Society of SAME American Military Engineers

WELCOME

VIRTUAL MEETING WILL BEGIN AT

12:00pm Central

Society of American Military Engineers

Omaha Post

August 10th Meeting

Dedicated to National Security Since 1920

Omaha Post Meeting

Society of American Military Engineers

Omaha Post

August 10th, 2023 Meeting

Meeting Agenda

- Pledge of Allegiance
- Invocation
- New Member/ Guest Introductions
- Lunch
- Announcements
- Membership Spotlight
- Presentation
- Q&A
- Split Kitty Drawing
- Closing Remarks

Pledge of Allegiance

I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one Nation under God, indivisible, with liberty and justice for all.

Invocation

Please remain standing

Introductions

Introductions

- Welcome to New Members
- Introduction of Guests

Lunch

Dismiss by table

Announcements

- **September General Membership Meeting**
  - ►September 14, 2023 @ Field Club
  - ►Topic: Hurricane Fiona impact, Scott Perkins
- **October Membership Meeting**
  - ►October 10, 2023 @ Field Club
  - ►Topic: Solar Energy

Announcements

Volunteers needed

- Committees: Programs, Registration, Industry Day, Resilience, Service Members and Veterans Outreach, Communications
- SMP Mentors

Announcements

Post Leadership Workshop

- Omaha Post Representatives:
  - Karlus Cozart, Brec Wilshusen, and Chris Artz
  - Will back brief at next BOD meeting

Announcements

- Maj. Gen. Michael Wehr, P.E., USA (Ret.) officially installed as New Executive Director of SAME.

Membership Spotlight

TETRA TECH SNAPSHOT

WORKS IN
100+
COUNTRIES

7
CONTINENTS

Publicly traded on NASDAQ as

TTEK

$4.5 billion
ANNUAL REVENUE

WORKS ON
100,000
PROJECTS
ANNUALLY

550 OFFICES WORLDWIDE

ENR RANKINGS	
#1	Water
#1	Environmental Management
#1	Water Treatment/Desalination
#1	Wind Power
#1	Hydro Plants

22,000 CLIENTS

27,000 EMPLOYEES

Tetra Tech Delta Technologies

Tetra.Analytics	AI, machine learning, analytics, and workflow and process optimization
Tetra.Cloud	Cloud computing, cybersecurity, and software development
Tetra.Design	Smart buildings, sustainability, and energy and asset management
Tetra.Maps	Data collection, geospatial analytics, interactive dashboards, and virtual reality
Tetra.Simulate	Scenario analysis, modeling, forecasting, risk, and impact analysis

Work at Tetra Tech

We’re changing the world, one innovative project at a time. Join us today.

tetratech.com/careers

CMMC in the Wild

CMMC Brief by SAME Resilience Community of Interest

Presented by Lori Jackson, CISSP, CCP, CMMC RP
President, White Raven Security, LLC

It’s All About the Data

Federal Contract Information (FCI)

- Data that is generated by or for the Government under a contract
- Not intended for public release
- Defined in FAR 52.204-21
- CMMC Level 1 – Basic Cyber Hygiene (17 NIST controls)

If it’s not marked for public release, consider it FCI

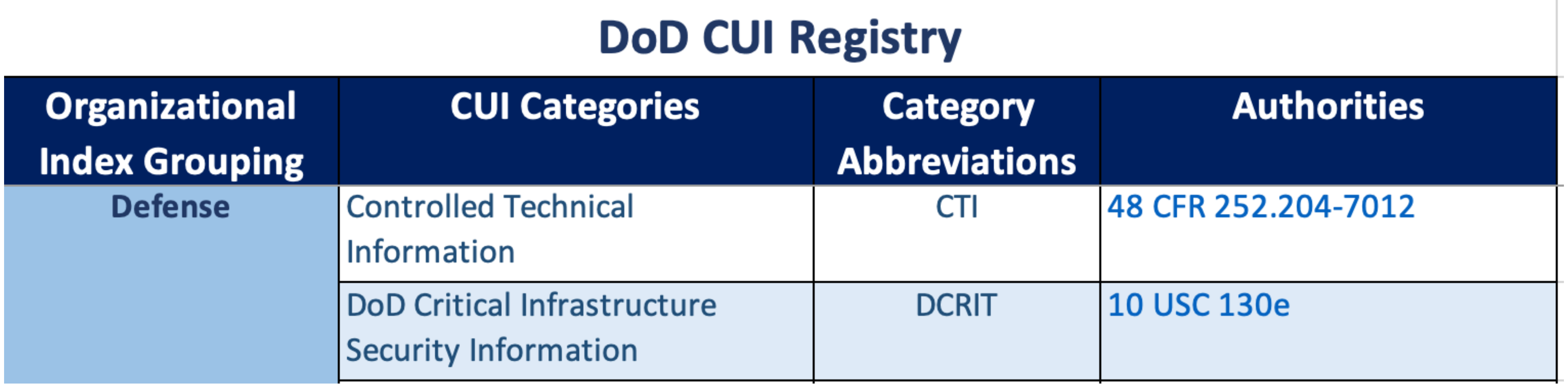
(at a minimum)

