CYBERNET

AMPLIFYING HUMAN PERFORMANCE THROUGH ADVANCED TECHNOLOGY

Winning Tactics for Cybersecurity Compliance

TODAY'S PRESENTERS:

Robert Biggers & Merrilee Maxon

Company Founded in 1989

- Headquartered in Ann Arbor, MI
  - Focused on R&D
    - Robotics
    - Autonomy
    - Networking
  - 69 US Patents Granted, 17 Pending
  - Diverse Technical Engineering Staff

Cybersecurity Division founded in 2009

- Headquartered in Orlando, Fl
  - Focused on
    - DoD Cybersecurity Engineering
    - DevSecOps
    - Continuous Authorization
  - 55+ ATOs granted – System Authorizations
  - Talented DoD 8140/8570 Certified CSWF

Cybernet improves processes through the targeted application of automation and artificial intelligence.

Proprietary to Cybernet Systems

Capabilities

We are a small, American, employee-owned Cybersecurity and Research & Development organization with over 30 years of technology development and commercialization experience.

- Cybersecurity Compliance – 55+ ATOs Granted
- Secure System Integrator
- Cybersecurity Software Solutions
- Centralized Cybersecurity Management
- Advanced Cybersecurity R&D
- 8140/8570 Certified, Cleared Staff
- Army, ARNG, USMC, Navy, DHS/TSA, USACE, NAVFAC
- CONUS and OCONUS – Classified & Unclassified
- CMMC Compliance, RPO

Cybernet's mission is to develop leading edge technology and incubate innovative products for the defense & commercial industries.

Past Performance

USMC	Navy	Army	NAVFAC	US ACE
• MV-22 • CH-53K / E • AH-1 / UH-1 • RQ-7B • ADVTE • MCAT • Aircrew	• LCS 1 / 2 • LCS MBT • DDG1000 • VMPA-MCST • VMPA-PPOT • MSAT	• STE CSE • HITSv4 • MSAR • LT2-IRS • I-MILES TVS	• NAVFACC NW/SW • F-35 Hangar • F-35 OSF • NAS JRB Pharmacy replacement	• FLW Hospital • Ambulatory Care Centers

For full list visit: https://cybersecurity.cybernet.com/past-performance/

A&E Design Requirements

- Design Requirements for Design-Bid-Build and Design-Build projects come from the UFC 04-010-06

- Targets Facility Related Control Systems such as:
  - Industrial Control Systems
  - Building Automation Systems
  - Operational Technologies
  - Medical Systems

