NORTH CAROLINA MILITARY BUSINESS CENTER
CYBERCHAT SERIES – WORKSHOP 1

Laura Rodgers and Bob Burton

- Laura – Business Development Professional with over 20 years in defense contracting with Lockheed-Martin and General Dynamics Information Technology; background in training, compliance, quality management systems and maturity models. Office at Wake Tech Community College – RTP campus. Full bio: www.ncmbc.us/laura-rodgers/

- Bob - Senior Manager, North Carolina Defense Technology Transition Office; retired Special Forces CSM with over 30 years of special operations leadership; served as a military mentor for Hacking for Defense. Office at First Flight Venture Center, RTP. Full bio: www.ncmbc.us/bob-burton/

NC Military Business Center

The North Carolina Military Business Center (NCMBC) is a statewide business development and technology transition entity of the North Carolina Community College System, headquartered at Fayetteville Technical Community College. Website: www.ncmbc.us .

The mission of the NCMBC is to leverage military and other federal business opportunities to expand the economy, grow jobs and improve quality of life in North Carolina.

The NCMBC's primary goal is to increase federal revenues for businesses in North Carolina. Business Development Professionals are located throughout the state to assist companies with their federal contracting needs.

One of our strategic initiatives is to provide tools such as training and resources to help overcome contracting obstacles – in this case, cybersecurity regulations.

NCMBC MatchForce

Companies can sign up for MatchForce, our free tool that matches North Carolina businesses to government contracts. http://www.matchforce.org/ . Receive a daily email with opportunities that match your company profile.

Bottom line- we are here to help companies in the NC federal marketplace succeed. Please let us know how we can help.

Agenda – CyberChat Workshop #1

- CyberChat series description
- Preliminary series syllabus
- Tour of CyberNC.us
- Why cybersecurity is important
- Terminology and regulations
- It’s all about the data – FCI/CUI
- Begin with the end in mind
- The “Big Picture”
- Latest CMMC/cybersecurity updates – Pilot Program and WhatsApp
- 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. The focus will be on developing a compliance roadmap using tools and information provided on www.cybernc.us.
- Developing a QMS requires a commitment on the part of the organization and its employees. Recommend designating someone to manage the QMS project – that individual will need time, financial resources and the authority required to complete the project successfully. It is helpful to have a designated space to work - a conference room or virtual workspace.

CyberChat Series Description

- Must have top management buy-in and support – tone at the top is ***critical*** to the success of the project.
- Employees must be informed and given the opportunity to contribute and participate in the process. Recommend a “lunch and learn” session to introduce the project and the person/team responsible for implementation.
- Requires IT, cyber and QMS/Maturity Model skills. Companies that don’t have IT/cyber staff may need a consultant. If the organization uses a service provider to handle IT/cyber management, the service provider needs to be involved in this project. If the service provider has access to your data, they need to be certified to the same CMMC Level. In the case of cloud service providers, they need to be FedRAMP moderate certified, or the equivalent.

CyberChat Series Description

- 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/

Cybersecurity Compliance Project

- Cybersecurity compliance project
  - Figure out where you are
  - Figure out where you need to be
  - Everything in between is the project

CyberChat Workshop Syllabus

- Workshop 1 – Terminology, regulations, data – FCI/CUI, cybersecurity quality management system prep, cyberNC.us
- Workshop 2 – CMMC Level 1 review, network diagrams, data flow, developing a cybersecurity training program
- Workshop 3 – Asset inventory, gap assessments, DFARS Interim Rule requirement to upload results of gap assessment to the Supplier Performance Risk System [SPRS]
- Workshop 4 - Risk assessments, audit scope, how to handle an audit.
- Workshops 5 – 13 – Going through the 17 CMMC Domains and corresponding controls

Tour of cyberNC.us

Tools and resources to help companies in NC with cybersecurity compliance

Why is Cybersecurity so Important?

- 70% to 80% of DoD data resides on contractors' networks and there are over 300,000 companies in the defense industrial base. Data is the new currency.
- $600B [1% of GDP] is lost to cyber theft each year to our adversaries
- Half of all cyber attacks are targeted at small businesses, and some never recover due to the high cost of a cyber attack
- Our adversaries are looking for our vulnerabilities and weaknesses in attempt to steal our technology and disrupt our supply chains.
- It is our duty to protect our country from its adversaries.
- The SolarWinds breach proved that our adversaries can find our vulnerabilities and capitalize on them. The latest count is 180K companies affected.

Terminology – FCI and CUI

- Federal Contract Information [FCI] is information that is not marked as public or for public release and is subject to minimum cybersecurity requirements. FCI does not include information provided by the government to the public or simple transactional information, such as that required to process payments. While this information is not as sensitive as CUI, it must still be protected.

- Controlled Unclassified Information [CUI] - is information that requires safeguarding or dissemination controls but is not considered classified – it is information that legally cannot be made public. CUI must be legally protected but is not deemed sensitive enough to require a high-level security level clearance to access. CUI is data, that if leaked or accessed by our adversaries, could negatively impact national security by showing our vulnerabilities or giving our adversaries an advantage.

Terminology - CUI

Examples of CUI include legal material, health documents, technical drawings and blueprints, intellectual property, ITAR controlled documents/products, etc. Click here for a link to the CUI Registry housed in the National Archives. It is important to look at each category, not just the Defense category.

Please click here to access DoD CUI training. The course is mandatory training for all of DoD and industry personnel with access to controlled unclassified information.

