ncmbc

CONNECTING BUSINESS AND MILITARY

# NORTH CAROLINA MILITARY BUSINESS CENTER CYBERCHAT SERIES – WORKSHOP 2

www.cybernc.us

20 January 2021

# Agenda – CyberChat Workshop #2

- Series description
- Questions since last session –
  - Direction from prime contractors – how to handle unnecessary flow-down requirements.
  - Google example
  - Asset protection for working remotely
- Homework review – management/ownership buy-in, CUI or FCI, current contracts, questions/comments
- Quick review
- Project status
- Network diagram
- Asset Inventory
- Latest CMMC/cybersecurity updates
- Homework

# CyberChat Series Description

- Objective: To help defense contractors develop a cybersecurity quality management system [QMS] program that is compliant with [DFARS 252.204-7021] – the new CMMC regulation – and protects national security.
- Technical advice regarding cybersecurity tools and providers will not be given by the NCMBC. The focus will be on developing a compliance roadmap using tools and information provided on www.cybernc.us.
- CyberChats are not to be used to sell products or services. IT/Cyber companies can sign up as a resource for defense/federal contractors. Note: the NCMBC does not vet these companies. https://www.ncmbc.us/matrices-resources/

# How to Handle Flow-Down Requirements

- Scenario #1 – your prime is flowing down requirements pertaining to CUI, such as CMMC Level 3 and/or Self-assessment to the 110 controls in NIST, but you don't believe you touch CUI. [Note: these instructions come from the Defense Acquisition University – not the NCMBC]
    - ➢ Send an email to your contact at the prime
        - ○ If CMMC is flowed down, ask for help locating an assessor. There aren't any available yet - they may need to find that out for themselves.
        - ○ State that you have done your due diligence in determining the type of data you process/create on behalf of the DoD and have determined that you do not touch CUI. [Due diligence means you have reviewed the contract thoroughly,  have reviewed the CUI Registry and taken the mandatory DoD training – links available on FCI/CUI tab on cyberNC.us]

# How to Handle Flow-Down Requirements

- ○ Give the prime 30 days to respond with a rebuttal – evidence that you do/will touch CUI. If you don't receive a response, proceed as though you don't process CUI. National security may be at stake – so be sure you are right.

- Scenario # 2 – your prime is flowing down cybersecurity requirements pertaining to CUI and you are confident that you do touch CUI.
  - ➢ Determine if you can do the work without touching CUI.
  - ➢ Present your ideas – in writing – to your contact at the prime. Include the cost differential between CMMC Level 1 certification and CMMC Level 3 certification. [$3000 vs $50,000]

# Google – FedRAMP Certified?

- Question:  Why are Google datacenters FedRAMP certified at different levels, and why isn’t there a datacenter certified FedRAMP “moderate” in North Carolina? What should NC companies do? Answers courtesy of Mike Parsons.
  - Answer: Certification depends on demand. For example, the datacenter in South Carolina is FedRAMP certified high and moderate, but there isn’t one in North Carolina with that same level of certification. Since Boeing is located in SC, it makes sense that they would demand a datacenter that is FedRAMP certified high or moderate
  - Contact your G-Suite rep. and ask them what it would cost to route you to another datacenter. Make sure it’s in the USA.

