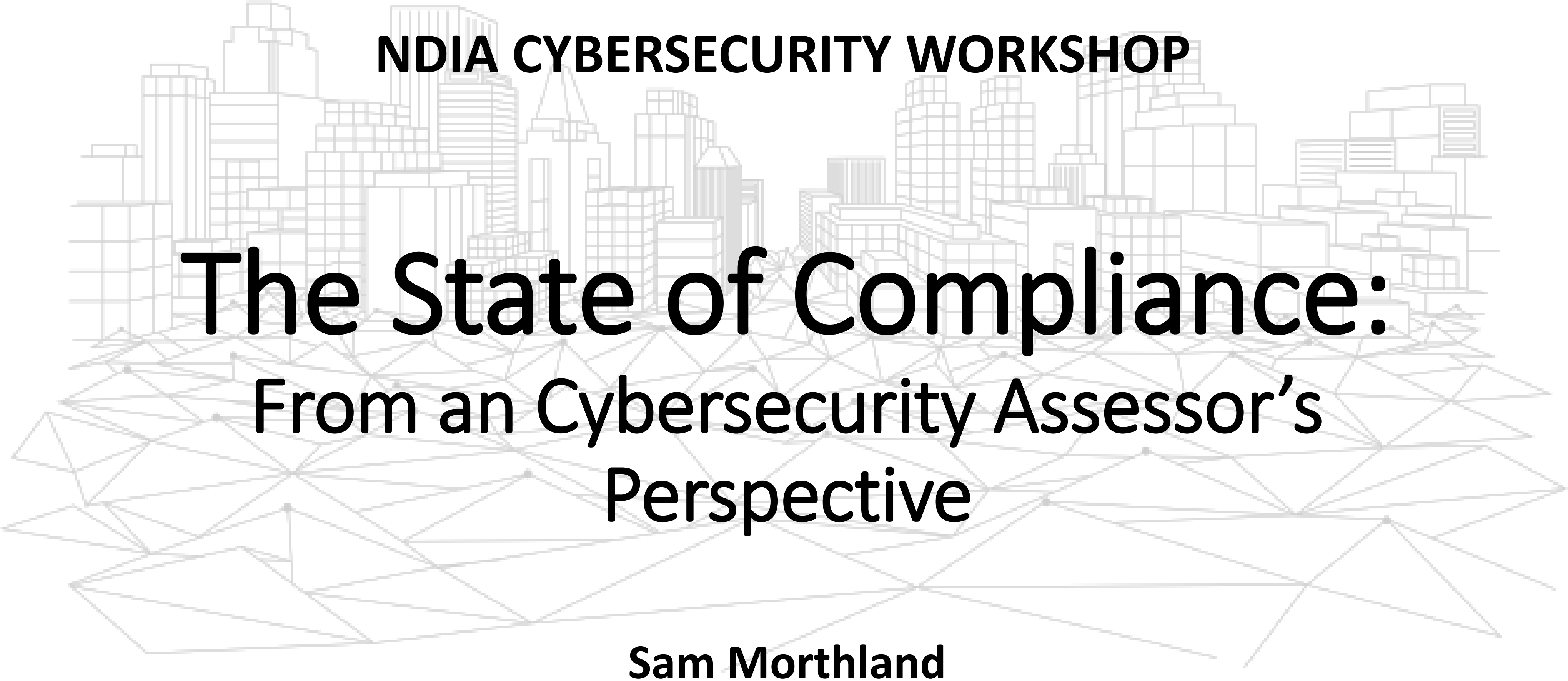
NDIA CYBERSECURITY WORKSHOP



The State of Compliance:

