CMMC

FACTS, FICTION, AND WHAT YOU NEED TO KNOW **NOW.**

WEBINAR

SEPTEMBER 30

Get actionable steps and your important questions answered

HUMANTOUCH

THE PATUXENT PARTNERSHIP

LIKE NO OTHER CONNECTION

RICK HILL, PMP, RP

SR. VICE PRESIDENT
HUMANTOUCH, LLC.

Head of the Cybersecurity Consulting Business at HumanTouch **(RPO & Candidate C3PAO)**

Former **Principal at Booz Allen Hamilton**

Computer Engineer, PMP, **RP**

BS and MBA from **Johns Hopkins University**

Published in National Defense News, and is a frequent contributor to AFCEA, Washington Business Journal, and G2Xchange

Led several **cyber panel discussions** for Federal News Radio

REGISTERED PRACTITIONER

CMMC-AB MARKETPLACE

25
YEARS

CYBER COMPLIANCE

EXPERIENCE

NIST PARAMETERS

Rick's hands-on experience with NIST parameters includes leading the contractor team that generated the initial 800 series guidance.

SPECIALTIES

Cyber Risk
Surface Area Threat
Vulnerability Management
Federal Civil & Financial Services Sector

HUMANTOUCH

JAMES NORRIS, RP

CYBER RISK ADVISOR
HUMANTOUCH, LLC.

Cyber Risk Advisor and Registered Practitioner at HumanTouch **(RPO & Candidate**

Published on CMMC in American Security Today

Cybersecurity **Mentor**

Certified in Sophos and Fortinet

Past performance with **SIEMs** – AlienVault, LogRhythm, Wazuh, Splunk

EDR – Carbon Black, Sophos, Fortinet

REGISTERED PRACTITIONER

CMMC-AB MARKETPLACE

4

YEARS

CYBER COMPLIANCE

EXPERIENCE

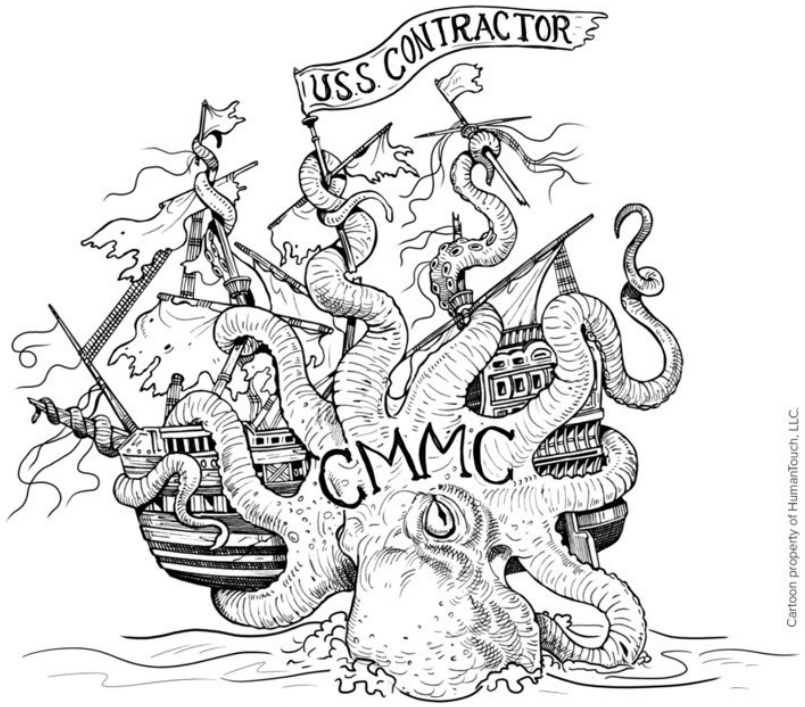
SPECIALTIES

24/7/365 Network Security Monitoring, vSOC, mSOC, SIEM | Phishing Awareness Training | Professional Consulting Services - VMaaS, Vulnerability Assessments, Penetration Testing, Incident Response, PCI, HIPAA, Hitrust, GDPR, NIST, CMMC

HUMANTOUCH

SURVEY QUESTION

How many of you have **started** your CMMC Certification
or entered your **800-171 results** into SPRS?