# Asset/Data Protection for Working Remotely

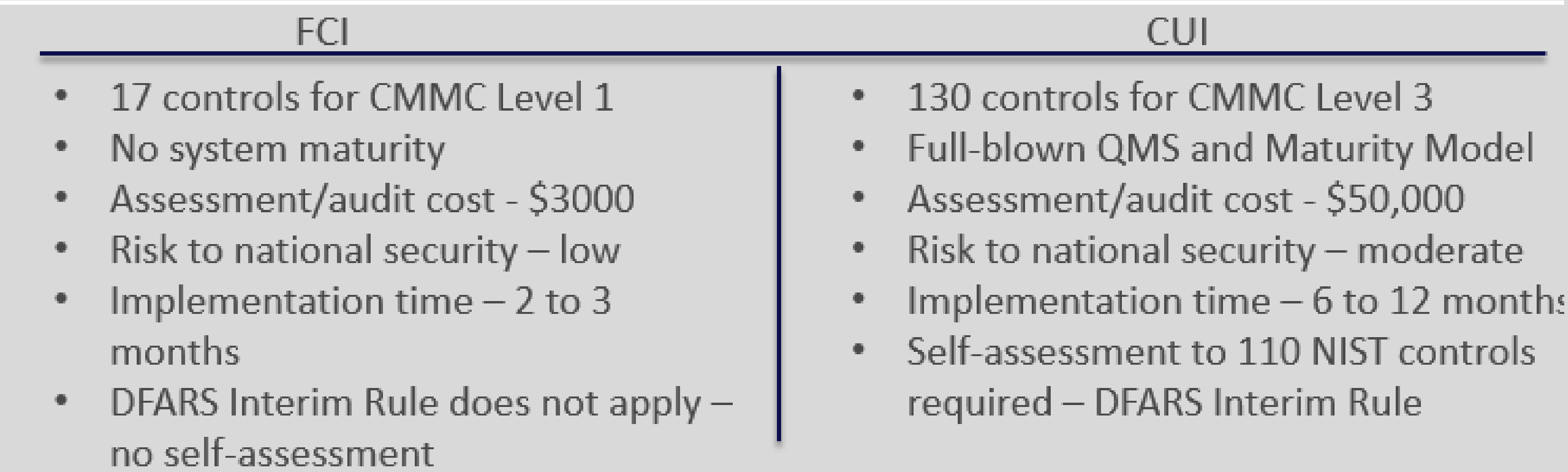
- Best Practices:
  - ✓ Employees working at alternative work sites must use company-provided computer and network equipment unless other devices have been approved.
  - ✓ Remote workers must not use their own mobile computing devices, computers, computer peripherals, or computer software for company teleworking business without prior authorization.
  - ✓ All systems that access company networks remotely must have an anti-virus package continually running.
  - ✓ Equipment should be located and/or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
  - ✓ Remote workers must not change the operating system configuration or install new software.

# CyberChat #1 Homework

QUESTIONS?

# CyberChat Workshop #1 - Review

- Data – cybersecurity regulations are data-driven
  - ✓ FCI – Federal Contract Information = CMMC Level 1
  - ✓ CUI – Controlled Unclassified Information = DFARS 252.204-7012/7019, then CMMC Level 3



FCI

- 17 controls for CMMC Level 1
- No system maturity
- Assessment/audit cost - $3000
- Risk to national security – low
- Implementation time – 2 to 3 months
- DFARS Interim Rule does not apply – no self-assessment