Society of SAME American Military Engineers

It’s All About the Data

Controlled Unclassified Information (CUI)

- Data that is not classified, but still requires safeguarding
  - A loss or compromise could have a serious adverse effect on mission or national security
- Defined by The National Archives and Records Administration (NARA)
- Identifying and properly labeling CUI
- CMMC Level 2 – NIST SP 800-171 (110 Controls)



DoD CUI Registry

Organizational Index Grouping	CUI Categories	Category Abbreviations	Authorities
Defense	Controlled Technical Information	CTI	48 CFR 252.204-7012
	DoD Critical Infrastructure Security Information	DCRIT	10 USC 130e

FAR 52.204-21

Basic Safeguarding of Covered Contractor Information Systems.

- Outlines minimum safeguarding measures required for Federal Contract Information (FCI)
- Requires flow-down to subcontractors if they will also handle FCI
- CMMC Level 1 maps to these requirements

DFARS 252.204-7012

Safeguarding Covered Defense Information and Cyber Incident Reporting

- Requires contractors and subcontractors to provide adequate security of CUI as it is stored or transmitted through their internal information systems
- Sets a deadline to comply with all 110 controls in the NIST SP 800-171 by December 31, 2017
- Mandates cyber incident reporting guidelines
- How to handle malicious actions (software/analysis/etc)
- Holding subcontractors accountable
- Requirements for cloud service providers

DoD Assessment Methodology

- Evaluate company’s compliance with NIST SP 800-171
- Assessment based on NIST SP 800-171A
- Uses a scoring methodology
- 3 assessment levels, each assigned a confidence level
    - Basic (self-assessment = Low confidence)
    - Medium (self-assessment + DoD assessment = Medium confidence)
    - High (self-assessment + DoD assessment + on-site verification = High confidence)
- Develop a System Security Plan to document NIST SP 800-171 compliance and a Plan of Action and Milestones for implementing each outstanding requirement

NIST SP 800-171

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

- Based on NIST SP 800-53r5
- System Security Plan (SSP)
- Plan of Action and Milestones (PoAM)

- 110 controls in 14 families
  - Access Control
  - Awareness and Training
  - Audit and Accountability
  - Configuration Management
  - Identification and Authentication
  - Incident Response
  - Maintenance
  - Media Protection
  - Personnel Security
  - Physical Protection
  - Risk Assessment
  - Security Assessment
  - System and Communications Protection
  - System and Information Integrity

DFARS Interim Rule

- DFARS interim rule change (DFARS Case 2019–D041) went into effect on November 30, 2020
- Purpose: remedy poor cybersecurity protections within the DIB
  - 252.204-7019: requires contractors to **complete a DoD Assessment** at least every three years and prior to contract award; and submit a score to the SPRS system.
  - 252.204-7020: requires contractors to **allow the government access to their facility**, systems, and personnel in order to conduct a Medium or High Assessment. Requires Primes to ensure their subcontractors have a proper and current assessment on file.
  - 252.204-7021: requires contractors have a CMMC level equivalent to the sensitivity of the information expected on the contract and maintain that level of compliance for the duration of the contract.