HUMANTOUCH

What is being said in the **marketplace**

RECENT NEWS

TO LEARN MORE, CLICK THE TITLE OF THE ARTICLE FOR THE LINK

Defense Industry Waits on Costly Trump-Era Cyber Rule Update

Not Just CMMC: New DoD Rule Creates Two Cybersecurity Assessment Frameworks

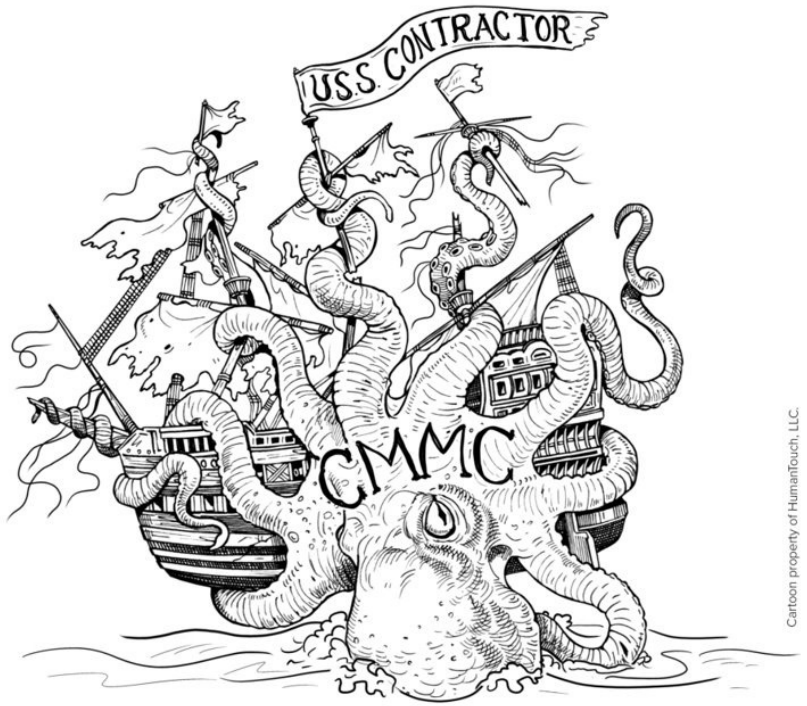
With CMMC certification, slow and steady wins the race

The Pitfalls of Factoring in Security and CMMC Costs

HUMANTOUCH

SURVEY QUESTION

Will CMMC **really** be a requirement?



HUMANTOUCH

What is also being said in the **marketplace**

RECENT NEWS

TO LEARN MORE, CLICK THE LINK

Pentagon Official Says CMMC Changes Will be Finalized 'Very Soon' Link

DoD Wants Industry to Continue With CMMC Prep Amid Program Review Link

Reputable Source:

Christine Michienzi,
Chief Technology Officer,
The Office of the Secretary of Defense

HUMANTOUCH

DFARS **requirements**

DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT

Purpose is to shore up lax cybersecurity across the US DIB. The challenge has been that, under DFARS 7012, a high percentage of suppliers have been self-attesting to DFARS compliance without verifiably bringing their systems and processes into compliance.

The **DFARS 7020 clause informs suppliers** that the DoD has the right to access "facilities, systems and personnel" that manage, process, store, or transmit controlled unclassified information.

DFARS 252.204-7020 (DFAR 7020)

DFARS 252.204-7012 (DFAR 7012)

HUMANTOUCH

What it means **for you**

IF YOU ARE CMMC COMPLIANT

Awarded DoD contracts

Maintain your business

Safeguard your organization

Protect national security

HUMANTOUCH

What is **CMMC**

CYBERSECURITY MATURITY MODEL CERTIFICATION

A unifying standard for the implementation of cybersecurity across the Defense Industry Base (DIB)

CMMC is designed to **provide increased assurance to the DoD that a DIB company can adequately protect CUI**

HUMANTOUCH

Controlled Unclassified Information **(CUI)**

WHAT IS IT?

