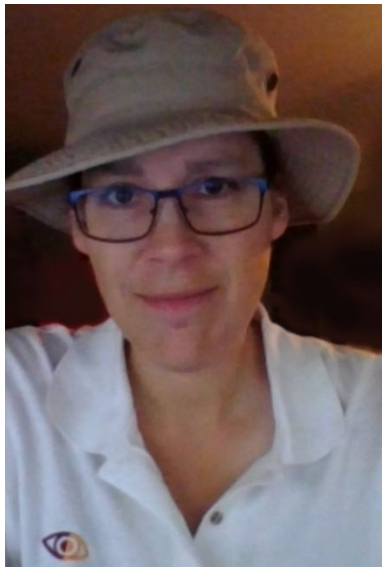
CMMC Update

Current As Of: December 2022

TODAY'S SPEAKERS

Ryan Heidorn

Chief Technology Officer,
C3 Integrated Solutions
Board Director, NDIA New England



Amira Armond

President, Kieri Solutions
Vice Chair, C3PAO Stakeholder Forum

Sponsored by:

Microsoft US Partner Award Winner 2022

SUMMIT7 COMPLIANCE

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- NIST 800-171 Released Jun ‘15 / Updated Aug ‘16: 110 controls
  - Revision 3 draft planned for release in Spring of ’23
  - Expect 110 number to go up
- CMMC announced Jul ’19 to independently assess cyber implementation
  - CMMC 2.0 announced Nov ’21
  - Interim rule expected March 2023
  - 60 days after Interim Rule published, CMMC requirements could appear in DoD solicitations/contracts

Sponsored by:

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Be working on these controls now!**
  - 18-24 months a reasonable, serious timeline; lower costs
  - 7 months a crash program with heavy investment
  - 7 days / 7 weeks un-executable at any cost
- Prioritize!
  - Some controls provide larger impact
  - 100% implementation extremely difficult