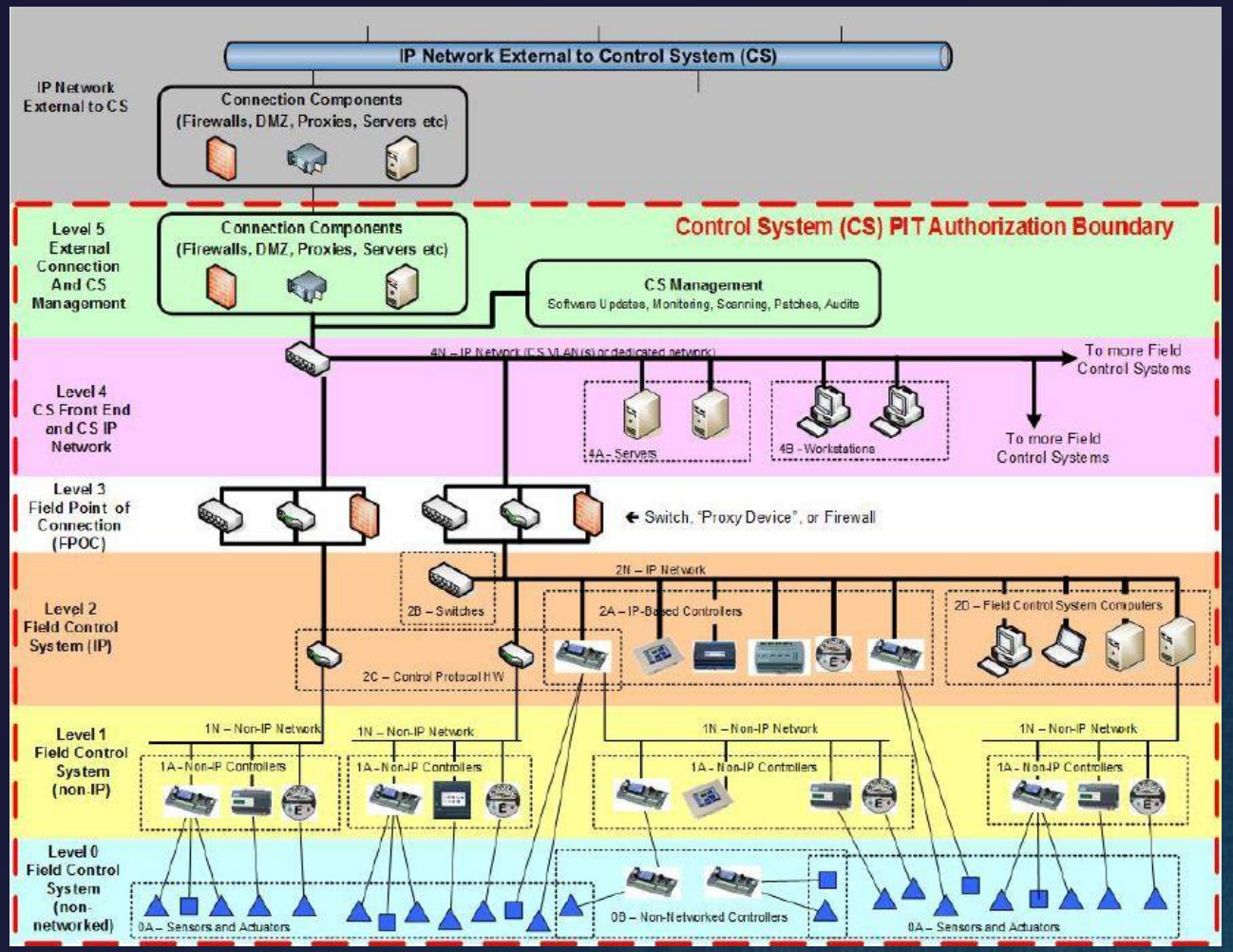
- Both networked (connected) and standalone (non-connected) systems need to be designed accordingly.

- Applies the Risk Management Framework (RMF) to building control systems.

System Type	System
Building Control Systems	Building Automation System HVAC Direct Digital Control System Elevators
ESS	Access Control System Video Surveillance System Intrusion Detection System Duress Alarm
Life Safety	Fire Detection and Alarm System Radio and Public Address System Mass Notification System
Medical	Infant Protection Alarm System Nurse Call System MedGas Alarm
Monitoring	Advanced Metering Infrastructure Generator Monitoring System Fume Hood Alarm System Lighting Control System Uninterruptible Power Supply System Utility Monitoring and Control System

Cyber Design Considerations

- Government Responsible POCs for Cyber should be identified early.
- Confidentiality-Integrity-Availability (CIA) ratings must be determined and agreed upon by the conclusion of 20% design.
- 5 Level Control System Architecture should be included with architecture drawings as soon as possible to aid Contractor-Gov't collaboration.
- The Design Team must include a Certified Information System Security Professional (CISSP).



Typical Cyber Design Process Flow

- May vary some based on project and contractor/government readiness levels.
- Determining responsible Gov't POCs to sign-off on Cyber submittals can be a challenge and should be made a project dependency by 20%.
- Riser diagrams of the proposed system architecture and interconnections need to be made available to the Cyber Designer as soon as possible for evaluation.
- Spec listings for Cyber should be included within the BOD along with any expected interconnections with new or existing system infrastructure.

Design Stage	Submittals
15% - 20%	• FRCSs identified • Client Responsible POCs identified • CIA Ratings established • Interconnections identified • BOD drafted
30% - 35%	• Control Correlation Identifier (CCI) list drafted • Initial Cyber schematics drafted • One per FRCS • BOD finalized
50% - 65%	• CCI list finalized • Cyber schematics pre-final • Cyber specs drafted • BOD revised if necessary
95% - 100%	• CCI list revised if necessary • Cyber schematics finalized • Cyber specs finalized

Scope or Work

- Cybernet has Subject Matter Experts (SMEs) that can assist your A&E firm ensure compliance with DoD standards at any stage of the project at any stage whether in Design-Bid-Build or Design-Build.

