CMMC Lessons Learned

"When new frameworks and regulations meet the small business Defense Industrial Base"

Hosted by

Kelly C. Kendall, MBA, PMP, CMMC-RP
CEO and President
KNC Strategic Services

KNC STRATEGIC SERVICES

CMMC Lessons Learned

Agenda

- Welcome
- Introductions
- Roundtable Presentations
  - Chris Newborn, DAU
  - Adam Austin, Totem Tech
  - Katie Stewart, CERT
- Q&A

KNC STRATEGIC SERVICES

Company Overview

Kelly C. Kendall, MBA
CEO and President
Disabled Veteran (US Marine Corps)

Chuck Buresh
EVP and COO

- ★ Formed 2018
- ★ CVE Verified SDVOSB/VOSB
- ★ Founded by Two Disabled Veterans, and one Veterans/ Military Advocate
- ★ Extensive Experience
- ★ An approved C3PAO

KNC STRATEGIC SERVICES

Roundtable Presentations

- Chris Newborn, DAU
  - Cybersecurity Professor
- Adam Austin, Totem Tech
  - Cyber guy
- Katie Stewart, CERT Division of SEI
  - Technical Manager, Cyber Assurance

Contractor Compliance - DFARS 7012 (Jan 2018 – Nov 2020)

- **By signing the contract, the contractor agrees to comply with the terms of the contract and all requirements of the DFARS Clause 252.204-7012**
- **Contractors are responsibility to determine whether they have implemented NIST SP 800-171 as well as any other security measures necessary to provide adequate security for Controlled Unclassified Information (CUI)**
  - The scope of DFARS Clause 252.205-7012 does not require DoD to 'certify' that a contractor is compliant with the NIST SP 800-171 security requirements
  - The scope of DFARS Clause 252.205-7012 does not require the contractor to obtain third party assessments or certifications of compliance
  - DoD does not recognize third party assessments/certifications of compliance

DFARS Case 2019-D041 - Interim Rule (DFARS Provision 252.204-7019)

- **Effective 30 Nov 2020,** DoD contractors are required to implement NIST SP 800-171 IAW DFARS clause 252.204-7012 and required at time of award to have at least a Basic NIST SP 800-171 DoD Assessment that is current (i.e. not more than three (3) years old unless a lesser time is specified in the solicitation) posted in the Supplier Performance Risk System (SPRS).
- **As of 1 Dec 2020**, DoD contracting officers are required to verify that the summary level score of a current NIST SP 800-171 Assessment for each covered contractor information system that is relevant to an offer, contract, task order or delivery order is posted in SPRS prior to:
  - **Awarding a contract, task order, or delivery order to an offeror or contractor that is required to implement NIST SP 800-171 in accordance with the clause at DFARS 252.204-7012; or**
  - **Exercising an option period or extending the period of performance on a contract, task order, or delivery order with a contractor that is required to implement the NIST SP 800-171 in accordance with the clause at DFARS 252.204-7012.**

DFARS Case 2019-D041 - Interim Rule (DFARS clause 252.204-7020)

- Requires a contractor to provide the Government with access to its facilities, systems, and personnel when it is necessary for DoD to conduct or renew a higher-level Assessment.
- Also requires the contractor to ensure that applicable subcontractors also have the results of a current Assessment posted in SPRS prior to awarding a subcontract or other contractual instruments.
- Provides additional information on how a subcontractor can conduct and submit an Assessment when one is not posted in SPRS.
- Requires the contractor to include the requirements of the clause in all applicable subcontracts or other contractual instruments.

DFARS Case 2019-D041 - Interim Rule (DFARS clause 252.204-7021)

