ncmbc
CONNECTING BUSINESS AND MILITARY

# NORTH CAROLINA MILITARY BUSINESS CENTER CYBERCHAT SERIES – WORKSHOP 5

www.cybernc.us

10 February 2021

# 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 #5

- Mobilize IO CyberChat Community – Bob Burton
- Latest CMMC/cybersecurity updates
- Questions from CyberChats 1, 2, 3 and 4 - management/ownership buy-in, CUI or FCI, current contracts, draw a network diagram, begin an asset inventory, data-flow diagram, employee intro. to cybersecurity, documentation, continuous improvement, cybersecurity risk analysis
- Risk review
- Scope
- Homework

# Mobilize CyberChat Community

**WHY:** To help companies in the North Carolina defense industrial base achieve compliance to cybersecurity regulations. Our goal is to “stack the deck” with companies that are compliant, so the DoD awards more contracts to North Carolina companies. The NCMBC will use the platform as an additional tool to keep you updated on cybersecurity events, activities, training, and resources.

**WHAT:** Mobilize is a private information sharing platform that allows members to collaborate, share knowledge; create teaming opportunities, and inform best practices. It’s easy to use and will take about 10 minutes to sign-up. There is more information inside the CyberChat Mobilize Community to help you navigate the community space.

# Mobilize CyberChat Community

HOW: Use this link to sign up: https://nc-defense-technology-transition-office.mobilize.io/registrations/groups/45745

1. First, you may create a welcome post in the CyberChat Community. You may upload a picture and share some information about yourself and your company to connect with others. This is a PRIVATE community.

2. Create posts – articles, ask questions, answer questions, etc.

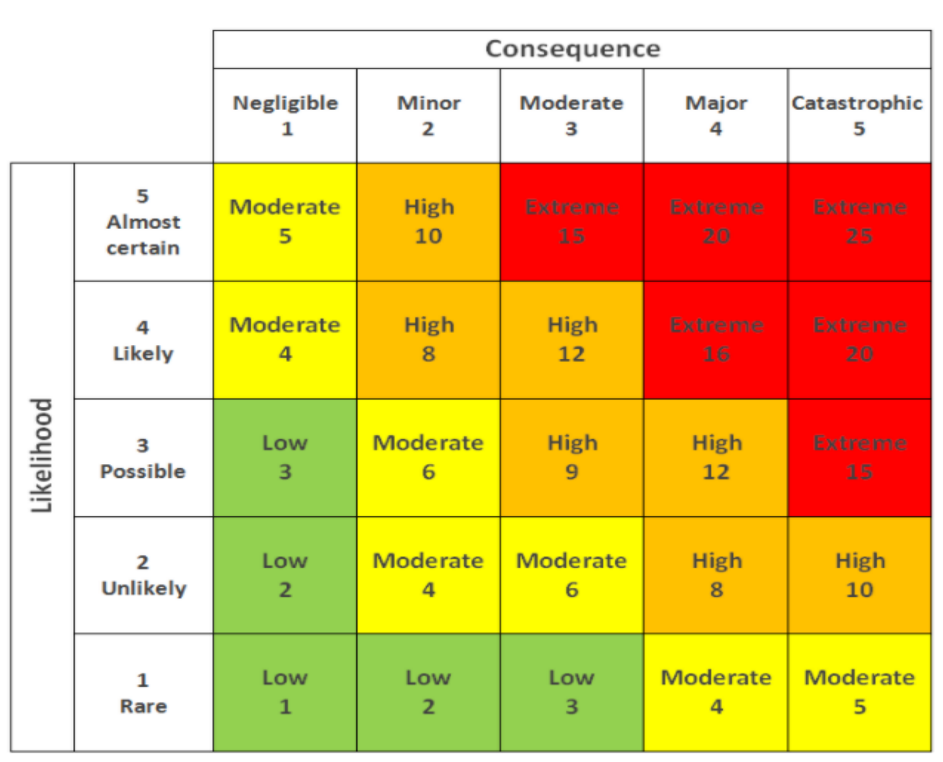
# CMMC/Cyber Updates

The National Defense Industrial Association's second annual study which provides "... an unclassified summary of the health and readiness of the defense industrial base...", shows that the DIB gets a grade of 'C'. Even more concerning is that the grade was given based on pre-COVID data. Industrial Security, one of the  “conditions” considered, gets a grade of 56.

While threats to intellectual property rights decreased, the threats to information security increased. "The decline reflects larger trends in the erosion of industrial cybersecurity despite increasing attention and resources dedicated to combating the threat."

# Cybersecurity Risk Assessment

- Need to define your level of risk by considering the likelihood of an event happening and the severity of the consequences (impact to your business) of the resulting consequences.
- ***Need to put time and money into high probability/high impact issues.***



| | | Consequence | | | | |
|---|---|---|---|---|---|---|
| | | Negligible<br>1 | Minor<br>2 | Moderate<br>3 | Major<br>4 | Catastrophic<br>5 |
| Likelihood | 5<br>Almost certain | Moderate<br>5 | High<br>10 | Extreme<br>15 | Extreme<br>20 | Extreme<br>25 |
| | 4<br>Likely | Moderate<br>4 | High<br>8 | High<br>12 | Extreme<br>16 | Extreme<br>20 |
| | 3<br>Possible | Low<br>3 | Moderate<br>6 | High<br>9 | High<br>12 | Extreme<br>15 |
| | 2<br>Unlikely | Low<br>2 | Moderate<br>4 | Moderate<br>6 | High<br>8 | High<br>10 |
| | 1<br>Rare | Low<br>1 | Low<br>2 | Low<br>3 | Moderate<br>4 | Moderate<br>5 |

# Cybersecurity Risks

**People Risks**

- Ransomware – a form of malware that attempts to encrypt your data then extort a ransom to release an unlock code. Typically delivered via email.
- Phishing – an attempt to gain sensitive information while posing as a trustworthy contact. Typically delivered via email. Spear phishing is a highly targeted attempt to gain information.
- Data leakage via mobile devices – because they are relatively cheap almost everyone has them, making them a target for data thieves.
- Hacking – gaining access to network from outside an organization
- Insider threats – malicious or inadvertent

# Cybersecurity Risks

Mitigation strategies (controls/practices)

- Staff awareness/training
- Malware/virus protection
- Software updates
- Data backups
- Spam filters
- Use encryption software when using portable storage devices
- Network firewalls
- Least privilege access
- Control the use of portable storage devices – such as flash drives
- Strong, complex passwords/phrases

*Policies/procedures (documentation) to back up these controls/practices*

Reducing “scope” is the best way to mitigate many cybersecurity risks.

# Supply Chain Cyber Risk

Requires thorough vetting process of both sides of the supply chain

- Check DUNS
- Review SAM profile
- Check website
- Check references
- Check for negative reviews
- Ask questions
  - What controls are in place to protect the network and data
  - Is the company in working toward compliance with DFARS/CMMC cybersecurity regulations

# Scope

- Understanding audit scope is critical to minimizing costs and reducing the risk of data getting into the wrong hands
- Companies that don’t reduce their scope run the risk of having their entire network and all their employees considered in scope to the audit.
- Large scope = high risk = high costs
- How to determine scope:
  - Use your data-flow diagram to understand how CUI/FCI flows through and/or is stored on your network.
  - Use your network diagram and asset inventory to determine which IT assets are impacted by the flow of data
  - List the employees that have access to the CUI/FCI

# Reducing Scope

- Understand your cybersecurity risks
- Identify the employees that must touch FCI/CUI in order to do their jobs
- Identify the IT assets that are necessary for the flow of FCI/CUI
- Segment the network so that only a portion of it is in scope
  - Examples of mechanisms that can be used for network segmentation – firewalls and routers

Remember – this is not just about passing an audit. The audit is a means to an end, with the end being protecting national security.

# Scoping Tool

- The best scoping guide to use is the Compliance Forge NIST 800-171 & CMMC Scoping Guide for FCI/CUI
    - https://www.complianceforge.com/free-guides/free-nist-800-171-cybersecurity-compliance-scoping-guide.html - download the guide. I will post it on my blog and on Mobilize IO

# Homework – CyberChat #5

1. Develop a strategy to reduce your scope.

**Remember to document your work!**

ncmbc
CONNECTING BUSINESS AND MILITARY

# NORTH CAROLINA MILITARY BUSINESS CENTER CYBERCHAT SERIES – WORKSHOP 4

www.cybernc.us

10 February 2021