- Cybernet performs all system lifecycle Cybersecurity/Information Assurance (IA) activities
  - System Security Engineering
  - Hands on Technical Lockdown of Systems within accreditation boundary
  - Creation of Documentation Packages and updates
  - Create Cybersecurity Cold-start Documents
  - Provides Cybersecurity Training to maintain compliance
  - Participate in all System Engineering Technical Review Process (SETR) events
  - Participate in regular Integrated Project Teams (IPT)
- Provide and Setup Cybersecurity Management Software

- Assist DoD Contractors with NIST 800-171 Compliance / Cybersecurity Framework (CSF) Compliance and CMMC Readiness Review

Take Away

Cybernet Cybersecurity Services

- ✓ All staff are at a minimum CISSP or Security+ Certified for superior System Security Engineering
- ✓ Hands-on Cybersecurity / Information Assurance, Certification & Accreditation, and System Security Engineering
- ✓ We create and develop products & tools to streamline Cybersecurity processes
- ✓ We have an expansive customer base and past performance
- ✓ CONUS and OCONUS experience
- ✓ Registered Provider Organization (RPO) with Registered Practitioners (RP) on staff that have been certified by the Cybersecurity Maturity Model Certification Accreditation Board (CMMC-AB).
- ✓ Supporting the Government Industry team to benefit the Warfighter

