NORTH CAROLINA MILITARY BUSINESS CENTER
CYBERCHAT SERIES – WORKSHOP 3

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/

Agenda – CyberChat Workshop #3

- Latest CMMC/cybersecurity updates
- Questions from last session
- Homework questions from CyberChats 1 and 2 - management/ownership buy-in, CUI or FCI, current contracts, draw a network diagram, begin an asset inventory
- Quick review of CyberChats 1 and 2
- Documentation
- Continuous Improvement
- Project status
- Homework

Notes from CMMC-AB Town Hall

- Two “pathfinder” programs; one from the Missile Defense Agency and one from DLA. DCMA performed mock assessments, worked on contract language, data flow, etc. DoD paid for pathfinder program.
- Remainder of DoD programs through Sept. 31, 2025 will be considered “pilot” programs and must go through various approvals to be considered for the pilot program.
- Anticipate the Navy F/A-18E/F Full Mod of SBAR & Shut Off Valve program to be the first pilot program with CMMC requirements.
- The initial 7 programs that were nominated for the pilot program will need to go through an additional vetting process due to the change in administration.
- DoD is continuing to look for medium-sized programs with CUI requirements to complete the goal of 15 programs in FY 2021.

Notes from CMMC-AB Town Hall

- Pilot programs will have priority for assessments.
- Currently have 100 certified provisional assessors. Looking at the possibility of adding more.
- DoD is working with the Dept. of Homeland Security, GSA and the Dept. of the Interior to get CMMC included in some of their programs. DHS will most likely be first – possibly a Coast Guard Program
- STARS 3 and Polaris are being considered for CMMC requirements
- Registered Practitioner training is being redeveloped. RPs that took the initial training must take the new training – at no charge
- Hoping to have licensed curriculum available by early summer
- CMMC-AB Marketplace is being redesigned

Notes from CMMC-AB Town Hall

- To be considered “registered” or “certified” you must be trained by a Licensed Instructor that is affiliated with a Licensed Training Provider. Individuals may not take exams without proof of training.
- CMMC-AB has contracted with Scantron to develop the exams. Currently working on exams for Certified Professionals and Certified Assessors at Levels 1 and 3
- The AB is continuing the executive search for a CEO
- “Final” rule expected to be approved sometime during the second quarter
- The CMMC-AB plans to attain registration to ISO 17011:2017 (international standard for accreditation bodies) in 24 months. At that point they will be an ISO Accreditation Body. After they have attained registration, C3PAOs will be required to attain registration to ISO 17020 – international standard for certification bodies.

Notes from CMMC-AB Town Hall

- There will be two distinct lines of business:
  - AB: responsible for C3PAO vetting, licensing and accreditation to DoD requirements and ISO 17020, informal training, RPOs and Registered Practitioners
  - CAICO: Responsible for training and testing Certified Assessors and License Instructors
- Organizations Seeking Certification (OSCs) do not need to have their cybersecurity system in place for a specified amount of time prior to a certified assessment.