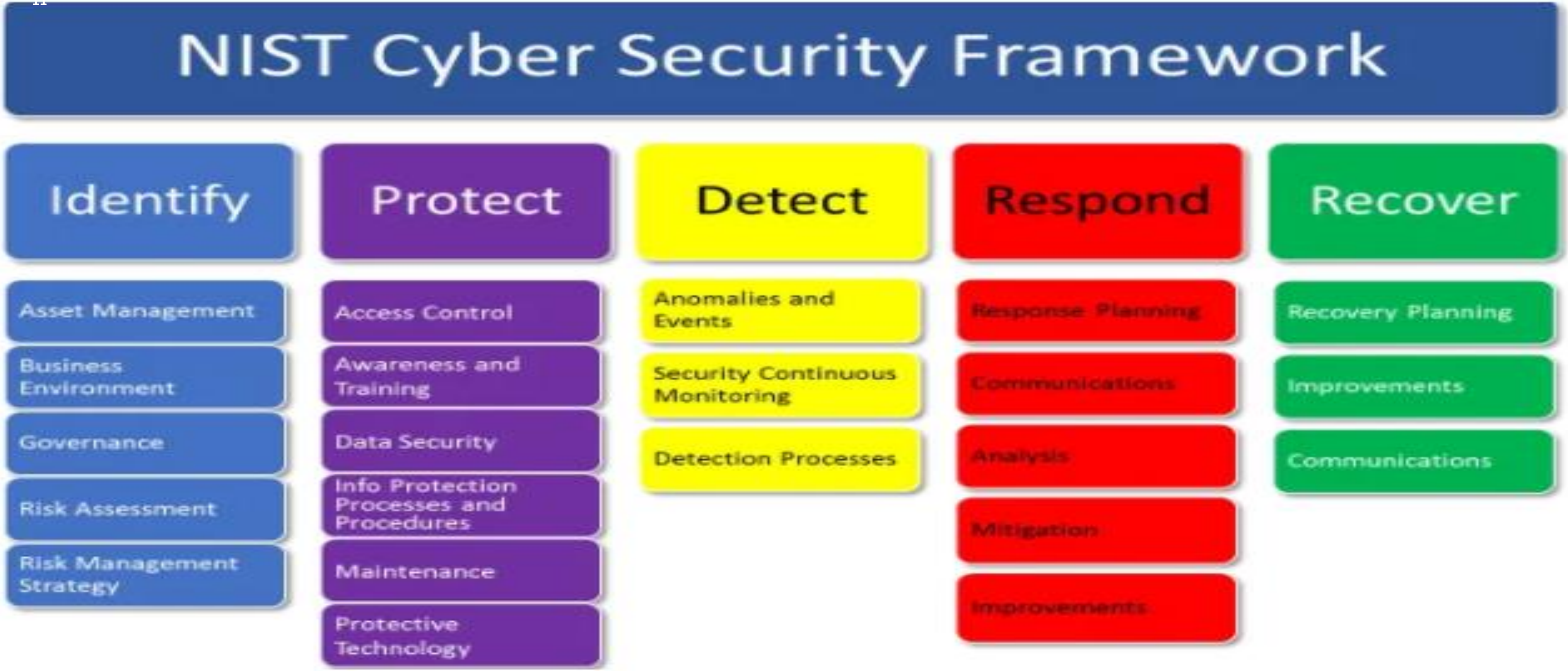
CUI

- 130 controls for CMMC Level 3
- Full-blown QMS and Maturity Model
- Assessment/audit cost - $50,000
- Risk to national security – moderate
- Implementation time – 6 to 12 months
- Self-assessment to 110 NIST controls required – DFARS Interim Rule

# CyberChat Workshop #1 - Review

- Work with primes/contracting officers/subs to eliminate/minimize CUI
- CMMC requires culture change – requires buy-in and support from upper management/ownership; cybersecurity must be integrated into every department/function and be considered when making company decisions; employees understand their responsibilities regarding cybersecurity; engage in continuous improvement of the system.
- Use the tools/resources/information on cyberNC.us.

# Big Picture



## NIST Cyber Security Framework

| Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|
| Asset Management | Access Control | Anomalies and Events | Response Planning | Recovery Planning |
| Business Environment | Awareness and Training | Security Continuous Monitoring | Communications | Improvements |
| Governance | Data Security | Detection Processes | Analysis | Communications |
| Risk Assessment | Info Protection Processes and Procedures | | Mitigation | |
| Risk Management Strategy | Maintenance | | Improvements | |
| | Protective Technology | | | |

# Cybersecurity Compliance Project Status

- Current State
  - ✓ Review contracts for cybersecurity DFARS clauses
  - ✓ Data – FCI or CUI
  - ✓ Upper management/ownership buy-in
  - ○ Initial employee training – project introduction
  - ○ Network Diagram
  - ○ Asset inventory
  - ○ Data flow diagram
  - ○ Risk assessment
  - ○ Gap analysis