NOTE: Not all company CUI is covered by the FAR/DFARS/CMMC. The regulations apply only to data that is processed, stored and/or created ***on behalf of the DoD****.*

Terminology and Regulations

- FAR: Federal Acquisition Regulation – set of rules regarding government procurement
  - FAR 52.204-21 – Basic Safeguarding of Covered Contractor Information Systems – covers FCI and is equivalent to CMMC Level 1 - applies to approximately 60% of defense contractors
- DFARS: Defense Federal Regulation Supplement – additional set of rules for DoD procurement
  - DFARS 252.204-7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting – covers CUI and points to the 110 controls in NIST SP 800-171. Applies to 38% of defense contractors.

Terminology and Regulations

- NIST – National Institute of Standards and Technology – physical sciences laboratory and non-regulatory agency of the US Dept. of Commerce whose mission is to promote innovation and industrial competitiveness. NIST SP 800-171 provides the 110 controls for compliance to DFARS clause 252.204-7012
- DFARS Interim Rule – 9/29/2020 – added 3 new DFARS clauses in addition to DFARS 252.204 -7012
  - 252.204-7019 – added the DoD Assessment Methodology. Companies must now do a self-assessment to NIST 800-171 using the new methodology and upload the score to the Supplier Performance Risk System (applies if a company touches CUI)
  - 252.204-7020 – provision for DoD auditors to have access to company facilities if it is determined that an audit is needed (applies if a company touches CUI)
  - 252.204-7021 – CMMC – applies if a company touches FCI or CUI. Does not apply to COTS

FCI or CUI?

Why does the type of data matter?

Why the Type of Data Matters

FCI	CUI
• 17 controls for CMMC Level 1 • CMMC assessment/audit cost - $3000 • Risk to national security – low • Implementation time – 2 to 3 months • No self-assessment needed to comply with DFARS Interim Rule	• 130 controls for CMMC Level 3 • CMMC assessment/audit cost - $50,000 • Risk to national security – moderate • Implementation time – 6 to 12 months • Self-assessment required per DFARS Interim Rule

Before you can begin your compliance project, it is **essential** to know what type(s) of data your company touches. It is also **essential** to reduce the amount of CUI housed with defense contractors. Will require unprecedented amount of collaboration between contracting officers, primes and subs.

Begin With the End in Mind

What does an optimized cybersecurity program look like?

- 100% compliant
- Developed around company - vision, mission, risks,
- Integrated into every department/function
  - ✓ C-Suite/top management – cybersecurity is foundational – considered when making decisions
  - ✓ Human Resources – Cybersecurity risks pertaining to employees considered, cybersecurity responsibilities in job postings, training during employee on-boarding, employee goals, employee evaluations.
  - ✓ Training – cybersecurity included in training programs.
  - ✓ IT – cybersecurity considered prior to changes in hardware, software, apps, etc. Can't "inspect" cybersecurity into a system. It must be designed into the system.

Begin With the End in Mind

- Employees – understand high-level cybersecurity regulation requirements, understand their responsibilities regarding cybersecurity, including reporting incidents and providing suggestions
- Subs/suppliers – ***appropriate*** cybersecurity regulations flowed down via contracts. Work with subs/suppliers on compliance issues
- Engaging in continuous improvement – establishing and collecting metrics, regular reviews of the system for what works and what doesn't, why it doesn't work – root cause analysis, options to fix the problems, etc.
- Staying up to date on the latest services, products, breaches, etc.
- Managing configuration of elements of the system

CMMC requires a change in company culture

Changing Company Culture

1. Starts at the top. There needs to be a clear value-proposition – why do we need to make this change? Protect national security, continue as a defense contractor, etc. *Passing an audit is not a good value proposition.*
2. Involves everyone – to get buy-in from employees they need to feel like they are involved in the change process – from the beginning. Need to solicit their ideas and feedback.
3. Provide detailed information about how the project will be handled – dates, milestones – the project plan.
4. Celebrate successes as a group.
5. Don't use failures as an opportunity to assign blame or prove that the project is going to fail. Do root cause analyses, then adjust – update policies/procedures, provide more training, etc.

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 Regulations - Update

- CMMC is expected to be in 15 solicitations in FY 2021. First round of pilot programs nominated for consideration:
  - U.S. Navy
    - ✓ *Integrated Common Processor*
    - ✓ *F/A-18E/F Full Mod of the SBAR and Shut off Valve*
    - ✓ *DDG-51 Lead Yard Services / Follow Yard Services*
  - U.S. Air Force
    - ✓ *Mobility Air Force Tactical Data Links*
    - ✓ *Consolidated Broadband Global Area Network Follow-On*
    - ✓ *Azure Cloud Solution*
  - Missile Defense Agency
    - ✓ *Technical Advisory and Assistance Contract*

WhatsApp's New Privacy Policy

"Long favored as a way to communicate with enhanced privacy, WhatsApp, has released a new privacy policy that removes its users' ability to opt out of sharing data with Facebook, WhatsApp's parent company." - Association for Data and Cyber Governance

"This isn't about WhatsApp sharing any more of your general data with Facebook than it does already, this is about using your data and your engagement with its platform to enable shopping and other business services, to provide a platform where businesses can communicate with you and sell to you, all for a price they will pay to WhatsApp." - Zak Doffman, Forbes

Homework

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

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

NORTH CAROLINA MILITARY BUSINESS CENTER
CYBERCHAT SERIES – WORKSHOP 1