TO LEARN MORE ABOUT CUI:
HTTPS://WWW.ARCHIVES.GOV/CUI

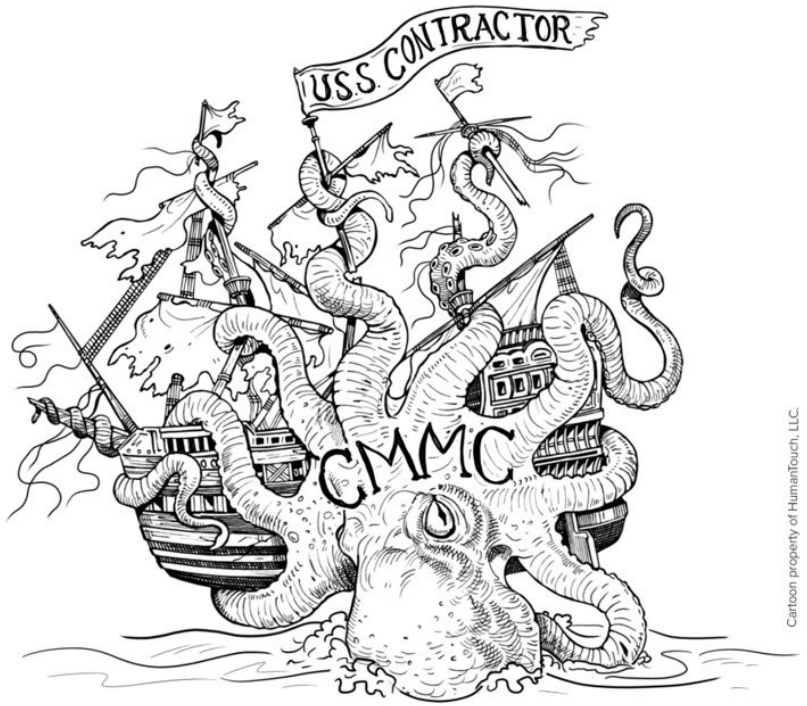
CUI is information the Government creates or possesses, or that a contractor creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy **requires an agency to handle using safeguarding controls**

- Information that is marked or identified as requiring protection under the CUI program.
- Minimum Security Requirements in a non-federal information system: **NIST SP 800-171**

HUMANTOUCH

SURVEY QUESTION

Do you currently have **CUI** in your IT infrastructure?



HUMANTOUCH

CUI consists of **20 categories**

EXAMPLES OF CATEGORIES IN THE DOD THAT CAN APPLY TO YOU:

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)

PROVISIONAL:

Homeland Security Agreement Information
Homeland Security Enforcement Information
Information Systems Vulnerability Information – Homeland
International Agreement Information – Homeland
Operations Security Information
Personnel Security Information
Physical Security – Homeland
Privacy Information
Sensitive Personally Identifiable Information

DEFENSE:

Controlled Technical Information
DoD Critical Infrastructure Security Information
Naval Nuclear Propulsion Information
Unclassified Controlled Nuclear Information – Defense

INTELLIGENCE:

Agriculture
Foreign Intelligence Surveillance Act
Foreign Intelligence Surveillance Act Business Records
General Intelligence
Geodetic Product Information
Intelligence Financial Records
Internal Data
Operations Security

PROCUREMENT & ACQUISITION:

General Procurement and Acquisition
Small Business Research and Technology
Source Selection

HUMANTOUCH

CUI Markings for Unclassified Documents

Example of markings on a CUI document with portion markings.