From an Cybersecurity Assessor's Perspective

Sam Morthland

November 13, 2019

Overview

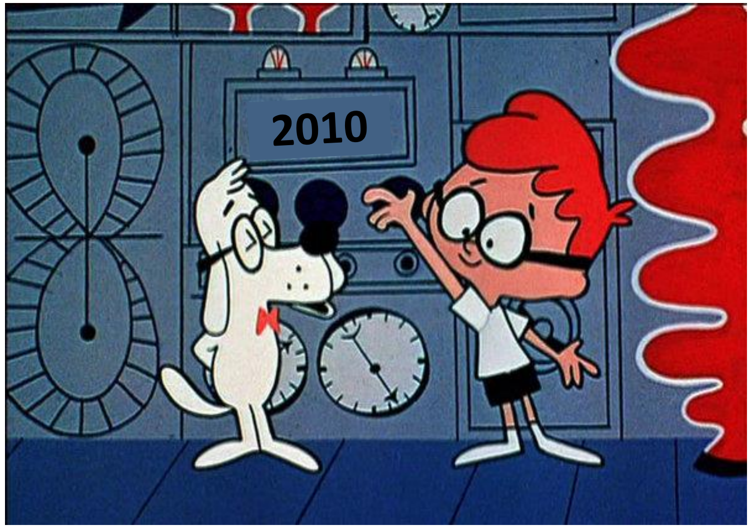
- Background
- *Reality Check* Report
- Changes in Guidance/Regulations
- Anticipating CMMC
- Recommendations for Businesses

A bit about us…

- Veteran Owned Small Business, established in 2011, previous DOD cybersecurity and intelligence members
- Payment Card Industry (PCI) - Qualified Security Assessor (QSA)
  - 1 of 147 US-based Assessors
- Federal Risk and Authorization Management Program (FedRAMP) accredited Third Party Assessment Organizations (3PAO)
  - Accredited by American Association for Laboratory Accreditation (A2LA) to ISO/IEC 17020:2012, Requirements for bodies performing inspection
  - 1 of 38 Federally approved FedRamp 3PAOs
- 8 years of serving the financial, commercial and Federal markets

Let’s Jump into the Wayback Machine…

- CUI Security - Executive Order 13556 – Nov 2010
- DFARS 252.204-7012 (Final Rule Nov 2013)
  - Comply with subset of NIST 800-53
- OPM Data Breach – Gov’t wake up call – Jun 2015
- DFARS 252.204-7012 (Interim Rule Dec 2015)
  - Initially 3 years to full compliance with NIST 800-171
- DFARS 252.204-7012 (Final Rule Oct 2016)
  - All DOD contractors to be compliant to NIST 800-171
    - As soon as practical - **NLT 31 Dec 2017**
  - Self Attestation of compliance - Required documents: SSP and POAM
- US Navy Sea Dragon Breach – Jul 2018
- MITRE’s “Deliver Uncompromised” - Aug 2018
- Geurts Memo– Sep 2018
  - Imposing enhanced security controls on “critical” Navy programs



The State of Compliance

Reality Check Report

- Early 2019 - Lot of discussion of changes coming
  - Standards, Policies, Compliance Monitoring/Audits
  - “TO BE” objectives
- Didn’t see where the “AS IS” information was provided
- Developed report based on incident responses and assessments over last 2 years
  - Provided an assessor’s view of compliance in the DIB
- Provided a snapshot of compliance and identified areas for DIB companies to focus efforts and resources

Reality check: Defense industry’s implementation of NIST SP 800-171

Keen insights from certified cybersecurity assessors.