CMMC Overview and CMMC Level 1 Requirements

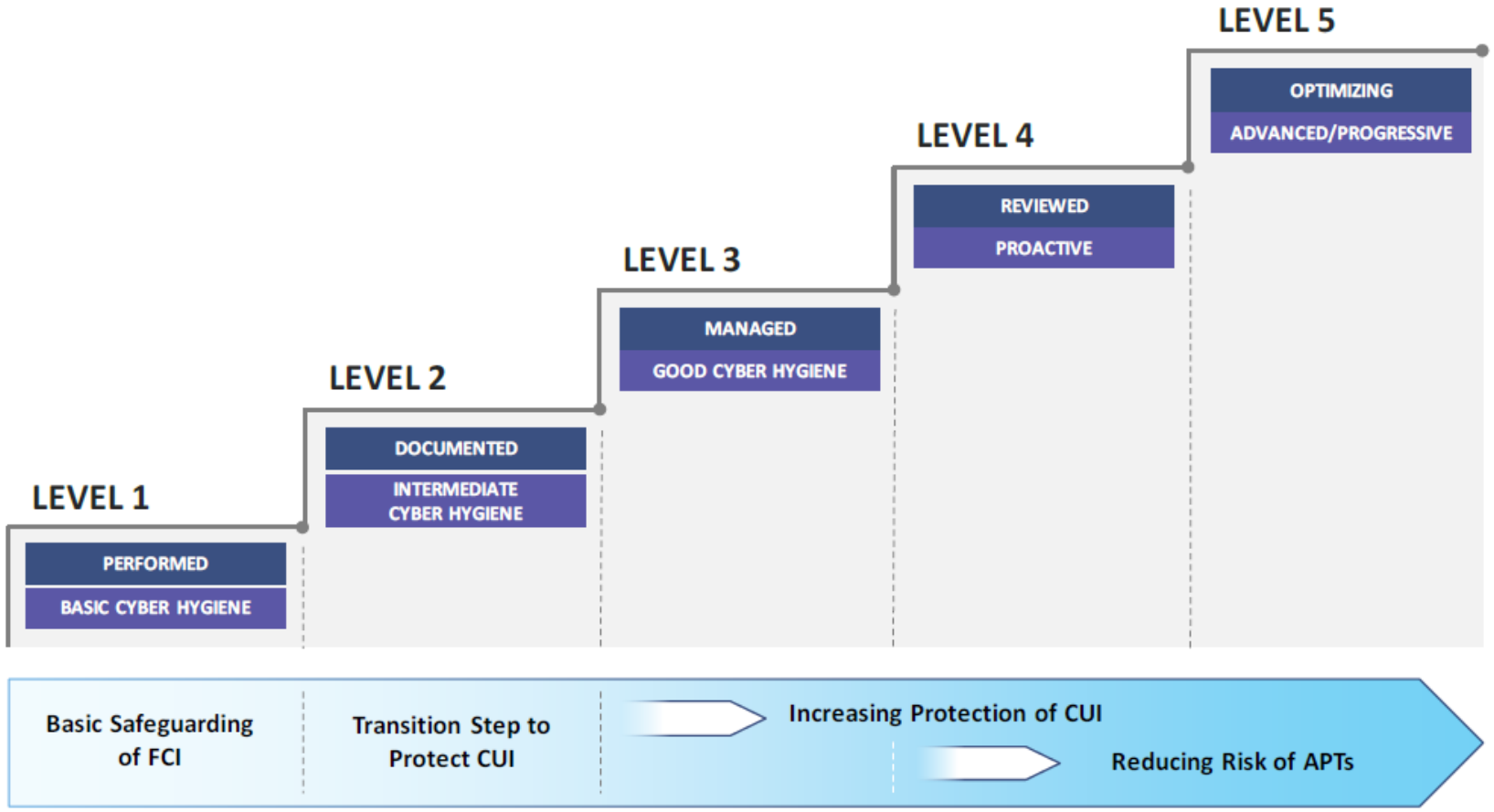
Presented By: Merrilee Maxon

What is CMMC?
Capability Maturity Model Certification

A unified cybersecurity standard for future DoD acquisitions

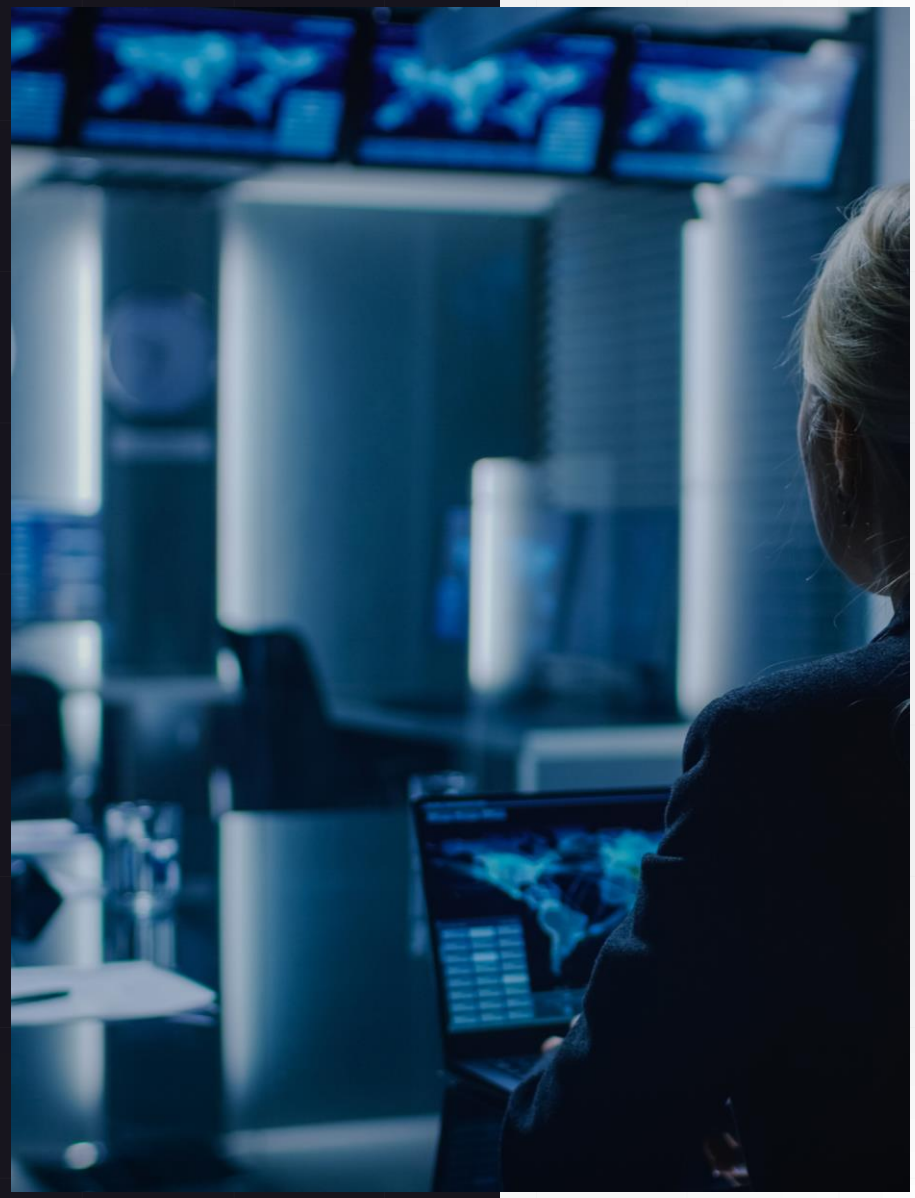
How does the CMMC Certification effect DoD Contractors, Subcontractors, and the DIB Supply Chain?