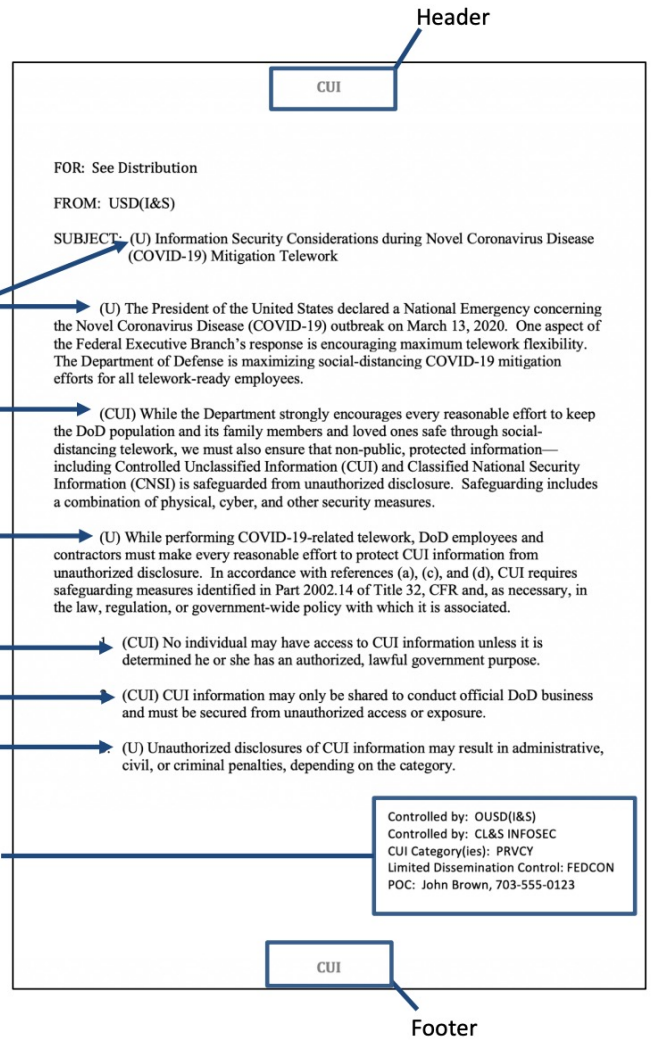
If all the sub-paragraphs or sub-bullet points carry the same classification as the main paragraph or bullet point, portion marking is not required for the sub-paragraphs or sub-bullet points.

However, if any of the sub-paragraphs or sub-bullet points carry different classifications from the main paragraph or bullet point, portion marking is required for all the sub-paragraphs or sub-bullet points as demonstrated here.

Portion marks

Portions include subjects, titles, paragraphs and sub-paragraphs, bullet points and sub-bullet points, headings, pictures, graphs, charts, maps, reference list, etc.

The CUI designation indicator block does not require a portion mark.