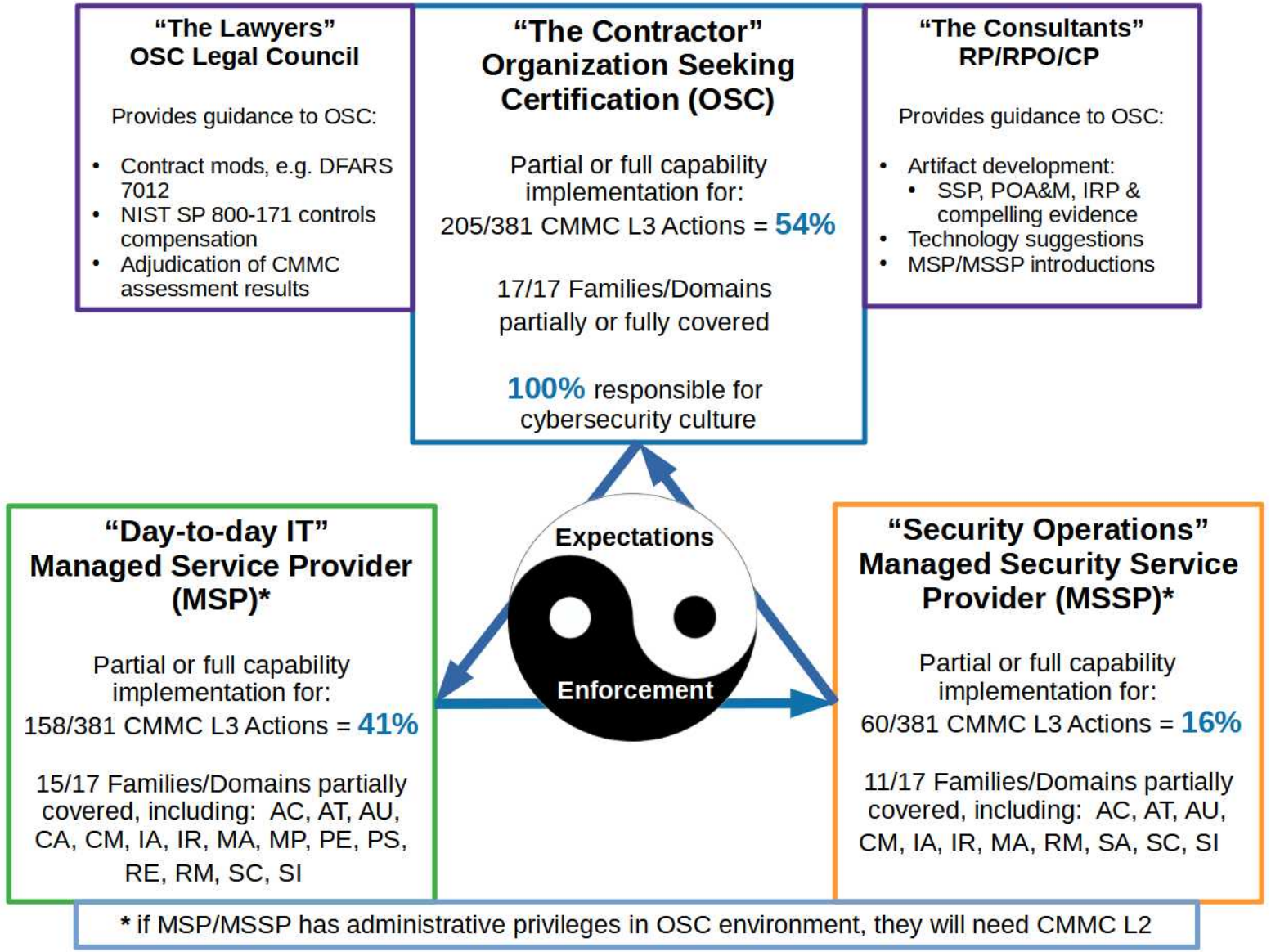
CMMC is a 5-year phased roll-out - contract award effective 1 Oct 2025

- Before 1 Oct 2025, all new acquisitions must be approved by OUSD (A&S)
- Contractor certification level must be maintained for contract duration
- Clause must be flowed down; primes must ensure subs are certified at required CMMC level prior to awarding subcontract

DFARS Implementation: 7012 Versus 7021

	7012	7021
Information Type:	CUI	FCI & CUI
Reference:	NIST SP 800-171	CMMC v2.01
Compliancy:	110 Security Requirements	5 Levels of Practices & Processes
Deliverable:	SSP & POA plus Artifacts	SSP plus Artifacts
Validation:	3-Levels of Assessments (basic, medium, high) using NIST SP 800-171 v1.2, DAM Tool	C3PAOs, Assessors
Governance:	7019, 7020	FAR 52.204-201 & DFARS 252.204-7012

Team approach to compliance



Delta 20's

Practice	Description
AM.3.036	Define procedures for the handling of CUI data.
AU.2.044	Review audit logs.
AU.3.048	Collect audit information (e.g., logs) into one or more central repositories.
CA.3.162	Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally-defined as an area of risk.
IR.2.093	Detect and report events.
IR.2.094	Analyze and triage events to support event resolution and incident declaration
IR.2.096	Develop and implement responses to declared incidents according to pre defined procedures.
IR.2.097	Perform root cause analysis on incidents to determine underlying causes.
RE.2.137	Regularly perform and test data back-ups.
RE.3.139	Regularly perform complete, comprehensive and resilient data backups as organizationally-defined.
RM.3.144	Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources and risk measurement criteria.
RM.3.146	Develop and implement risk mitigation plans.
RM.3.147	Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.
SA.3.169	Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.
SC.2.179	Use encrypted sessions for the management of network devices.
SC.3.192	Implement Domain Name System (DNS) filtering services.
SC.3.193	Implement a policy restricting the publication of CUI on externally owned, publicly-accessible websites (e.g., forums, LinkedIn, Facebook, Twitter, etc.).
SI.3.218	Employ spam protection mechanisms at information system access entry and exit points.
SI.3.219	Implement email forgery protections
SI.3.220	Utilize email sandboxing to detect or block potentially malicious email.

KNC STRATEGIC SERVICES

Q & A

KNC STRATEGIC SERVICES

Thank You

KNC Strategic Services

4416 Maple Drive

Oceanside, CA 92056

Toll-Free 833-562-7700

KNCSS.com

Duns 081030113 / Cage 825L7