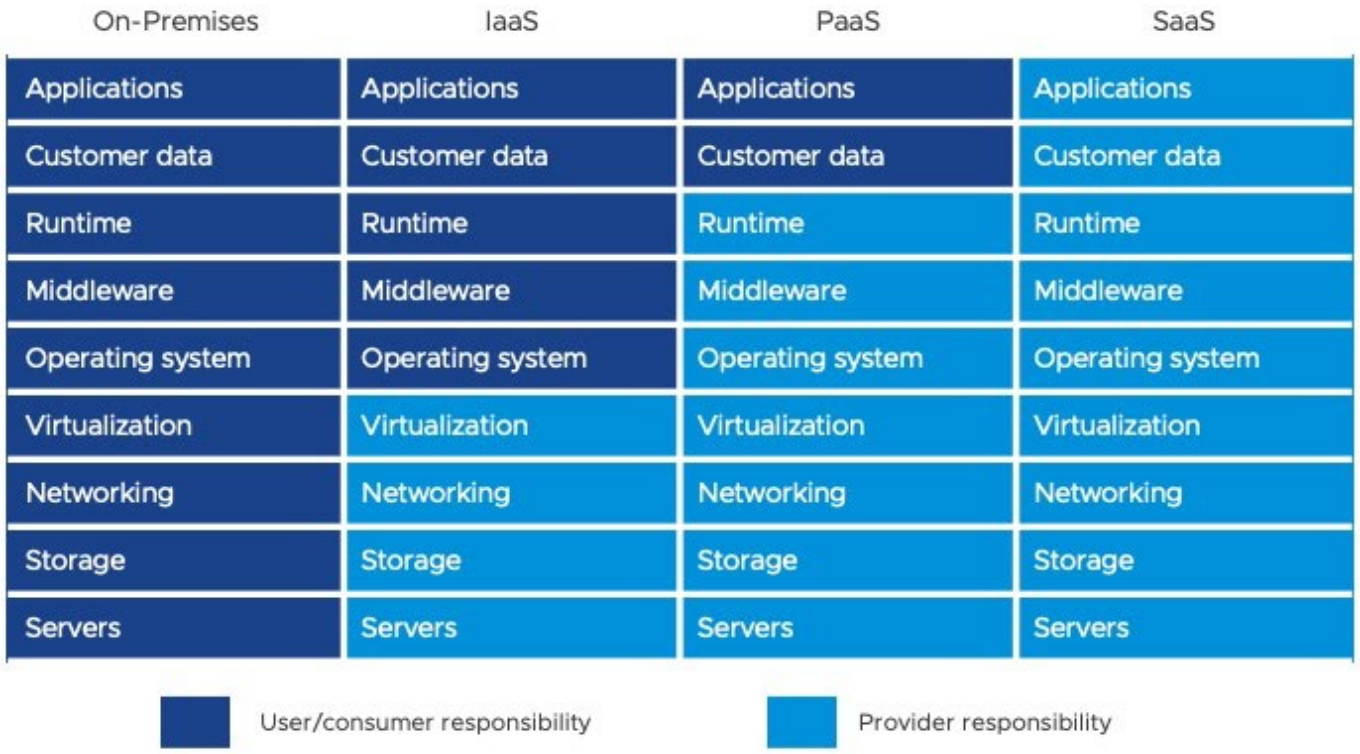
Three Big Questions

- **What are we trying to protect? And why?**
  - We cannot protect information/data if we don't understand why something should be "Controlled"
  - We cannot protect CUI if it is not properly marked
- **From whom are we trying to protect it?**
  - Assume all US persons have access?
  - Is "Need to Know" a component of access?
  - What about friends, partners and Allies?
- **Can NDIA encourage the government to begin by:**
  - Focusing on most critical data/information
  - Providing some guidelines on releasability

What is a Cloud Services Provider (CSP)?

- CSP examples: Microsoft, Amazon Web Services, Google, and cloud-delivered applications (software-as-a-service)

- Definition: “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”
- DFARS 252.239-7010, NIST SP 800-145



Sponsored by:

Compliance Considerations for CSPs

- When used to store, process, or transmit CUI, CSP must implement security requirements equivalent to FedRAMP Moderate baseline per *DFARS 252.204-7012(b)(2)(ii)(D)*
- FedRAMP authorized vs FedRAMP equivalent
- Per DFARS 252.204-7012 CSP must also comply with:
  - Incident reporting
  - Media preservation
  - Damage assessment requirements

Compliance Considerations for CSPs

- **CSP Responsibilities:**
  - Define security controls in Customer Responsibility Matrix (CRM)
  - Prove CSP protecting CUI
    - Verify CSP on FedRAMP marketplace AND DIB Company using FedRAMP offerings
    - https://marketplace.fedramp.gov/
    - If not on marketplace, Assessor will likely need to verify CSP's SSP for FedRAMP controls implementation
- **DIB Company Responsibilities**:
  - Implement security controls defined in CRM
  - Obtain CSP's SSP if CSP not on FedRAMP marketplace

IT/Security Skillsets for CMMC Implementation

- What are the required skills for *implementing* and *maintaining* a compliant IT infrastructure?
- NIST's NICE Framework (SP 800-181), defines roles based on knowledge, skills, and abilities (KSAs)
- Small businesses often outsource these KSAs to external service providers such as an MSP

Role	Training	Salary	Notes
Systems Requirements Planner (Securely Provision)	Minimum 2 years of apprenticeship/hands-on training; systems requirements documentation, computer and system engineering	$88,000–130,000	KSAs may only be required annually, per RMF minimums
System Administrator (Operate and Maintain)	Systems administration, security fundamentals	$60,000-87,000	KSAs may only be required a few days per week
IT Project Manager (Oversee and Govern)	Workplace-provided training, online training, workshops, boot camps for IT project management, leadership, public speaking, network security vulnerability	$85,000-95,000	KSAs will be time-intensive during projects, less so during continuous upkeep and lifecycle management
Cyber Defense Incident Responder (Protect and Defend)	Network security vulnerability, advanced network analysis, basic cyber analysis/operations, network traffic analysis, cyber operator, computer forensics invest and response, information security, information systems, network security, information assurance, troubleshooting, security operations, cryptography	$90,000-137,000	Availability of this role's KSAs must be maintained, however cannot be planned for without historical data regarding incident likelihood

What is a Managed Services Provider (MSP)?