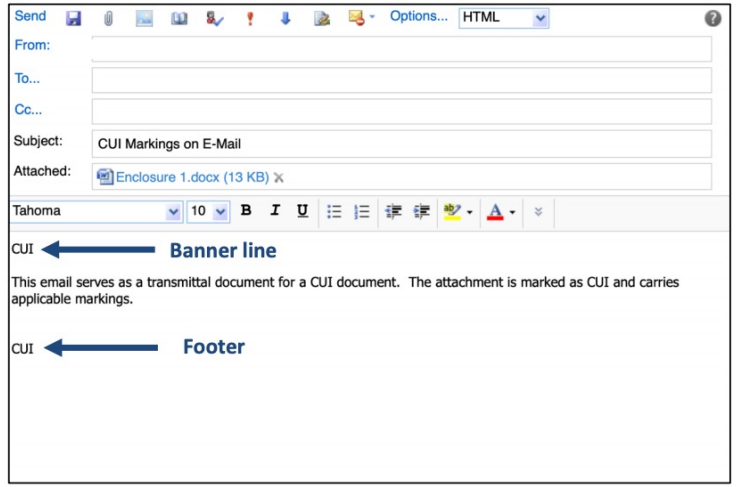


Reference: DoDI 5200.48, Controlled Unclassified Information (CUI), para. 3.4

Markings are for training purposes only

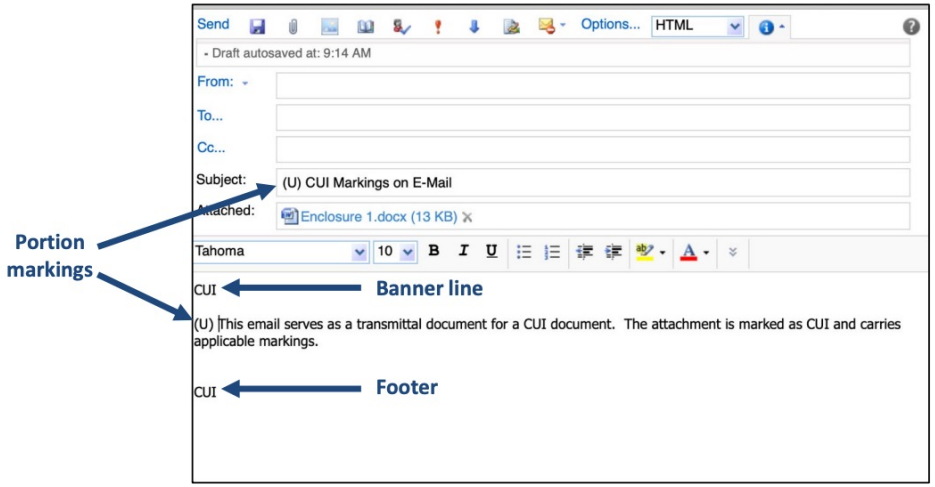
CUI Markings for Unclassified Documents

Minimum markings



The CUI designation indicator block does not need to be placed on an unclassified e-mail that serves as a transmittal document for a CUI document. As an option, the banner and footer lines can read:
CUI (with attachment)

Portion markings included

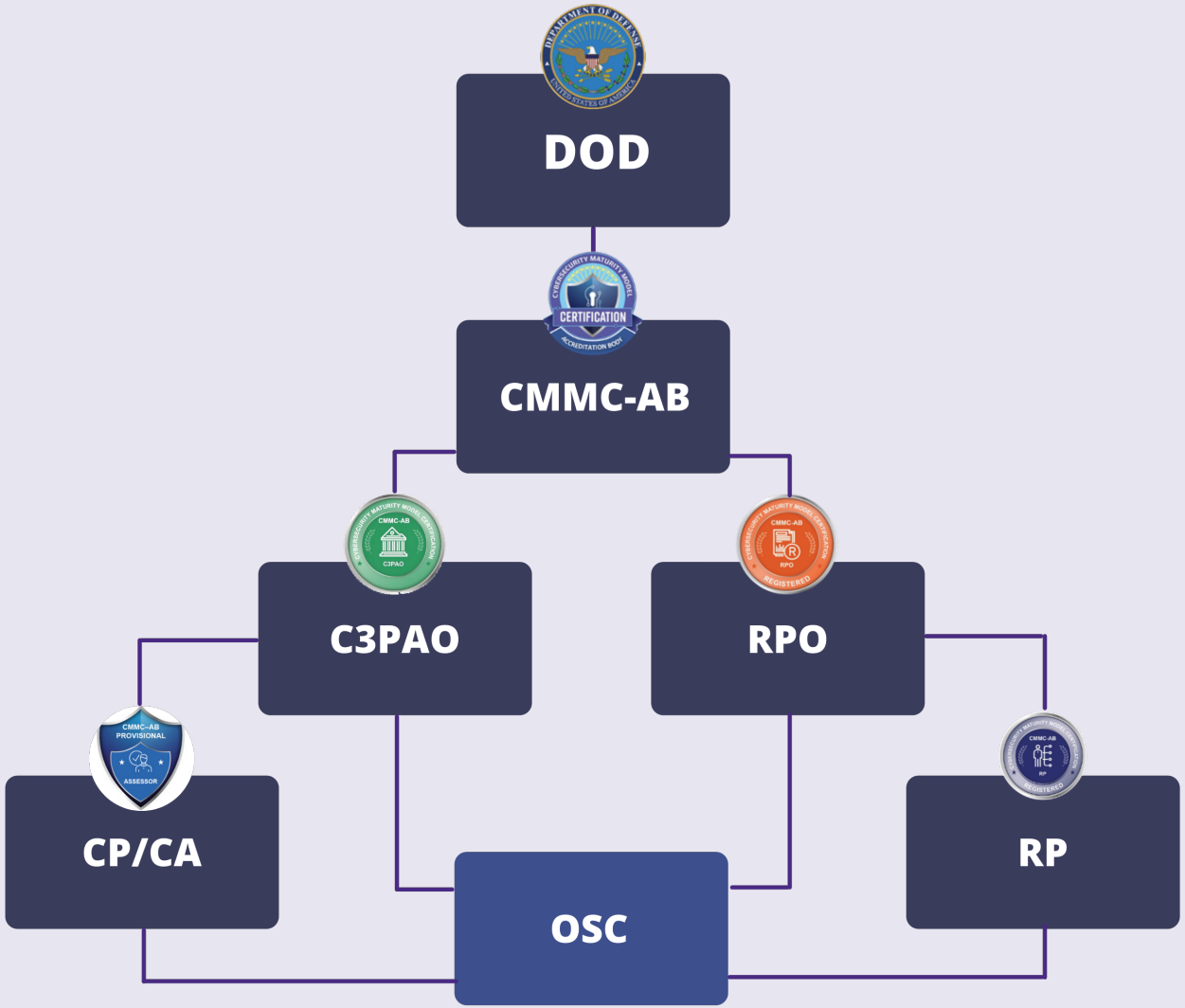


Reference: DoDI 5200.48, Controlled Unclassified Information (CUI), para. 3.4

Who are the players?