CMMC Certification Model



CMMC Certification Model

Maturity Level	Maturity Level Description	Processes
ML 1	Performed	*There are no maturity processes assessed at Maturity Level 1.* *An organization performs Level 1 practices but does not have process institutionalization requirements.*
ML 2	Documented	Establish a policy that includes [DOMAIN NAME].
		Document the CMMC practices to implement the [DOMAIN NAME] policy.
ML 3	Managed	Establish, maintain, and resource a plan that includes [DOMAIN NAME].
ML 4	Reviewed	Review and measure [DOMAIN NAME] activities for effectiveness.
ML 5	Optimizing	Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.



- It is extremely important you understand your requirements for CMMC certification.
- CMMC-AB certified assessors cannot determine the level of certification you will need to obtain.
- This will be stated in your contract; whether you're a prime contractor, working directly with the DoD, or you're a subcontractor, working as a DoD contracting partner.
- If you need help determining the level of certification you're required to obtain; you may reach out to your Government contact or contracting

Federal Contract Information (FCI)

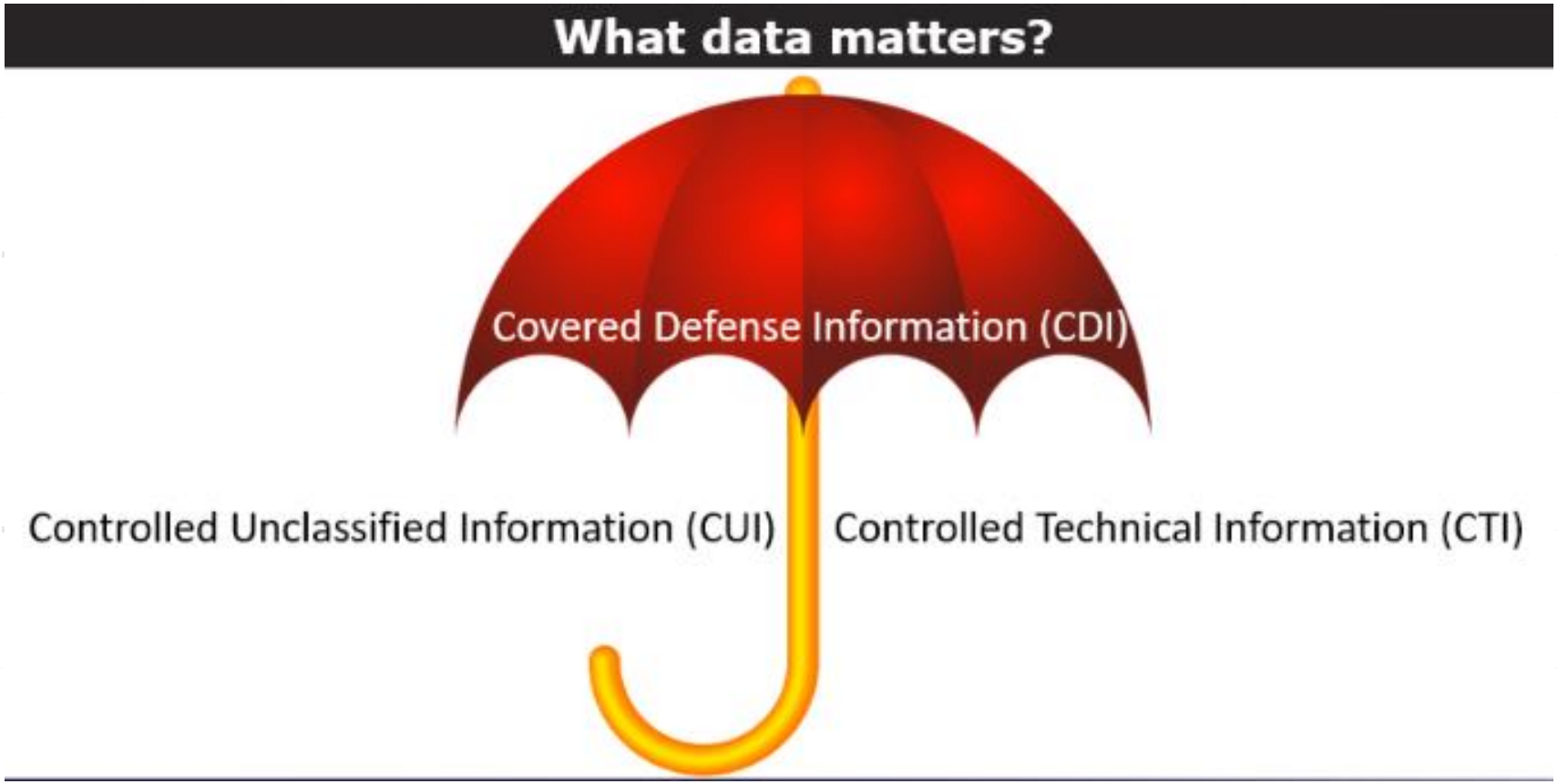
FCI is the specific information pertaining to a good or service not intended for public release.