- ***DoD is working on a CUI guide and guidance for acquisition commands!***

Notes from CMMC-AB Town Hall

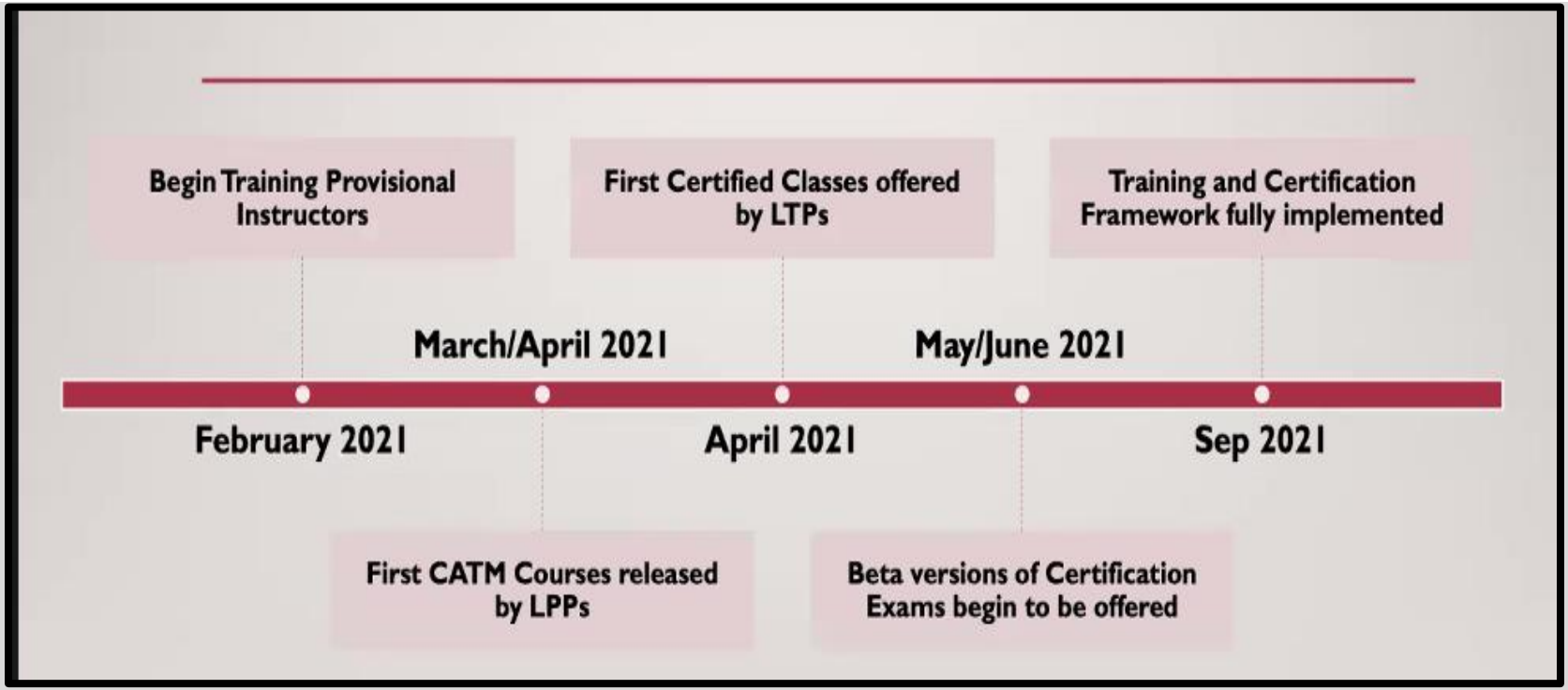
- Licensed Software Provider (LSP) – leverage specifications and requirements provided by the CMMC-AB to build software solutions that assist Certified Assessors, Certified Professionals, C3PAOs, RPs and RPOs in delivering consistent, high-quality CMMC services to their clients.

Notes from CMMC-AB Town Hall

CURRENT STATUS OF CREDENTIALS

Credential	December: Total	December : Pending	December: Approved	January Total	January Pending	January Approved
RP	980	511	469	1439	378	1060
RPO	297	46	251	382	43	339
C3PAO	369	349	20	408	355	53
LPP	16	0	16	18	2	16
LTP	0	0	0	22	10	12
Provisional Assessors	100	0	100	100	0	100

Notes from CMMC-AB Town Hall



CyberChat #1 Review - Data

- 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	CUI
• 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	• 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

