GCAT

GOVERMENT CONTRACTING ADVISORY TEAM

CMMC Cybersecurity Req is Coming: What You Need to Know

Presented by:

Ed Kinberg, Attorney, Stewart Law CS

&

Ray Corriveau, VP Business Development, Artemis IT

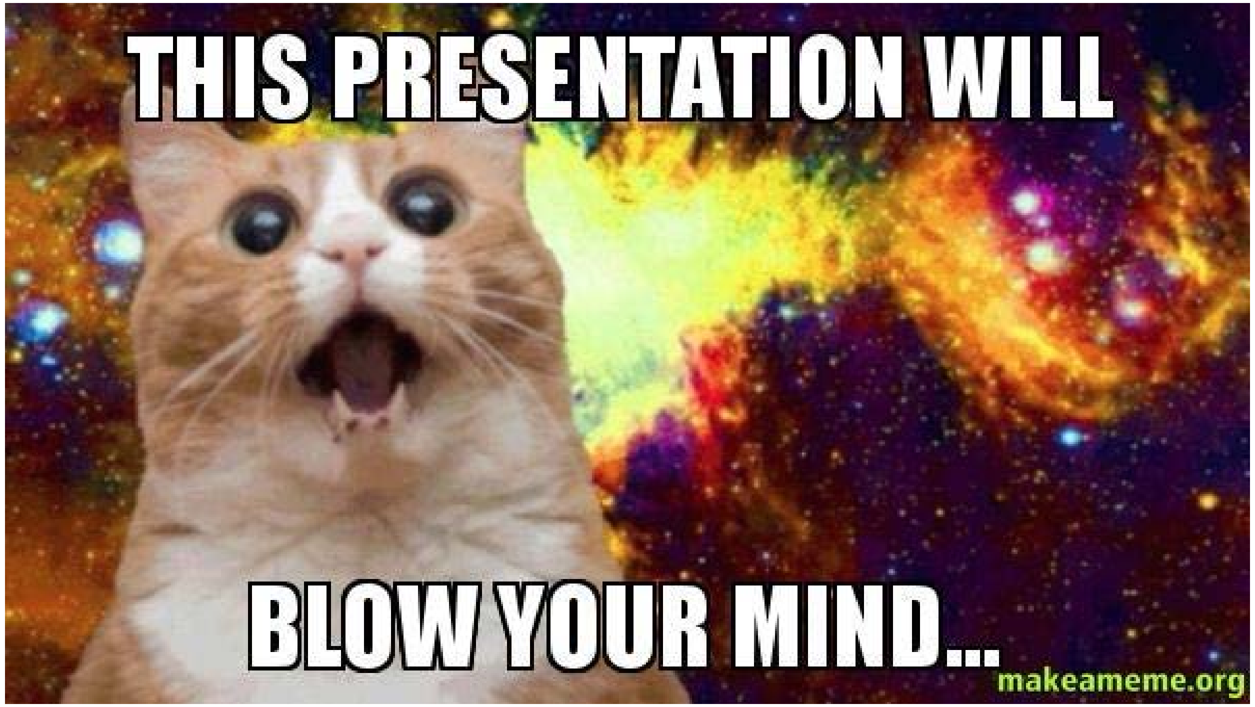
A Brief Diversion

Other New Developments

- FBO moving to SAM on 1 November, New and Improved

- DUN Numbers to be changed: Ernst and Young, will use a government-owned unique entity identifier called the SAM Managed Identifier (SAMMI) within SAM and GSA's Integrated Award Environment.

e



THIS PRESENTATION WILL
BLOW YOUR MIND...
makeameme.org

Controlled Unclassified Information

The Beginning…

CUI defined by George W. Bush directive May 2008

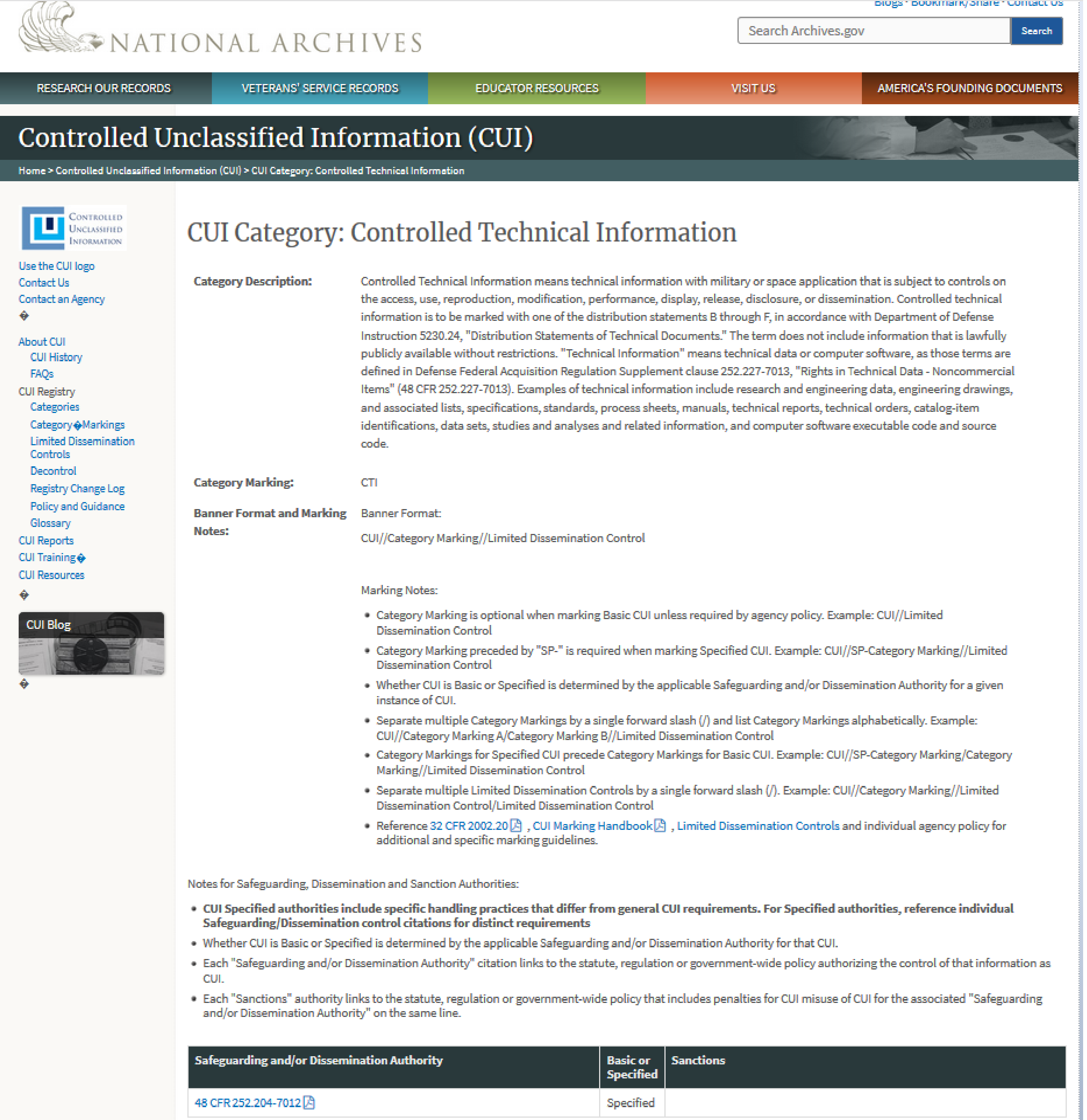
- replaced For Official Use Only and Sensitive But Unclassified
- rescinded and expanded in November 2010 by Barrack Obama
- CUI phrase coined in 2004 DHS study
- NIST SP 800-53 = federal systems
    - FISMA = 462 pages / 212 controls
- NIST SP 800-171 = non-federal systems
    - DFARS = 125 pages / 109 controls
    - Flows down from prime to subs

Controlled Unclassified Information

What is considered CUI?

CUI includes, but is not limited to:

- Privacy (including Health)
- Tax
- Law Enforcement
- Critical Infrastructure
- Export Control
- Financial
- Intelligence
- Privilege
- Unclassified Nuclear
- Procurement and Acquisition



Blogs · Bookmark/Share · Contact Us
NATIONAL ARCHIVES
Search Archives.gov
Search
RESEARCH OUR RECORDS
VETERANS' SERVICE RECORDS
EDUCATOR RESOURCES
VISIT US
AMERICA'S FOUNDING DOCUMENTS

Controlled Unclassified Information (CUI)

Home > Controlled Unclassified Information (CUI) > CUI Category: Controlled Technical Information

CUI Category: Controlled Technical Information

Category Description: Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

Category Marking: CTI

Banner Format and Marking Notes: Banner Format:

CUI//Category Marking//Limited Dissemination Control

Marking Notes:

- Category Marking is optional when marking Basic CUI unless required by agency policy. Example: CUI//Limited Dissemination Control
- Category Marking preceded by "SP-" is required when marking Specified CUI. Example: CUI//SP-Category Marking//Limited Dissemination Control
- Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for a given instance of CUI.
- Separate multiple Category Markings by a single forward slash (/) and list Category Markings alphabetically. Example: CUI//Category Marking A/Category Marking B//Limited Dissemination Control
- Category Markings for Specified CUI precede Category Markings for Basic CUI. Example: CUI//SP-Category Marking/Category Marking//Limited Dissemination Control
- Separate multiple Limited Dissemination Controls by a single forward slash (/). Example: CUI//Category Marking//Limited Dissemination Control/Limited Dissemination Control
- Reference 32 CFR 2002.20, CUI Marking Handbook, Limited Dissemination Controls and individual agency policy for additional and specific marking guidelines.

Notes for Safeguarding, Dissemination and Sanction Authorities:

- **CUI Specified authorities include specific handling practices that differ from general CUI requirements. For Specified authorities, reference individual Safeguarding/Dissemination control citations for distinct requirements**
- Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for that CUI.
- Each "Safeguarding and/or Dissemination Authority" citation links to the statute, regulation or government-wide policy authorizing the control of that information as CUI.
- Each "Sanctions" authority links to the statute, regulation or government-wide policy that includes penalties for CUI misuse of CUI for the associated "Safeguarding and/or Dissemination Authority" on the same line.

Safeguarding and/or Dissemination Authority	Basic or Specified	Sanctions
48 CFR 252.204-7012	Specified	

GCAT
Government Contracting Advisory Team

CUI Registry

https://www.archives.gov/cui

The CUI Registry is the Government-wide online repository for Federal-level guidance regarding CUI policy and practice. However, agency personnel and contractors should first consult their agency's CUI implementing policies and program management for guidance.

NIST SP 800-171

Current Special Publication referenced…

NIST publication 800-171 is a body of government requirements for protecting Controlled Unclassified Information (CUI). NIST 800-171 is applicable to organizations in the public and private sector, including: government contractors; manufacturers; state, local, and tribal governments; and colleges and universities. Effective as of 2015, NIST 800-171 is a sub-set of NIST 800-53, and covers 14 different control families:

1. Access Control
2. Awareness and Training
3. Audit and Accountability
4. Configuration Management
5. Identification and Authentication
6. Incident Response
7. Maintenance
8. Media Protection
9. Personal Security
10. Physical Protection
11. Risk Assessment
12. Security Assessment
13. System and Communication Protection
14. System and Information Integrity

CMMC

The Next Generation…

The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) recognizes that security is foundational to acquisition and should not be traded along with cost, schedule, and performance moving forward. The Department is committed to working with the Defense Industrial Base (DIB) sector to enhance the protection of controlled unclassified information (CUI) within the supply chain.