Controlled Unclassified Information (CUI)

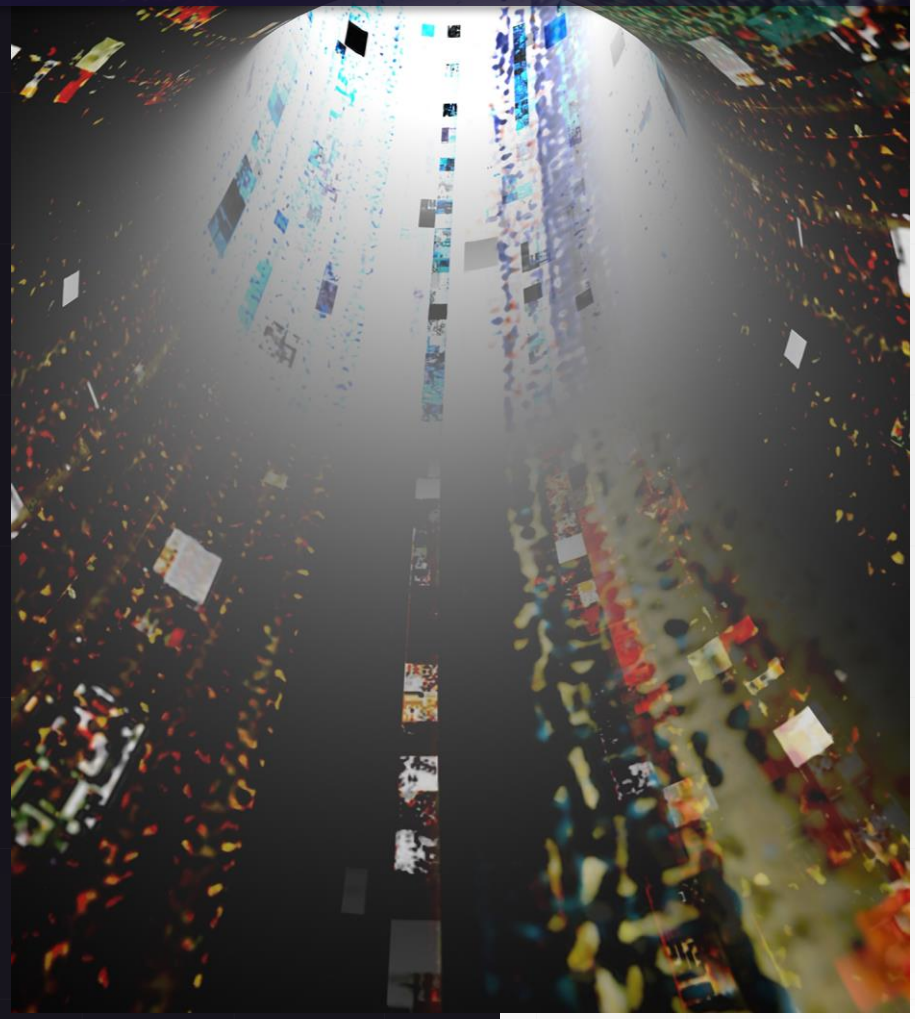
Information the Government creates or possess, or that an entity creates or possess for or on behalf of the government, that law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

Controlled Technical Information (CTI)

Technical Information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination



Getting Started



Documentation

- Start documenting your processes now!

Establish Roles and Responsibilities

- System Owner, Network Admin / System Security Officer(s), FSO, HR/Admin.

Define the Network, devices, and Data Access

- The company network, data stores, and system/data access will help determine the technology ‘boundaries and protected devices.

The CMMC-AB board has stated that initial CMMC certification will be a slow rollout and first-time certification requests will take priority over re-assessments.

CMMC Level 1

CMMC Level 1 Overview

- 17 Practices or Controls
- You will be asked by a certified assessor, to explain how you comply with each practice and show this solution or piece of evidence, proving compliancy
- These 17 controls fall into 6 Categories the CMMC-AB calls, ‘Domains’.

CMMC Level 1 Capability Domains

- Access Control (AC)
- Identification & Authentication (IA)
- Media Protection (MP)
- Physical Protection (PE)
- System & Communications (SC)
- System & Information Integrity (SI)

Access Control (AC)

Account Management | Authorized Users | AC.1.001
Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).

Account Management | Transaction and Function Types | AC.1.002
Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

Use of External Information Systems | AC.1.003
Verify and control/limit connections to and use of external information systems.

Publicly Accessible Content | AC.1.004
Control information posted or processed on publicly accessible information systems.

Identification & Authentication (IA)

Identification and Authentication (Organizational Users) | IA.1.076

Identify information system users, processes acting on behalf of users or devices.

Identification and Authentication (Organizational Users) | IA.1.077

Authenticate (or verify) the identities of those users, processes or devices, as a prerequisite to allowing access to organizational information systems.

Media Protection (MP)

Media Sanitization | MP.1.118

Sanitize or destroy information system media containing Federal Contract Information (FCI) before disposal or release for reuse.

Is there a policy and process in place for Sanitizing and/or Destroying systems and media containing Federal Contract Information (FCI) before disposal or reuse?

Physical Protection (PE)

Physical Access Authorizations | PE.1.131
Limit physical access to organizational information systems, equipment and the respective operating environments to authorized individuals.

Visitor Control | PE.1.132
Escort visitors and monitor visitor activity.

Visitor Access Records | PE.1.133
Maintain audit logs of physical access.

Physical Access Control | PE.1.134
Control and manage physical access devices.

System & Communications (SC)

Boundary Protection | SC.1.175

Monitor, control and protect organizational communications (e.g., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

Public Access Protections | SC.1.176

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

System & Information Integrity (SI)

Flaw Remediation | SI. 1.210
Identify, report and correct information and information system flaws in a timely manner.

Malicious Code Protection | SI.1.211
Provide protection from malicious code at appropriate locations within organizational information systems.

Malicious Code Protection | Automatic Updates | SI.1.212
Update malicious code protection mechanisms when new releases are available.

Malicious Code Protection | SI.1.213
Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed.

CMMC Level 3

CMMC Level 3 Overview

- 130+ Practices
- You will be asked by a certified assessor, to explain how you comply with each practice, show this solution, etc. and show the documentation, policy, etc. that pertains to the controls.
- The documentation you provide to an assess must have a ‘maturity’ level and show that it has been maintained regularly with versions, etc. .

Navigating CMMC Level 3

- CMMC Level 3 Certification can be cumbersome and overwhelming for a small or medium sized business; without a dedicated IT team.
- Navigating technical controls, correctly, and creating the needed documents and policies may be outside of nontechnical staff abilities.

QUESTIONS ?

Robert Biggers
rbiggers@cybernet.com
407-xxx-xxxx

Merrilee Maxon
mmaxon@cybernet.com
407-xxx-xxxx

For more information

1-800-CYBERNET
cybersecurity@cybernet.com
https://www.linkedin.com/company/cybernet-systems-corporation

Thank you for your time

Cybernet Systems

Cybersecurity Division – Orlando, Florida

- 10 years of DoD Cybersecurity focus
- 50+ Authority to Operate (ATO) granted for our customers
- Multiple DFARS 252.204-7012 assessments
- Certified and knowledgeable
- ISC2 CISSP, CompTIA Security+, Cisco CCNA-Security, CEH, etc.
- NIST, IEEE, ISO, COBIT, CMMC, CMMI

CYBERNET

AMPLIFYING HUMAN PERFORMANCE THROUGH ADVANCED TECHNOLOGY

Production Space

16,000 square feet of office in Ann Arbor MI, manufacturing, and storage space. Includes machine shop, electronics lab, software development space, etc.

Test Facilities

Approximately 4,000 square feet of dedicated test warehouse space near office. Complete with shelves, multiple pallet types, overhead doors, and overhead obstructions.

Orlando Office

1,500 square feet office suite in Orlando FL. Includes office space, software development, and cyber security.