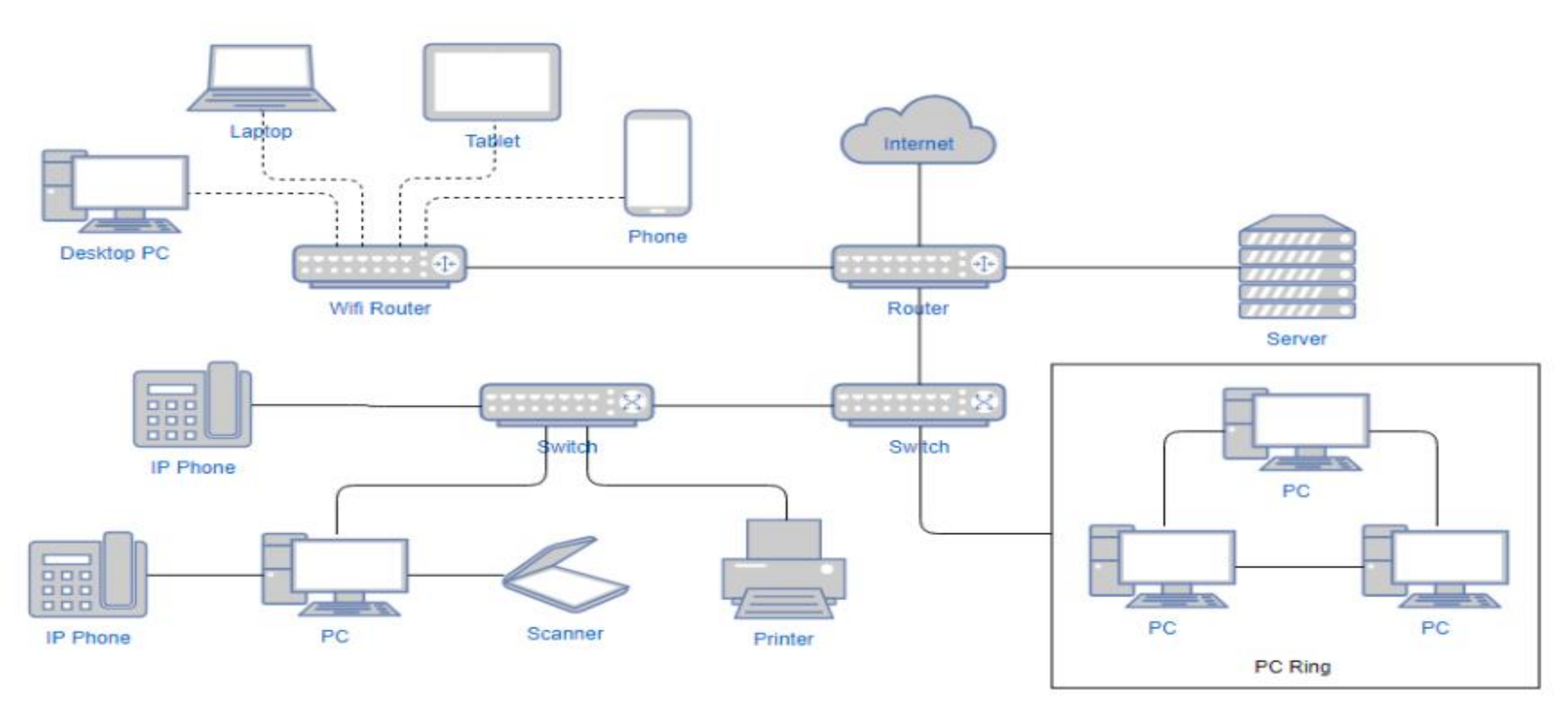
# Employee Introductory Training

- Why do employees need to understand your cybersecurity compliance project?
  - ➢ The majority of cyberattacks target people; e.g., business email compromise [impersonating trusted people] and email account compromise [compromise a victim’s email account and send convincing emails using their credentials]
  - ➢ Employees are your first line of defense against those attacks, so you need their buy-in that the company culture surrounding cybersecurity is changing
  - ➢ They need to understand the project and what might be required of them, including their responsibility for continuous improvement
  - ➢ Prepare them for technical training

# Employee Introductory Training

- Training should cover:
  - ➢ Why changes in cybersecurity culture are needed [can use slides from CyberChat #1 or any other cybernc.us presentation]
    - ✓ Protect national security
    - ✓ DoD regulations
    - ✓ Protect company
  - ➢ Project details
    - ✓ Assess current state – data, IT assets, network, data flow, gap analysis, risk analysis
    - ✓ Implementation phase – filling gaps in controls/practices, establishing policies and procedures, employee technical training
    - ✓ Assessment
    - ✓ Continuous improvement

# Network Diagram



# Asset Inventory

- Cloud storage
- Contracts with 3rd party technology suppliers
- Desktop computers
- Digital cameras
- Fax machines
- Scanners
- Keyboards
- Laptops
- Monitors
- Mouse
- Printers
- Routers
- Switches
- Servers
- Smartphones
- Software applications
- Software licenses
- Tablets
- Internet of Things [IoT]
- Cables

# CMMC/Cybersecurity Updates

- It appears that Katie Arrington will continue in her position – her job won't be affected by the change in administration

# Homework – CyberChat #1

1. Review your DoD contracts to see if DFARS 252.204-7012 or FAR 52.204-21 are referenced. DFARS = CUI     FAR = FCI
2. If DFARS 7012 is referenced, try to determine if you really do touch CUI. If you don't, then the clause doesn't apply.
3. If you need help understanding CUI, check out the CUI Registry and the DoD CUI training. Links are in the chat and on cyberNC.us under the FCI/CUI tab.
4. If you do touch CUI but don't feel it's necessary to perform the project, consider talking to your contracting officer or prime about ways to eliminate the need to process/store/create CUI.
5. Develop a presentation – or use one of ours – for upper management. You need their buy-in to do this project and provide you with the authority and resources necessary to do it effectively.

# Homework – CyberChat #1

- Request CMMC Level 1 in a Box materials from cyberNC.us website

# Homework – CyberChat Workshop #2

- Draw a network diagram
- Begin an asset inventory

ncmbc
CONNECTING BUSINESS AND MILITARY

# NORTH CAROLINA MILITARY BUSINESS CENTER CYBERCHAT SERIES – WORKSHOP 2

www.cybernc.us

20 January 2021