As an Organization Seeking Certification (OSC), you'll directly interact with:

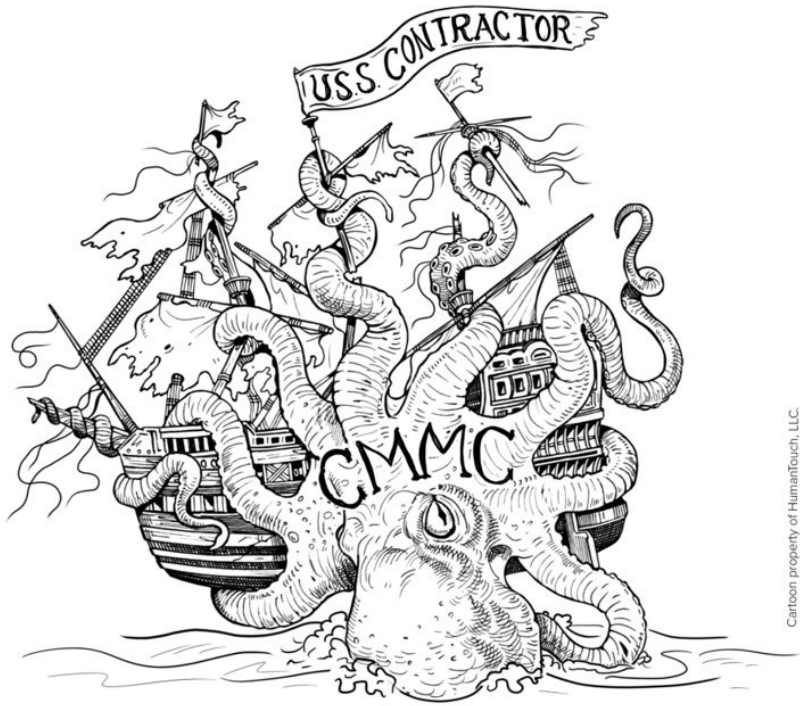
- Registered Practitioners
- Registered Provider Organization
- Third-party Assessment Organization
- Certified CMMC Professionals



HUMANTOUCH

SURVEY QUESTION

How many of you understand the
scope of the CMMC?



HUMANTOUCH

CMMC **Compliance Levels**

SOURCE: OFFICE OF THE UNDERSECRETARY OF DEFENSE, UNCLASSIFIED

HUMANTOUCH

CMMC **Model Structure**

SOURCE: CYBERSECURITY MATURITY MODEL CERTIFICATION ACCREDITATION BODY

HUMANTOUCH

10 Steps to CMMC

SOURCE: CYBERSECURITY MATURITY MODEL CERTIFICATION ACCREDITATION BODY

NIST 800-171: This is where NIST fits into CMMC, it's the true first step - the baseline assessment of your security posture.

1

Understand CMMC requirements

2

Identify your scope. Enterprise, Organization Unit or Program Enclave

3

Identify the desired Maturity Level

4

Baseline organization against the practices & processes for the CMMC level

5

Close any identified gaps to satisfy POA&M and finalize SSP

6

Find a C3PAO on the CMMC-AB Marketplace

7

Conduct the Assessment with C3PAO's Certified Assessment team

8

Allowance of up to 90 days to resolve findings (if any)