- Outsourced IT and security labor delivered as services
- May manage cloud infrastructure on behalf of an organization
- Most MSPs are unlikely to process, store, or transmit CUI
- Common MSP responsibilities:
  - Configure and manage networks, servers, and cloud infrastructure
  - Manage day-to-day IT needs (system administration, help desk support)
  - Monitor security tools and respond to alerts and incidents

Applicable CMMC Practices for MSP

- People: training, privileged management, account requirements, background screening
- Technology: MSP will be expected to perform internal security for their systems if persistent connections exist to your network (remote management tools, VPNs)
- Facility: only if storing CUI at MSP
- Compliance activities: Change Mgmt., Incident Mgmt., maintenance, vulnerability scanning, etc.
- Assessor will need to evaluate MSP to verify any compliance activities they perform on DIB Company's behalf

How to Select an MSP for CMMC

- Demand a Shared Responsibility Matrix (SRM) designed for use with CMMC
- Ask:
  - Does the MSP maintain remote access connections to your environment?
  - How does the MSP manage changes to your environment?
  - Does the MSP have staff qualified to act as CISO for you?
  - Are all MSP employees U.S. Persons?
  - What clouds and subcontractors does the MSP use to support you?
  - Has the MSP implemented NIST SP 800-171 for its internal systems?

Additional Resources for Vetting MSPs

- MSP Shopping Guide
  - https://ndisac.org/wp-content/uploads/2022/12/NDISAC-SMB-WG-MSP-Shopping-Questionnaire-Rev-4.5.pdf
  - ND-ISAC, SMB Working Group
- MSPs and CMMC Compliance
  - https://www.cmmcaudit.org/msps-and-cmmc-compliance/
- MSP Maturity Check: 21 Questions to Ask Your MSP
  - https://steelroot.us/resource/msp-cybersecurity-check/

Sponsored by:

NDIA Concerns Associated with cloud/MSP

- Conflation of CSPs/MSPs in the draft CMMC Assessment Process (CAP)
- Necessity of practice inheritance in the assessment process
- Interpretation of some CMMC practices in cloud-native architectures
- No process to assess CMMC compliance for CSPs/MSPs prior to client DIB Company assessments
- NDIA submitted comments on the Cyber AB's draft CAP in August

NDIA Recommendations

- **Current plan as NDIA understands it will result in significant failure rates across the DIB (and government)**
- **3 Recommendations**

1. **DoD CIO include industry in their assessment plan**
   - Without correction, 1st year assessments could carry 75%+ failure rate
   - Likely to drive industry opt outs, anger & additional congressional oversight
2. **Assess MSPs as part of a cohesive strategy**
   - Verify providers meet standards on behalf of their clients
3. **Adjust implementation plan – Move away from cliff implementation**
   - Max 10% / 11 controls auto-fails
   - 80% of 110 controls = PASS
   - Consider further adjustments for small business

Secure Your Networks and Systems In Physical Space and Cyberspace

NDIA

- **Be working on these controls now!**
  - 18-24 months a reasonable, serious timeline; lower costs
  - 7 months a crash program with heavy investment
  - 7 days / 7 weeks un-executable at any cost
- Prioritize!
  - Some controls provide larger impact
  - 100% implementation extremely difficult

Sponsored by:

Microsoft US Partner Award Winner 2022

SUMMIT7 COMPLIANCE

Questions?

Sponsored by: