
# Improving Cybersecurity and Resilience Through Acquisition

# About SoundWay

- ✓ Cyber AB Authorized C3PAO
  - One of only 48 C3PAOs Nationwide
- ✓ Expert Cybersecurity Professionals
  - CMMC Certified Assessor (CCA)
  - CMMC Certified Professional (CCP)
  - Industry Certifications:
    - CISSP • Security+ • PMP
- ✓ TOP SECRET Facility Clearance
- ✓ HUBZone, SDVOSB, WOSB
- ✓ FAR & DFARS Compliant or over 12 years

**SOUNDWAY CONSULTING INCORPORATED *("SOUNDWAY")*** was founded by Diane Bellegarde, a U.S. Army Service-Disabled Veteran, in 2011.

SoundWay provides information technology, mission support & cybersecurity professional services to the U.S. Department of Defense **(DoD)**, Intelligence Community **(IC)**, federal government civil agencies, and commercial businesses.

SoundWay's commercial business is focused on providing cybersecurity compliance, CMMC certification readiness, & as a C3PAO we are authorized to conduct CMMC certification Assessments.

Since 2018, SoundWay has worked tirelessly to become a leader in cybersecurity; dedicated to demystifying & simplifying Government compliance mandates & making compliance affordable for its fellow contractor community.

SoundWay

# *Improving Cybersecurity and Resilience through Acquisition*

**Final Report of the**
**Department of Defense and**
**General Services Administration**



**November 2013**

II. ***Address Cybersecurity in Relevant Training.***
As with any change to practice or policy, there is a concurrent need to train the relevant workforces to adapt to the changes. Incorporate acquisition cybersecurity into required training curricula for appropriate workforces. Require organizations that do business with the government to receive training about the acquisition cybersecurity requirements of the organization's government contracts.

III. ***Develop Common Cybersecurity Definitions for Federal Acquisitions.***
Unclear and inconsistently defined terms lead, at best, to suboptimal outcomes for both efficiency and cybersecurity. Increasing the clarity of key cybersecurity terms in Federal acquisitions will increase efficiency and effectiveness for both the government and the private sector. Key terms should be defined in the Federal Acquisition Regulation.

IV. ***Institute a Federal Acquisition Cyber Risk Management Strategy.***
From a government-wide cybersecurity perspective, identify a hierarchy of cyber risk criticality for acquisitions. To maximize consistency in application of procurement rules, develop and use "overlays"[10] for similar types of acquisition, starting with the types of

*A Security Life Cycle Approach*, NIST Special Publication 800-37, Revision 1 (Feb. 2010), and *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Revision 4, (Apr. 2013).

[10] An overlay is a fully specified set of security requirements and supplemental guidance that provide the ability to appropriately tailor security requirements for specific technologies or product groups, circumstances and conditions, and/or operational environments.



acquisitions that present the greatest cyber risk.

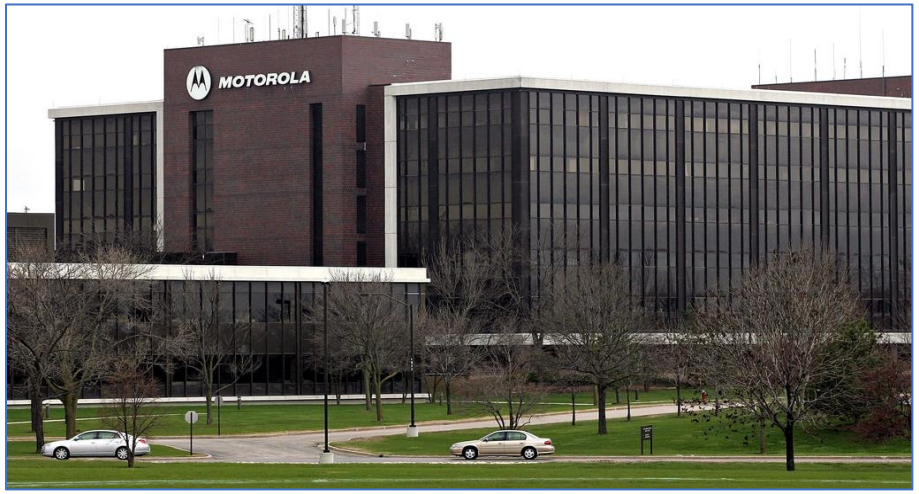
V. ***Include a Requirement to Purchase from Original Equipment Manufacturers, Their Authorized Resellers, or Other "Trusted" Sources, Whenever Available, in Appropriate Acquisitions.***
In certain circumstances, the risk of receiving inauthentic or otherwise nonconforming items is best mitigated by obtaining required items only from original equipment manufactuers, their authorized resellers, or other trusted sources. The cyber risk threshold for application of this limitation of sources should be consistent across the Federal government.

VI. ***Increase Government Accountability for Cyber Risk Management.***
Identify and modify government acquisition practices that contribute to cyber risk. Integrate security standards into acquisition planning and contract administration. Incorporate cyber risk into enterprise risk management and ensure key decision makers are accountable for managing risks of cybersecurity shortfalls in a fielded solution.

# Setting the Stage

The year: 2008

The location: Schaumburg, IL




The audience:

- 2-Star General
- 3 Procurement Specialists
- 15 Motorolans

# "2018 DISA Systems Engineering Tech & Innovation (SETI) Contract HC10147-17-R-001"

$7.5B IDIQ for IT/cyber related matters with 38 awardees

**Questions:**

- *Who reviewed and w*
  *review?*
- *What training did th*
  *Contracting Officer c*


Section L - Instructions, Conditions and Notices to Bidders (*nothing about Cyber*)



- Mitigation and Response: provide the process on how the threat will be mitigated and responded to upon discovery.
- Lessons Learned and Action Plan: provide lessons learned and an action plan that will help all interested parties avoid repeated and similar attacks.
- Subcontractors: explain how your subcontractors will be required to implement this requirement within

f the plan, the contractor shall submit verification to the PCO and COR

t Plan is addresses at the Base Contract level. However, should a task e required, it will be identified in the PWS for the task order.

UIPMENT
nployed for remote access to a Government network must meet or exceed ent (GFE) cyber security computing requirements. The contractor shall e) employed to access these environments meet the following minimum nd provide periodic certification of compliance as a pre-requisite to being

is prohibited;
ns must be configured for compliance with the applicable Security (STIGs);
-spyware software must be installed and signatures must be configured to asis;
must be utilized and configured to permit traffic by exception only, ost-level firewall provides intrusion detection or prevention, the signatures or rules must be updated at the same intervals as the anti-virus software;

(5) Computers must be Information Assurance Vulnerability Management (IAVM) compliant;
(6) Computers must be scanned with the currently approved DoD scanner solution at a minimum of every 30 days. All vulnerabilities must be remediated and reported to the cognizant Information Assurance Manager;
(7) Contractor employees must possess a current Government issued Common Access Card (CAC) and install Government certified CAC readers; and
(8) Verification of compliance with these requirements must be provided to an appointed government representative on a monthly basis.

# SBIR – Software Solution for the USAF

## 2020 Award issued with following conditions

1) Must demonstrate compliance with CMMC Level 1 (CMMC 1.0)
2) Conformance with 252.204-7012
3) Allowance of $10K budget towards cyber implementation for CMMC L1
4) TPOC convinced an ATO was not required as they were in GovCloud

Results:
- Delays
- > $20K in non-reimbursable costs to GovCon to conform with L1
- ATO determined to be required (testing done by USG at no charge) to GovCon

# Historical Progress

2013 – DoD & GSA Approve Final Report "*Improving Cybersecurity and Resilience through Acquisition*"

2017 – NIST SP:800-171r1

2019 – CMMC 1.0

2020 – NIST SP:800-171r2

2021 – CMMC 2.0

2023 – NIST SP:800-171r3 (Draft)