9

CMMC-AB reviews submitted assessment

10

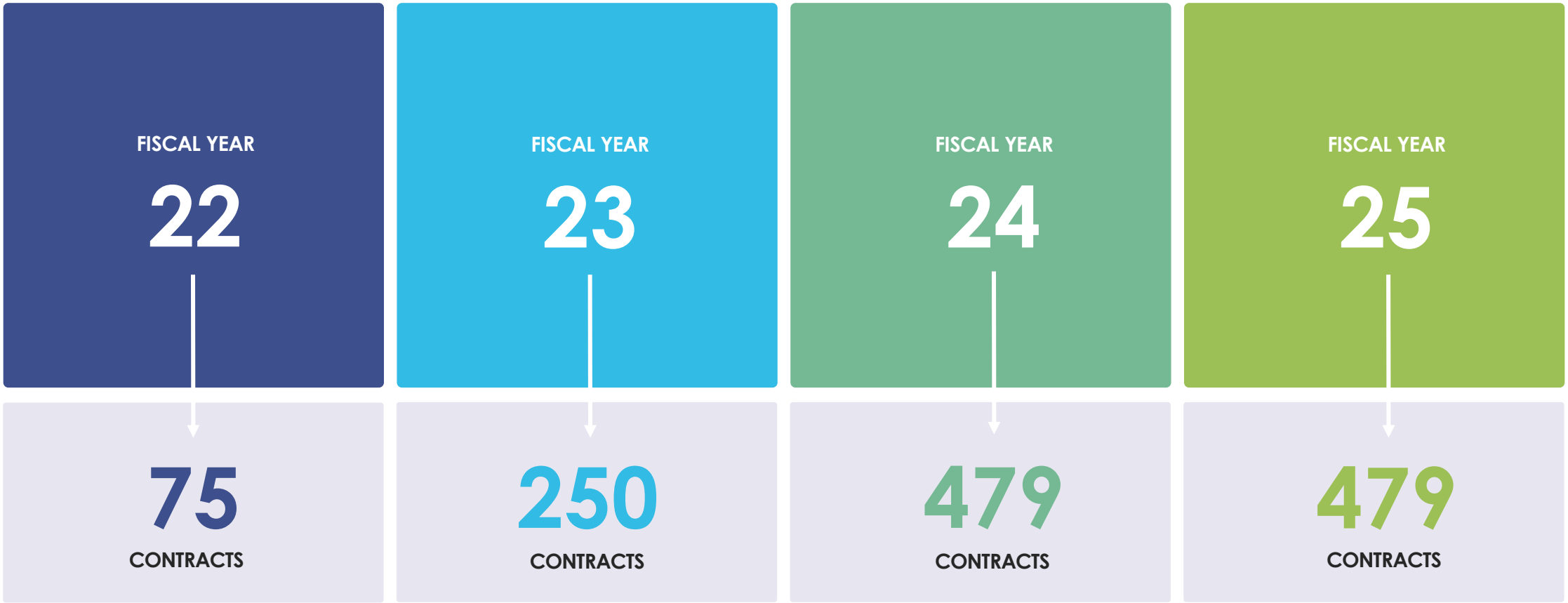
Upon approval: 3-year certification is issued