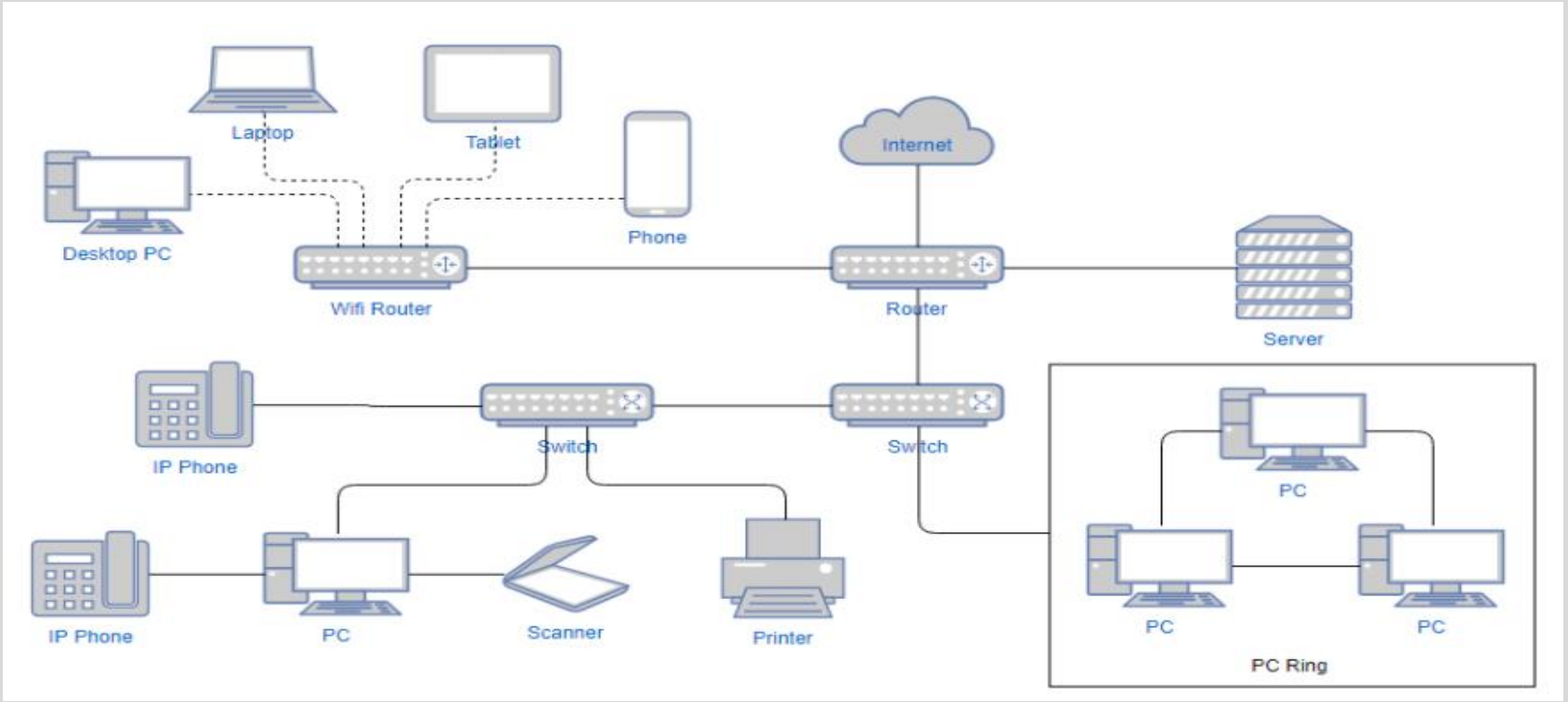
CyberChat #2 Review – Employee Training

- 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

CyberChat #2 Review – Employee 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

CyberChat #2 Review - Network Diagram



CyberChat #2 Review - 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

Documentation

- As you work through setting up your cybersecurity quality management system, it is a good idea to begin documenting the process.
  - Meetings/work sessions should be documented with attendees, dates, action items – who they are assigned to and due date.
  - Track action items to completion
  - If you want to keep everything in one place, use the CMMC Level 1 in a Box Guide. Tabs can be added to record meetings, actions, etc.
  - Documenting the process will help keep you organized, and the documents can be used as audit “artifacts” – documents that provide proof that you are doing what you said you are doing.

If an activity isn’t documented, it didn’t happen.

Continuous Improvement

Example: A new employee clicks on a link that contains a virus that disrupts the company network. Do you fire the employee or try to figure out the root cause of the error? If your company embraces continuous improvement, you want to get to the root cause of the error, so it doesn't happen again. So, you begin your investigation:

1. You speak with the employee and find out he never did the required cybersecurity training.
2. You speak with HR to find out why he was authorized to begin work without going through the appropriate training. HR tells you that the Operations Manager needed this person immediately due to production schedule issues.
3. You speak with the Operations Manager and find out that a huge unscheduled order had come in and the only way to make schedule was to get the new person working immediately.

Continuous Improvement

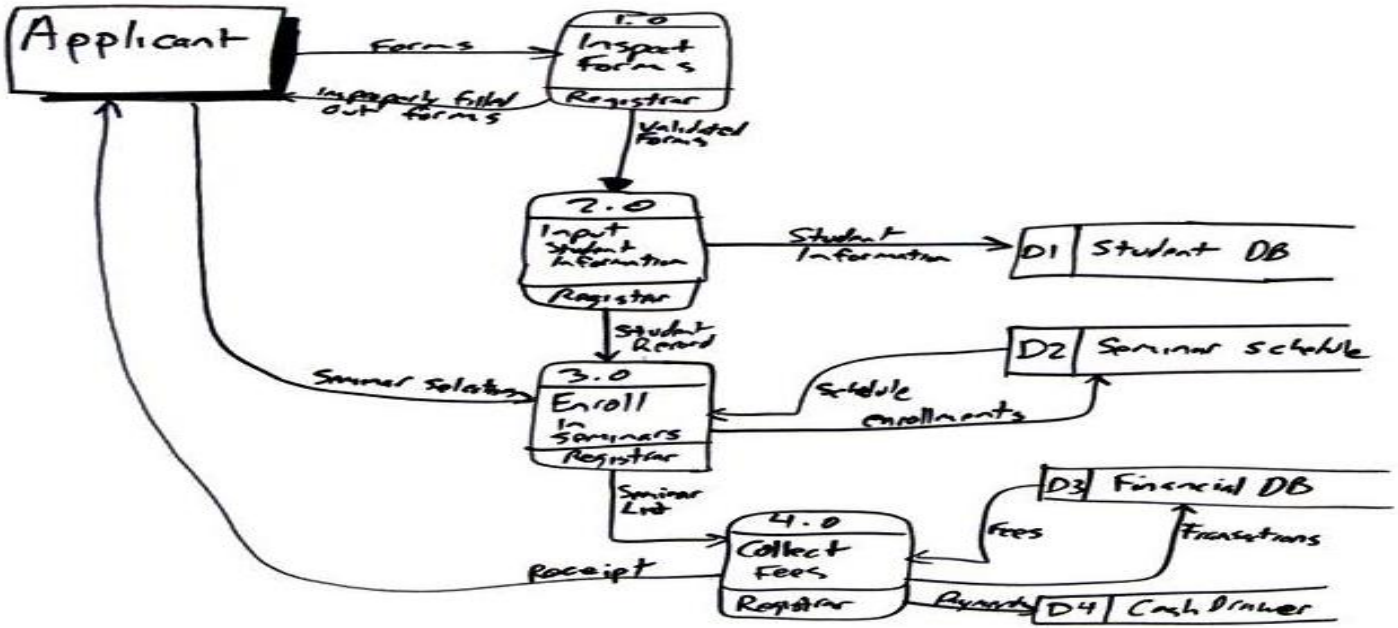
4. You speak with the Sales Manager about why the order was “unexpected”. You find out that the order was expected but somehow didn’t get added to the production schedule.
5. You go back to the Operations Manager to find out why the order never got added to the production schedule. You find out that the scheduler was on vacation a few weeks ago – the time when the order was taken.
6. You speak with the IT manager to find out why the email got through the spam filter. You find out the settings had not been changed since the last “incident” because there was no corrective action taken.

So, the real root cause of the virus shutting down your network is a lack of policies and procedures and a lack of understanding of the importance of cybersecurity.

Data Flow Diagram

- Diagram the flow of **DoD data** in your network – from when the data "enters" your network until it flows out of your network. The information may come from the contracting officer, your prime, etc. and may be flowed down to your subs/suppliers.
- No need for a formal diagram. The goal is to know how and where the data flows, is stored, transmitted, etc. and who is handling the data and who has access to the data.
- This exercise is critical to determining "scope"

Data Flow Diagram



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 – for DoD data
  - Risk assessment
  - Gap analysis

Homework – CyberChat #3

1. Develop a presentation (doesn't have to be formal) to introduce employees to the cybersecurity program you are creating
2. Begin working on a data-flow diagram

Remember to document your work!

Homework – CyberChat Workshop #3

- Draw a network diagram
- Begin an asset inventory

NORTH CAROLINA MILITARY BUSINESS CENTER
CYBERCHAT SERIES – WORKSHOP 3