbeachhead.com



www.rain.tech