HUMANTOUCH

Projected CMMC Roll-out

TOTAL NUMBER OF CONTRACTS WITH CMMC REQUIREMENT, PER FISCAL YEAR

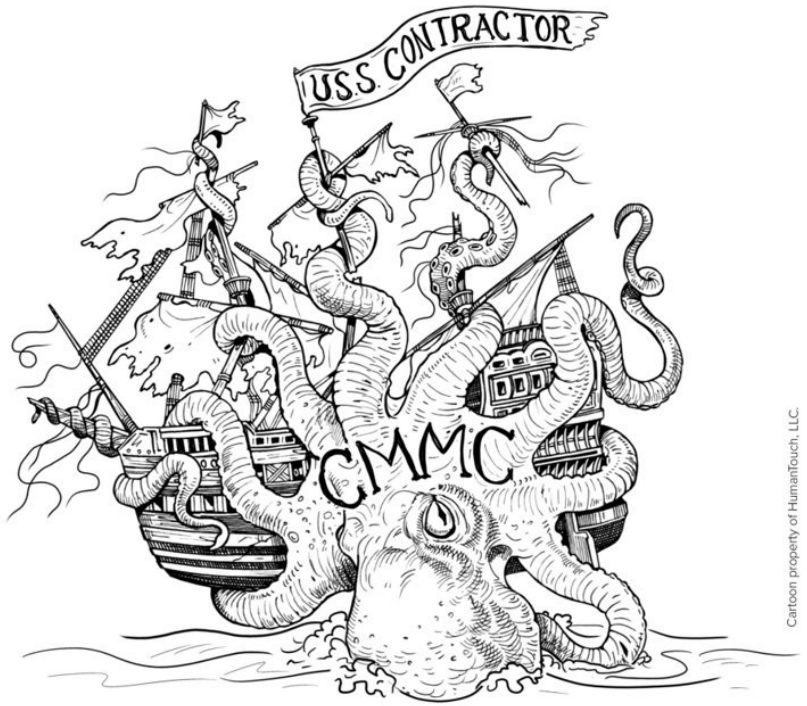
SOURCE: OFFICE OF THE UNDERSECRETARY OF DEFENSE, UNCLASSIFIED



HUMANTOUCH

SURVEY QUESTION

What **CMMC requirements** do you see showing up in Federal procurements?



HUMANTOUCH

Summary

WE'VE COVERED A LOT

Do **not** wait.

It's **going** to happen
It's not a question as to **IF**
It's a question as to **WHEN**

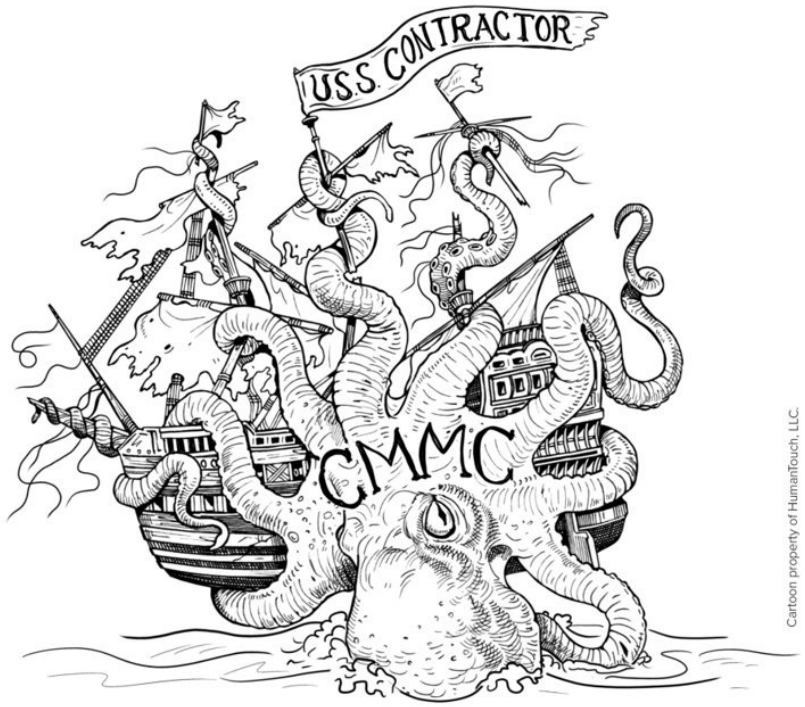
Protect yourself, ask RPOs:
Are they registered with the CMMC-AB? (Check the CMMC-AB Marketplace)
Do they have Registered Practitioners (RPs) on their staff?

Please talk to multiple RPOs and compare.
Make sure your advisor **understands the CMMC process.**

HUMANTOUCH

OPEN DISCUSSION

How many of you have been approached by somebody **trying to sell you CMMC services** – how do you know how to pick the right service provider?



Anyone willing to share?
So, others can learn.

HUMANTOUCH

Resources

FOR MORE INFO, CLICK THE LINK

CMMC Insight/Articles

CMMC Marketplace – search RPOs for reputable consult

CMMC Model & Assessment Guides

Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification - CMMC FAQs

The U.S. National Archives and Records Administration - Controlled Unclassified Information

DoD initiated program called "Project Spectrum" to address Cybersecurity threats

CUI Quick Reference Guide

CUI Info Sheet

CUI Handbook

CUI

Maryland MEP

Funding and assistance for Defense Contractors to comply with the DFARS and NIST 800-171 Standards for cybersecurity

Manufacturing Extension Partnership – SMBs that manufacture or procure parts and supplies

Microsoft Product Placement for CMMC – understand what MS offerings (e.g., O365, Azure, GCC) cover what aspects of CMMC

Rick Hill, PMP, RP
Richard.hill@humantouchllc.com
T: 703-910-5090 ext. 59

James Norris, RP
James.norris@humantouchllc.com
T: 703-945-1596

HUMANTOUCH