May 2019

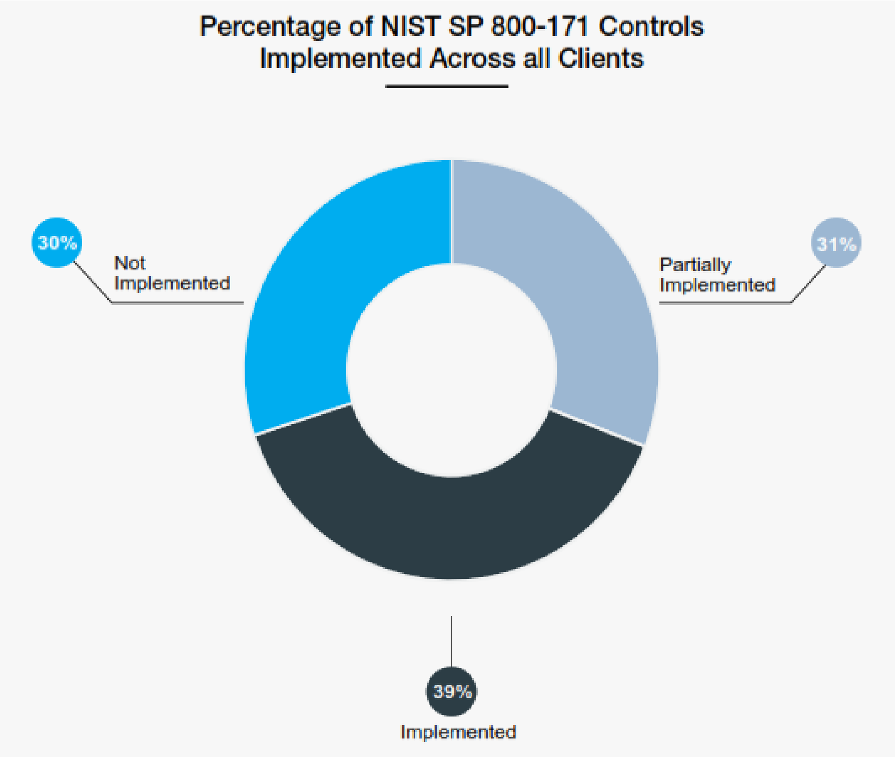
SERABRYNN

GLOBAL LEADER IN CYBERSECURITY COMPLIANCE

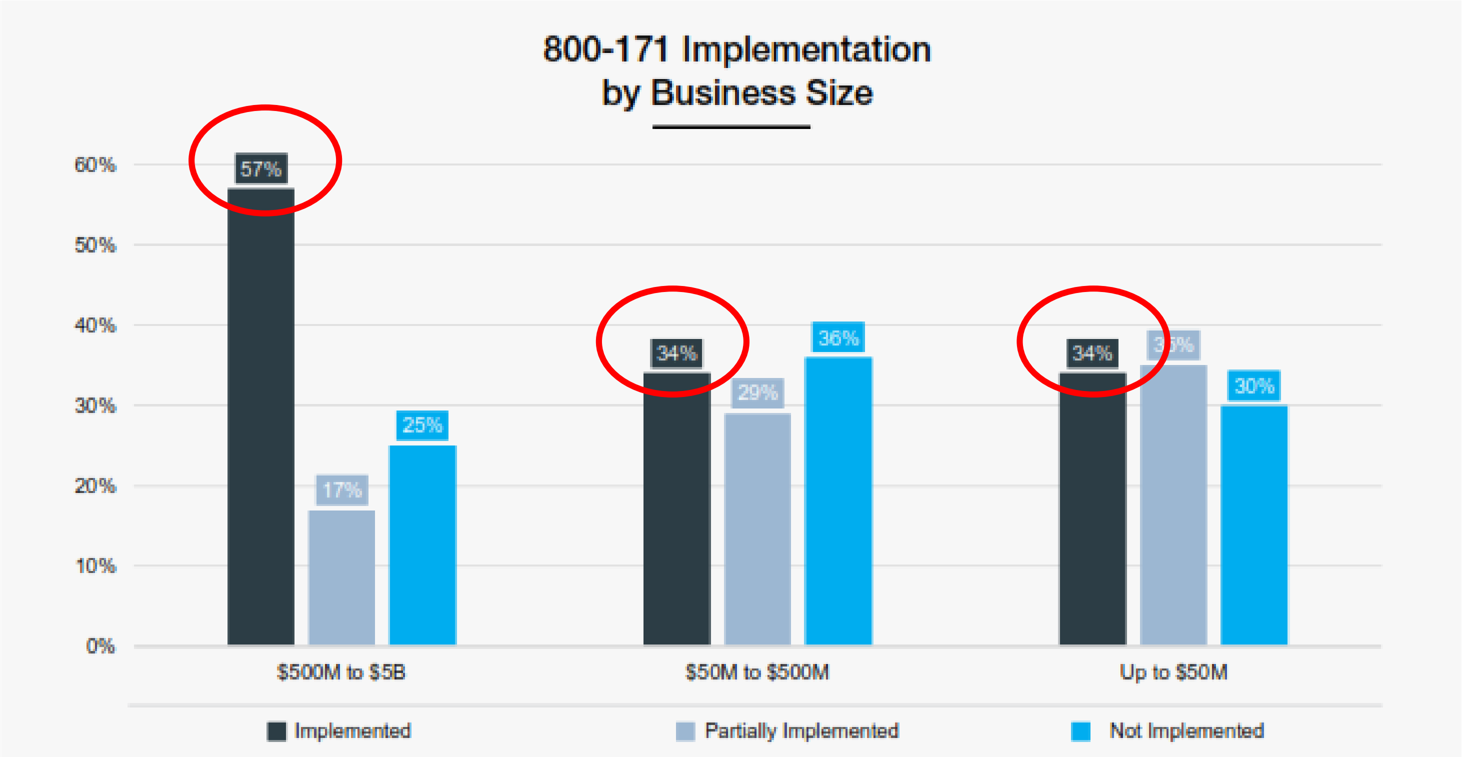
The State of Compliance

NO COMPANIES WERE 100% COMPLIANT

Large Business Leading, Small Business Lagging



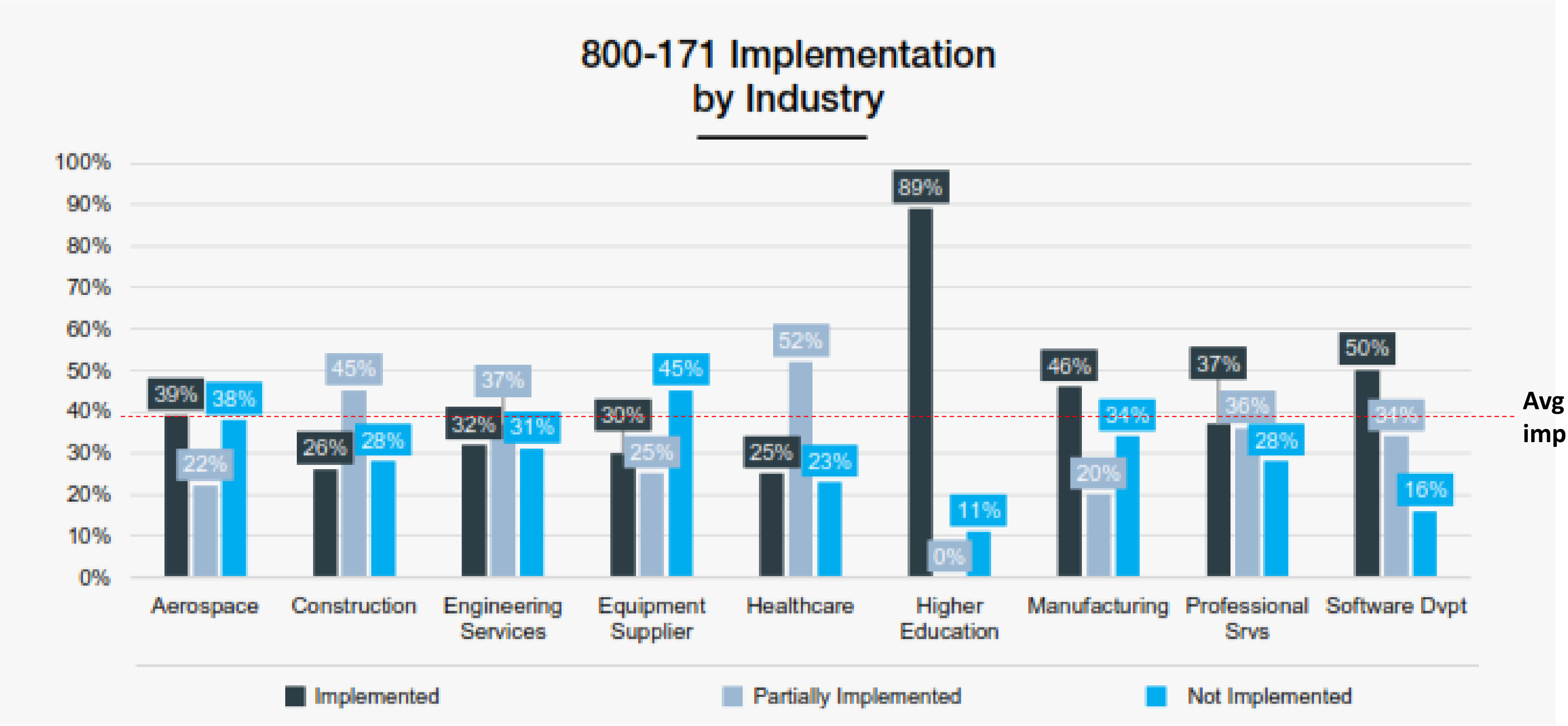
Percentage of NIST SP 800-171 Controls Implemented Across all Clients