- Unintentional Release of CMMC 2.1 documentation

DFARs 252.204-7012

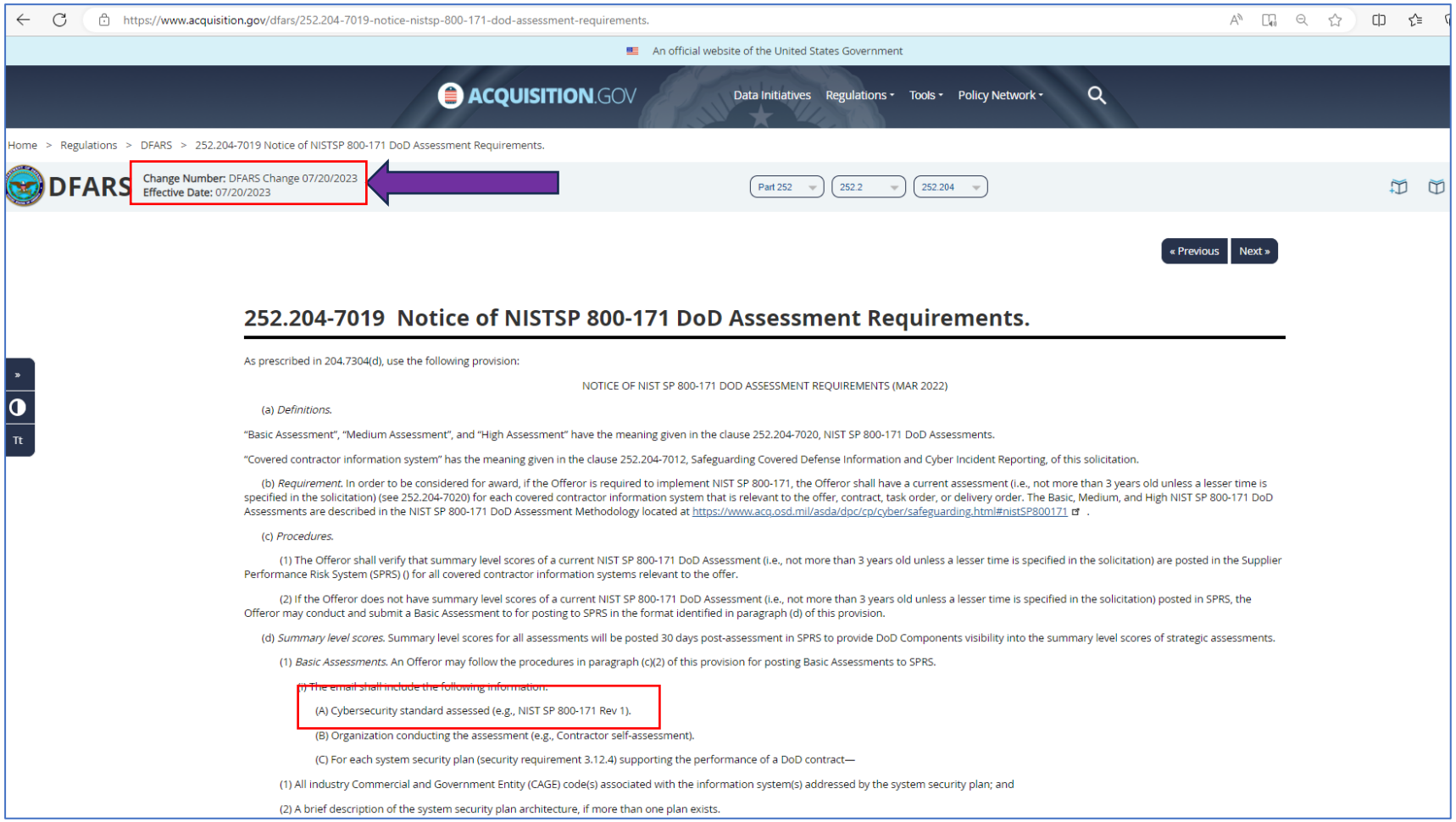
DFARs 252.204-7019

DFARs 252.204-7020

DFARs 252.204-7021

# Challenges

## Devils in the details



SoundWay

# Impact of the Threat on the Acquisition System

**Cost**
**Schedule**
**Performance**

# Likely Increases in Protests

- Issues with “Self-Deleting Clauses”

  DFARs 252.204-7012 (AND) CMMC Level 1 is in solicitation/contract

- Misrepresentation within SPRS

  DIBCAC and C3PAO community both agree

- Challenging CMMC L2 Obligations when no CUI is applicable in the actual performance of work

  FOIAs, disclosures by subcontractors, etc.

# By The Numbers - 2020

| Organization | Number of Active Contracts | New Opportunities |
|---|---|---|
| AIR FORCE | 183,050 | 1,387 |
| ARMY | 465,469 | 2,194 |
| DOD | 642,895 | 1,286 |
| NAVY | 341,755 | 1,618 |
| MARINES | 31,409 | 194 |
| Veterans Affairs | 103,527 | 1,255 |
| Totals | 1,768,105 | 7,934 |

USG Reports that .003% of all contracts contend with a protest = 5,328

~ Rand & GAO 2021

# Fun Fact

For every 2,000 protests

$81.1M

# Considerations for Improving

- Ensure KO's, COTRs and PM's understand FY 25 can/should be  a new way of doing business.
- Build more time into the acquisition process to alleviate the "cut/paste" mentality.
- Evaluate in-depth training beyond video instruction available via DAU.
- Rubrics for "Spot Inspections" of SPRS scores
- Conduct analyses of more recent breaches of GovCon – how do ancillary fees and penalties impact Cost, Schedule and Performance?

# Questions

Carter Schoenberg, CISSP | QTE | CCP

Vice President & Chief Cybersecurity Officer

c.Schoenberg@soundwayconsulting.us

www.soundwayconsulting.com