Cyber Security Compliance in Government Contracting

Presented by Leonard Bean,
Norcal PTAC Procurement Specialist

The Procurement Technical Assistance Center (PTAC) is funded in part through a cooperative agreement with the Defense Logistics Agency.
Your Hosts

Kristina Kunkel
Program Director
Norcal PTAC

Lenny Bean
Procurement Specialist
Norcal PTAC
Who We Are

✓ Nonprofit organization

✓ Help businesses compete & succeed in the government marketplace

✓ All services are no cost - funded by federal, state and local grants and contracts

✓ Hosted by Humboldt State University SPF

✓ In Fiscal Year 2018, Norcal PTAC clients won more than $166 million in government contract awards
Our Service Area
Our Services

All of our services are provided at no-cost to you!

One-on-one counseling

Workshops and seminars

Bid-matching services
Apply for our Services

1. Visit our website at www.norcalptac.org

2. Click on APPLY NOW

3. Fill out the evaluation form

4. We will contact you within two business days

**If you are an existing Norcal SBDC client, send an email to info@norcalptac.org to request your application.**

Out of Norcal PTAC's service area? Find your SBDC or Find your PTAC
Disclosure
The information provided herein is accurate to the best of my ability at the time of this presentation. Some or all of the provisions mentioned herein could or may be changed by the current administration, with or without prior notice.
Today’s Objectives

► Cyber Security Threats for Business
► Regulations to Combat Cyber Threats
► Federal Contracting Requirements
► Cyber Compliance
► Cyber Certifications
Cyber Threats

► Cybercrime is one of the biggest threats businesses of all sizes face.

► More than 75 percent of data breaches target small and medium-sized business.

► Sixty percent of small businesses affected by cybercrime will close within six months of the breach.
Regulatory Overview

► Executive Order 13556 – Controlled Unclassified Information
  ▪ Signed by President Obama
  ▪ November 4, 2010

► National Archives and Records Administration

► Executive Agent
Regulatory Overview

► National Institute of Standards and Technology (NIST)

- Various NIST documents have provided guidance aimed at standardizing cybersecurity
- NIST Special Publication 800-171R1 addresses Controlled Unclassified Information residing with contractors utilizing standards from NIST 800-53
- NIST Special Publication 800-53 provide best practices in 14 distinct areas (called families) of information security including access control, incident response, physical protection, and risk assessment.
Regulatory Overview

► NIST is a Non regulatory agency of the government “neutral source of technical expertise”
► NIST standards are merely guidance. However they have been often utilized in regulations.
► DFARS 204.73 and clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
Safeguarding Covered Defense Information and Cyber Incident Reporting - DFARS Subpart 204.73

► DoD contractors (including small businesses) must:

► Provide adequate security to safeguard covered defense information that resides in or transits through their internal unclassified information systems from unauthorized access and disclosure; and
Safeguarding Covered Defense Information and Cyber Incident Reporting - DFARS Subpart 204.73

► Rapidly report cyber incidents (within 72 hours) and cooperate with DoD to respond to these security incidents, including access to affected media and submitting malicious software.

► Federal contracting officers are required to provide in each work statement or specification the identification of any covered defense Information.
Requirements

► There are 14 Security Requirements bases to be in compliant with 800-171

► Each area has specific security controls for a total of 110

► Basic Requirements are from FIPS 200
  https://www.norcalptac.org/sites/default/files/Cyber_Requirements_Worksheet_PTAC.xlsx

► Derived Requirements from 800-53
  ▪ Total of 110

► Note: The clause is not required to be applied retroactively, but that does not preclude a CO from modifying an existing contract to add the clause.
Requirements

NIST 800-171 Security Families

► AC - Access Control (3.1) 22
► AT - Awareness & Training (3.2) 3
► AU - Audit & Accountability (3.3) 9
► CM - Configuration Management (3.4) 9
► IA - Identification & Authentication (3.5) 11
► IR - Incident Response (3.6) 3
► MA - Maintenance (3.7) 6
► MP - Media Protection (3.8) 9
► PS - Personnel Security (3.9) 2
► PE - Physical Protection (3.10) 6
► RA - Risk Assessment (3.11) 3
► CA - Security Assessment (3.12) 3/4
► SC - System & Communications Protection (3.13) 16
► SI - System & Information Integrity (3.14) 7
► TOTAL REQUIREMENTS: 109/110
Prime and Subcontractor Requirements

Subcontractors

► These requirements are to flow down to all subcontractors

▪ No matter what level they are in the supply chain

Deadlines

► These requirements need to be met by 12/31/2017

► This applies to both Primes and Subcontractors
Compliance

➢ To be in compliance with these requirements:
   ▪ Need to review your systems
   ▪ Have written policies/plans in place that address the 14 families (that apply to your business)
     • System Security Plan
       – Passwords at least 12 characters long
       – Train your employees
     • Incident Response Plan
       – Train your employees
     • Plan of Action/Mediation
       – Train your employees
Non-Compliance

► Could be Debarred as a company
► Individuals could be debarred
► Could lose government contract work
► Primes may not accept you as a competent / responsive vendor
► Competition will seek you out
Certification-Today

► The rule does not require “certification” of any kind, either by DoD or Federal contractors. Nor will DoD give any credence to 3rd party assessments or certification.

► By the contractor signing the contract they agree to comply with the terms of the contract.

► It is up to the contractor to determine that their systems meet the requirement.
CMMC is the Cybersecurity Maturity Model Certification-DOD

► Combines various cybersecurity standards and “best practices”
► Maps these practices and processes across several maturity levels that range from basic cyber hygiene to advanced
► For a given CMMC level, the associated practices and processes, when implemented, will reduce risk against a specific set of cyber threats.
► The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements.
► The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels
► The intent is for certified independent 3rd party organizations to conduct audits and inform risk
CMMC Next Steps

► CMMC Vision
  ▪ Be a unified cybersecurity standard for DOD acquisitions to reduce exfiltration of
  ▪ Controlled Unclassified Information (CUI) from the Defense Industrial Base (DIB)

► CMMC Schedule
  ▪ CMMC Rev 1.0 will be released in January 2020
  ▪ Will be included in RFIs starting in June 2020
  ▪ Will be included in RFPs starting in Fall 2020
CMMC Next Steps

► Multiple Opportunities for Stakeholder Feedback


Public comment of draft CMMC Rev 0.4 in September 2019

Public comment of draft CMMC Rev 0.6 in November 2019
Summary

► Cyber Security is real
► Non-Compliance could lead to debarment
► These clauses are required to be flow down to all levels of subcontractors doing business with the Federal Government
► If there is a breach in your system you have 72 hours to notify the appropriate sources
► Train your employees
Resources Available

► NIST SP 800-171

► Procurement Technical Assistance Program (PTAC)

  • Cybersecurity Requirements Worksheet:
    [https://www.norcalptac.org/sites/default/files/Cyber_Requirements_Worksheet_PTAC.xlsx](https://www.norcalptac.org/sites/default/files/Cyber_Requirements_Worksheet_PTAC.xlsx)
Questions?

707.826.3916
info@norcalptac.org