OUSD(A&S) is working with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDC), and industry to develop the Cybersecurity Maturity Model Certification (CMMC).

- The CMMC will review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats.
- The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements.
- The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels.
- The intent is for certified independent 3rd party organizations to conduct audits and inform risk.

https://www.acq.osd.mil/cmmc/

OK, so what does this mean?

DoD CMMC Policy

The CMMC will review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats.

The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements.

The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels.

The intent is for certified independent 3rd party organizations to conduct audits and inform risk

e

Cybersecurity Maturity Model Certification

The Basics

- Will be mandatory for all DoD Contractors and Subcontractors
- Replaces the Cybersecurity Requirements of DFARS 252.204-7012
- Third Party Verification will be required in order to bid on Gov’t Contracts.
- Implementation starts this year but time line is uncertain.
- Cybersecurity Accreditation Body will be responsible for certifying companies/ individual to perform certification.

e

Cybersecurity Maturity Model Certification

Time Line

- Version 1 should be released in January 2020.
- RFI for Accreditation Body Current under review.
- RFP for Accreditation Body: to be released soon.
- RFP with CMMC requirement should start appearing last half of 2020
- Once CMMC is final, certification will be required by time of contract award.
- Certification for contract with classified work may be done separately by DoD (DCMA, DCSA.

e

Cybersecurity Maturity Model Certification

Levels

- Level 1: Basic Hygiene
- Level 2: Intermediate Hygiene
- Level 3: Good Cyber Hygiene and effective implementation of controls
- Level 4: Substantial and proactive cybersecurity program
- Level 5: Advanced or progressive cybersecurity program with a demonstrated ability to optimize cybersecurity capabilities

DoD anticipate most businesses will not have to go beyond level 3.

e

Cybersecurity Maturity Model Certification

Oversight

- CMMC Accreditation Body (CMMC-AB) – 19 November 2019

- Mission: To serve as the singular voice of the Defense Industrial Base (DIB) in receiving and taking custody of the Completed CMMC Standard (expected January 2020) and will be responsible for implementing the audit of all contractors to DoD.

- 12 Members, 6 appointed, applications for six additional positions currently under consideration.

e

Cybersecurity Maturity Model Certification

Status

- Oversight Board Established.
- Certified 3rd Party Assessment Organization (C3PAO) not yet selected.
- Draft CMMC Model v.07 under review
- CMMC Model 1.0 pending release
- Sign up for Advisory Board updates at cmmcab.org (bottom of page)

e

Cybersecurity Maturity Model Certification

Key Terms

- Assessor
- Assessment
- Certified 3rd Party Assessment Organization (C3PAO)
- Controlled Unclassified Information (CUI)
- License Number

For current CCMC glossary, click here.

e

WITHOUT GOVERNMENT
WHO WOULD WATER TREES IN THE RAIN?
imgflip.com

Meeting gov cybersecurity and data protection requirements starts with a good computer network baseline….

Computer Network Baseline - Products

You should have these anyway…

1. Business grade firewall w/ active update subscription
   - monitors and controls incoming and outgoing network traffic
   - SonicWALL, Cisco, Juniper, Sophos, Fortinet, WatchGuard, etc.
2. Network switch supporting virtual LAN's
   - connects devices on a computer network - vlan's segregate network traffic for security and optimization
   - Dell, Netgear, Cisco, Juniper, HP, FS, etc.
3. Email Defense w/ active update service
   - filter inbound / outbound mail to quarantine spam, malware, suspicious links, encrypt email, etc.
   - Barracuda, iboss, SolarWinds, SpamHero, Cisco, Sophos, Microsoft ATP, SpamTitan, Mimecast, etc.
4. Anti-virus software w/ active update service
   - program designed to detect, and remove viruses and other malicious software
   - Cylance, TrendMicro, Vipre, Bitdefender, Norton, McAfee, AVG, Kaspersky(!), etc.
5. Data backup
   - monitored on premise and remote data backup system with periodic tests

Computer Network Baseline - Products

Your mileage may vary…

1. Business grade firewall w/ active update subscription
   - SonicWALL TZ 400 w/ 3 years Advanced Gateway Security Suite: ~$2,500
2. Network switch supporting virtual LAN's
   - Dell 48 port switch with Power Over Ethernet (PoE): ~$2,900
3. Email Defense w/ active update service
   - Barracuda Advanced Email Security: ~$3 per mailbox per month
4. Anti-virus software w/ active update service
   - Cylance advanced AI-based endpoint protection: ~$4 per month per device
5. Data backup
   - 8 TB Buffalo TeraStation NAS w/ Windows Storage Server for local backup: ~$1,500
   - Backup software + 1TB remote cloud storage for 2 x server: ~$150 per month

Computer Network Baseline - Policies

You should have these anyway…

1. Password Policy
    - defined minimum complexity, change periodically
2. IT Policies
    - IT Security, Acceptable Use, Employee On/Off Boarding, BYOD, Disaster Recovery / Business Continuity
3. Cybersecurity Education Program
    - spot phishing emails and scams, safe computing do’s & don'ts, detect social engineering, etc.

Advanced Network Protection

You may also need…

1. Encryption for data at rest
   - encrypted data in the wild may not require reporting
2. Network activity reporting
   - reports showing who accessed what and when
3. Multi-factor authentication
   - Send onetime password or code to cell phone / email, require USB key, biometrics, etc.
4. Mobile device management
   - secure tablets, cell phones, etc. – prevent unauthorized installs, encrypt data, remotely wipe device, etc.
5. Security Operations Center (SOC)
   - monitor network 24/7 for suspicious activity and mitigate threats - for SMB, service provider makes most sense
6. Penetration Test
   - external / internal venerability test performed by a 3rd party
7. Physical security
   - access control, locking networking cabinets or rooms, cameras w/ XX days retention,

Office 365, Microsoft 365, & Cloud

Just a head's up, be on the look out for Gov Moderate or High Impact Level hosting requirements…

Real Life Example: 100 user manufacturing / engineering company

- Microsoft Office 365 Government - GCC High E3 needed for contract if using cloud email and apps
- Customer content is logically segregated from customer content in the commercial Office 365 services from Microsoft
- Customer content is stored within the United States
- Access to restricted to screened Microsoft personnel
- Complies with certifications and accreditations required for US Public Sector customers
- Includes a suite of security tools and audio conferencing, Teams, Flow, Planner, etc.
- Quote for 100 Office 365 GCC High users = $60k per year

- Staying on premise with Exchange instead
  - Exchange 2019 requires 128 GB RAM min.

Seek Help

Bring in the SME's…

1. What does the contract actually require?
   - do you have the expertise in-house to untangle the clauses, pubs, etc. referenced?
   - how can you comply cost-effectively?
2. Does CMMC overlay other programs / requirements?
   - can you cross walk ISO, PCI, HIPAA, CCPA (California), DFARS, NIST, ITAR, GDPR, CMMC, etc.?
   - Yes! Example below, maps 800-171 controls to 800-53, ISO 27002:2013, and DFARS 7012
   - https://library.educause.edu/resources/2016/9/nist-sp-800-171-compliance-template
3. Compliance must be an ongoing program
   - policies, employee sign off, activity tracking
   - not compliant if you can't prove it

Consequences

- Not eligible for Contract Award
- Failure to follow compliance program
  - Contract Termination
  - Suspension
  - Debarment
  - False Claims Act
  - Civil Penalties
  - Criminal Penalties.

Key Websites

DoD, Office of Secretary of Defense for Acquisition and Sustainment Cybersecurity Maturity Model Certification

Draft CMMC Model v0.7: As new versions are released, this link should be updated.

CMMC Accreditation Body

e

THAT IS THE END OF THIS PRESENTATION
THANK YOU