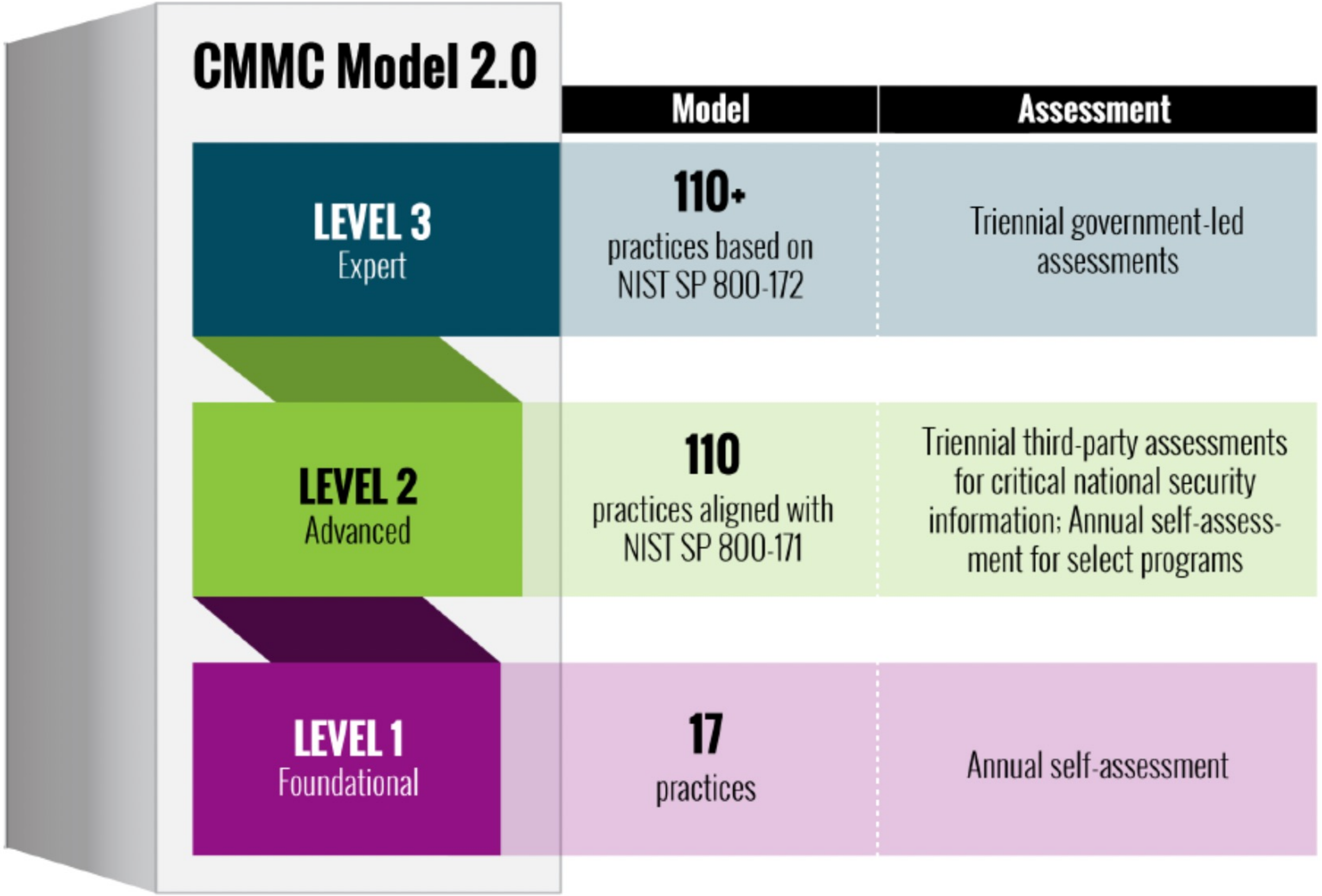
Status of the CMMC Rule

- DFARS 252.204-2021: The first CMMC rule
  - 800+ public comments, led to CMMC version 2.0
- CMMC Version 2.0
  - Level realignment (CMMC aligns solely with NIST SP 800-171)
  - Self-assessment and attestation
  - Allowed PoAMs (with caveats)
  - Level 2 “bifurcation”

- July 28, 2023: DoD submitted a proposed rule to OMB Office of Information and Legislative Affairs
  - Expected to amend Title 32 (48 CFR will be amended after 32 CFR)
  - Expected to be a proposed rule with a 60-day public comment period.

Cybersecurity Maturity Model Certification (CMMC)

- The DoD expects cybersecurity to become a core pillar - like quality and safety
- *Most* contractors will need to be certified by a 3rd party assessor in order to work on any DoD contract
- Framework aligns with NIST Special Publication 800-171 (110 security controls)



CMMC Model 2.0

	Model	Assessment
LEVEL 3 Expert	**110+** practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	**110** practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	**17** practices	Annual self-assessment

A Path Forward for Small and Medium Businesses

Recognize the Importance

“Failure to have or to make progress on a plan to implement NIST SP 800-171 requirements may be considered a material breach of contract requirements. Remedies for such a breach may include: withholding progress payments; foregoing remaining contract options; and potentially terminating the contract in part or in whole.”

