CUI/CMMC/ITAR COMPLIANCE FOR FEDERAL GOVERNMENT CONTRACTORS

BY ALAN SUGANO, ADS CONSULTING GROUP

THE SENTINELS OF YOUR IT GALAXY

AGENDA

- Why this Matters
- What is CUI?
- What is CMMC?
- What is ITAR?
- Practical steps
- Q&A

WHY THIS MATTERS

- We don’t want Controlled Unclassified Information (CUI) falling into the wrong hands.
- If you are not in compliance, the Federal Government can cancel your contracts.
- Increasing cybersecurity requirements
- Government contract eligibility
- Protect sensitive information
- Avoid penalties and business risk

WHAT IS CUI?

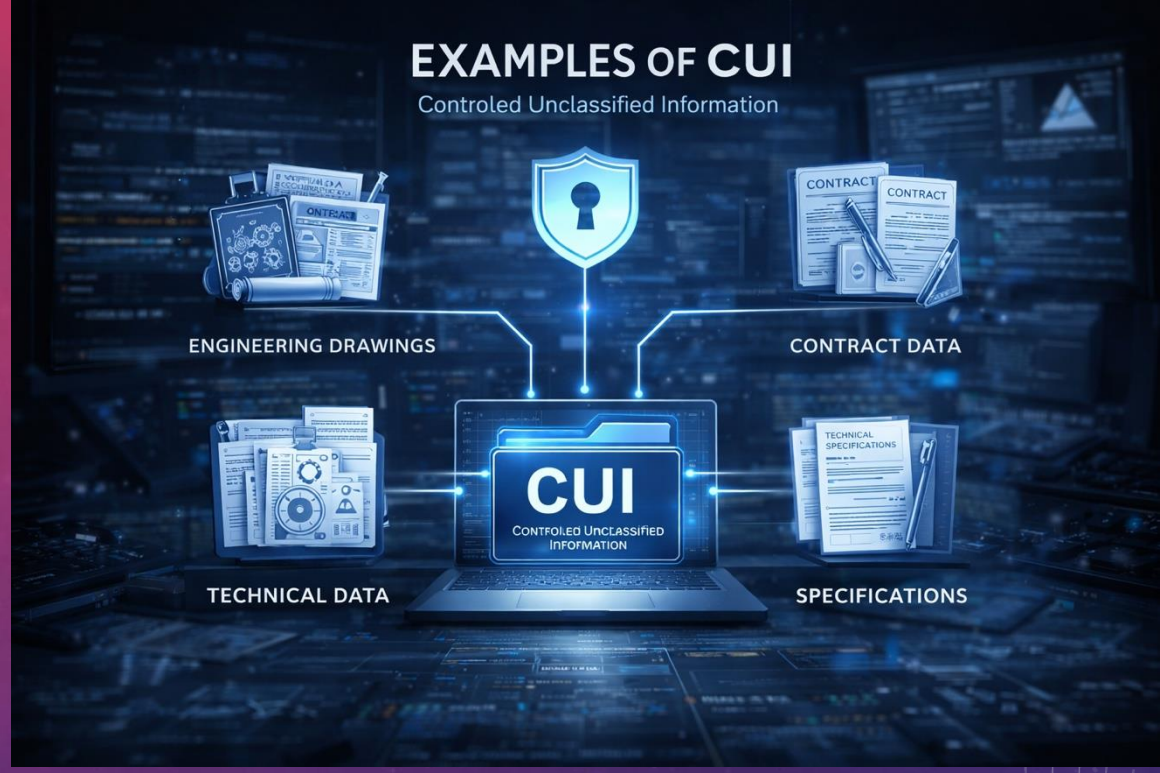
- Controlled Unclassified Information
- Sensitive but not classified
- Defined by U.S. Government
- Assets must be properly handled and protected.

WHAT IS CUI

- Two Levels
  - NIST 800-171
    - Your company has Controlled Unclassified Information
    - 110 Security Controls.
    - 90% of Government Contractors are at this level.
  - NIST 800-172
    - 145 Security Controls
    - Your company has High-Value Department of Defense Contracts.

EXAMPLES OF CUI

- Intellectual Property
  - Engineering drawings
  - Technical data
  - Contracts and Specifications.
  - Export-controlled information.
- Anything Confidential/Proprietary



WHAT IS CMMC?

- Cybersecurity Maturity Model Certification
- Department of Defense (DoD) requirement
- Ensures contractors protect CUI
- Framework to maintain good Cyber Hygiene.
- Three Levels

WHAT IS CMMC?

- Three Levels
  - Level 1 Basic Safeguards
    - Handle Federal Contract Information, but not any Controlled Unclassified Information (CUI).
  - Level 2 CUI
    - Required when you have CUI.
    - Comply with NIST 800-171
  - Level 3 High-Sensitivity CUI
    - High-value CUI
    - Comply with NIST 800-172

WHAT IS ITAR?

- International Traffic in Arms Regulations
  - Controls export of defense-related data
  - Applies to physical + digital sharing
  - Strict penalties for violations

WHAT IS ITAR?

- Register with the U.S. State Department (DDTC).
- Identify and Control ITAR-Regulated Items.
- Obtain Export Licenses When Required.
- Restrict Access and Screen Parties.
- Maintain Compliance Program (Training, Records, Audits).

ITAR EXAMPLES

- Defense designs
- Military components
- Sharing with foreign nationals
- Cloud storage considerations

CUI VS CMMC VS ITAR

- They are kissing cousins.
  - CUI: The data
  - CMMC: The cybersecurity standard and maintenance framework
  - ITAR: Export control law
- They often overlap

COMMON CHALLENGES

- Significant gaps between the current state of your IT Cybersecurity and the compliance requirements.
- Not knowing where data resides
- Over-sharing access
- Lack of user training
- Legacy systems

PRACTICAL STEPS

- Start with a Gap Analysis
  - Create a baseline of the current state of your Cybersecurity and Information Technology.
  - Compare that against the requirements of CUI/CMMC/ITAR
- Create a plan to close any Gaps.
- Prepare for the Third Party Audit
- Pass the audit and become certified.

WHAT AUDITORS LOOK FOR

- Policies and procedures
- Access control
- Incident response
- Evidence of implementation

KEY TAKEAWAYS

- This is about protecting sensitive info
- Compliance = business opportunity
  - Barrier to entry.
- Get started now.
  - You don’t want to risk cancellation of your Federal Government Contracts.

QUESTIONS?


why
when
who
where
what
why
QUESTIONS
who
how
where
who
what
how
why
when

THANK YOU!

ALAN SUGANO

ASUGANO@ADSCON.COM

WWW.ADSCON.COM

YOUTUBE.COM/@ADSCON

SCAN THE QR CODE TO GO TO OUR CUI COMPLIANCE PAGE.