- Contractual Remedies to Ensure Contractor Compliance with Defense Federal Acquisition Regulation Supplement Clause 252.204-7012, June 2022

Review Your Contracts

- Look for DFARS 252.204-7012 in your contract or subcontract agreements
- Avoid CUI if possible
  - No CUI = CMMC Level 1
  - CUI = CMMC Level 2 (and potentially a 3rd party assessment)
- Examine your supply chain – if subconsultants will handle CUI, flow-down the requirements

Action Items:

✓ Review all contracts

✓ Determine your CMMC level goal (do you already have a NIST requirement?)

✓ Determine the data your subs will handle

Asset Inventory

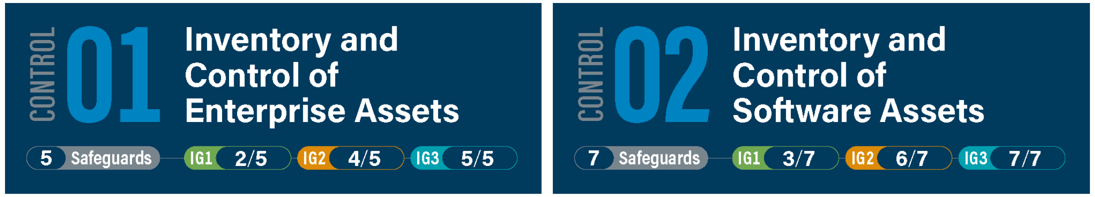
- Determine *all* the devices that are connected to your network, as well as software installed
- Unmanaged or unknown devices or software can be an entry point into your system
- Remember that any device that you don't control should not contain company or government data (this includes personal devices)

Action Items:

✓Develop an asset inventory

✓Keep it up-to-date

✓Prevent or manage the use of personal devices



CONTROL 01 Inventory and Control of Enterprise Assets

5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5

CONTROL 02 Inventory and Control of Software Assets

7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7

-CIS Critical Security Controls, v8

Understand Your Data

- Inventory the data you have – where might you have CUI?
- Understand how the data flows and who can access it
- Have a plan for how you'll dispose of devices with old data

Action Items:

✓Create a data management process

✓Develop a data inventory

✓Create a data flow diagram

CONTROL 03 Data Protection

14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14

-CIS Critical Security Controls, v8

Define Your Network

- Understand the boundaries around and within your network
- Compare that with your data flow diagram to understand where data resides and where it flows
- Determine if CUI can be segmented away from the whole system – a smaller surface area is easier to protect

Action Items:

✓Develop a network diagram

✓Identify where your data flows

✓Narrow your scope, if possible

Conduct a DoD Self-Assessment

- Follow the DoD Assessment Methodology and assess your system
- Determine which controls you are meeting and where you have gaps
- Gather evidence as you go
- This can be a daunting task; hire help if you need it

Action Items:

✓Score yourself against NIST SP 800-171

✓Develop a System Security Plan

✓Create a Plan of Action and Milestones for the controls you have not implemented

Assessing Risk

- Now that you know your gaps, what risks do they pose?
- Is your company frequently targeted with phishing emails?
- Determine your risks based on how you conduct business.
- Identify potential threats, how they might impact the business, and how you could remediate them.

Action Items:

✓Conduct a risk assessment

✓Develop a plan to remediate risks

Documentation is Critical

- Documentation is the first thing an assessor will ask for
- Be sure you can follow your own documentation
- Make employees aware of the documents/rules that pertain to them
- Use documentation to monitor your systems and progress, and update when necessary

Action Items:

✓Document your processes

✓Maintain a repository of vendor agreements – responsibility matrix

✓Develop policies and procedures to address security controls

Updates are Important

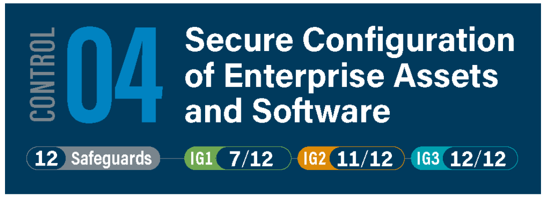
- Be sure that all devices and software are updated when new patches are released
- Sign up for alerts from manufacturers, software vendors, and CISA
- Use your inventory to guide when and what updates are necessary

Action Items:

✓Sign up for alerts

✓Keep your inventory up-to-date

✓Develop a process for updating hardware and software



CONTROL 04 Secure Configuration of Enterprise Assets and Software

12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12

-CIS Critical Security Controls, v8

Meeting Close

- Split Kitty Drawing
- PDHs available from the Omaha Post Website