800-171 Implementation by Business Size

The State of Compliance

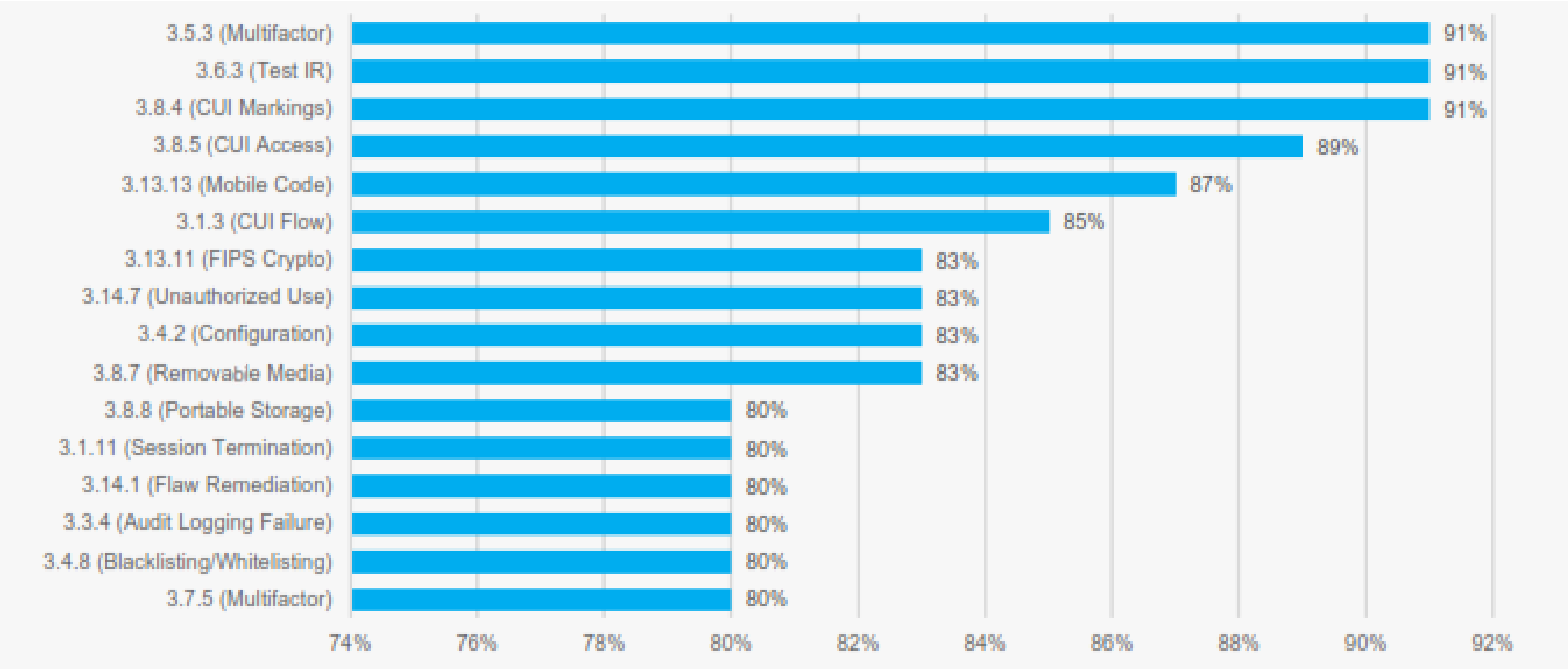
Higher Ed beats DIB Implementation



Avg of only 39% of controls implemented by DIB

The State of Compliance

80% of companies failed to implement 16 controls

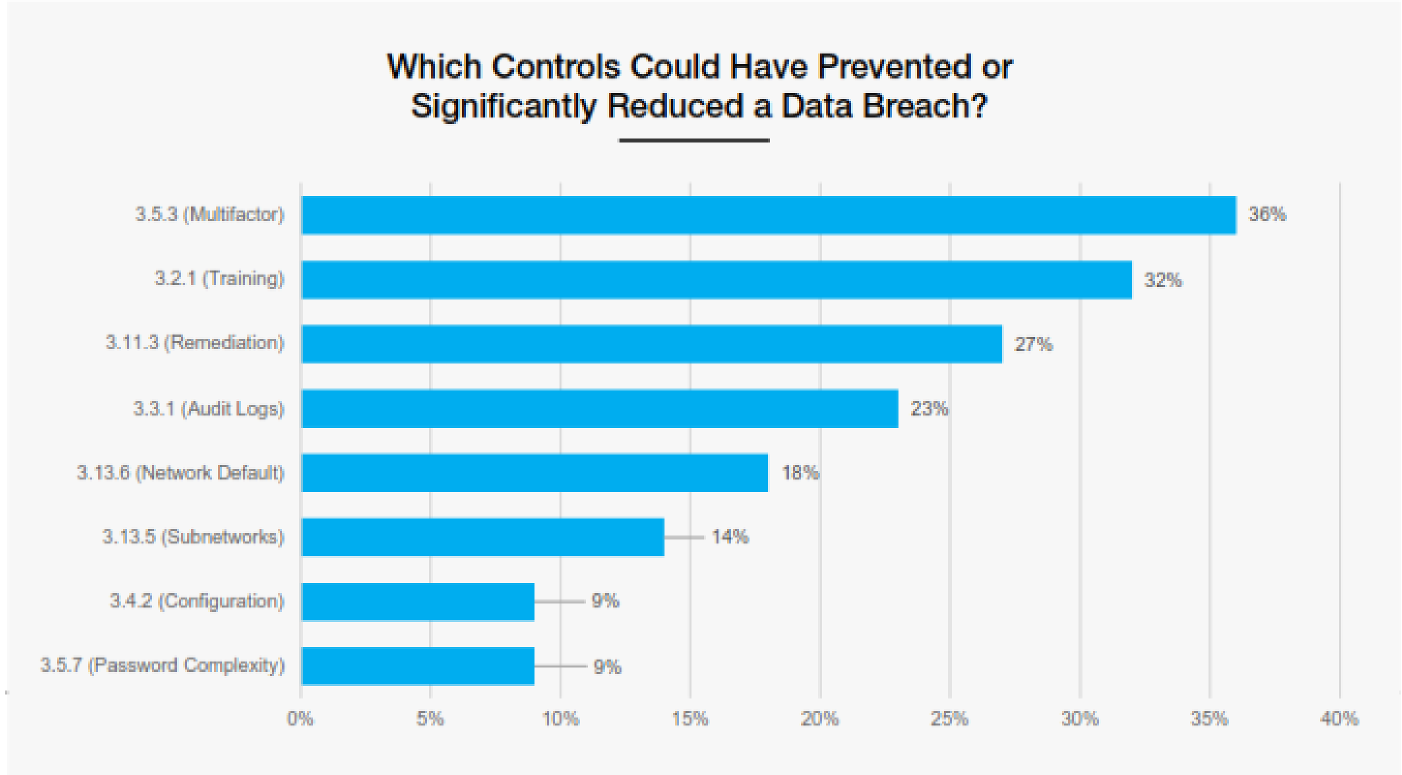


Larger issues with implementing NIST SP 800-171

- Misunderstanding the controls
  - Many IT personnel are fully engaged in support of the availability of the network. Seeking to discern meanings from government policies tends to be low on their list of priorities
- Cultural issues
  - Security is not seen as a profit driver – significant additional costs
  - Security requires change – changing people’s access levels
- Cloud Services
  - Enable centralized storage of documents in a secure environment – BUT minimally secure regarding outside access, requires additional controls
  - Many cloud services in use are not FedRAMP Moderate baseline compliant

Incident Response Findings

- In most cases, 800-171 controls would have prevented a breach or significantly reduced the impact
- In particular,
  - Lack of MFA (3.5.3)
  - Untrained users (3.2.1)
  - Poor patch management (3.11.3)
  - Lack of Audit Logs (3.3.1)



Findings Similar to Jul 2019 DOD IG Study

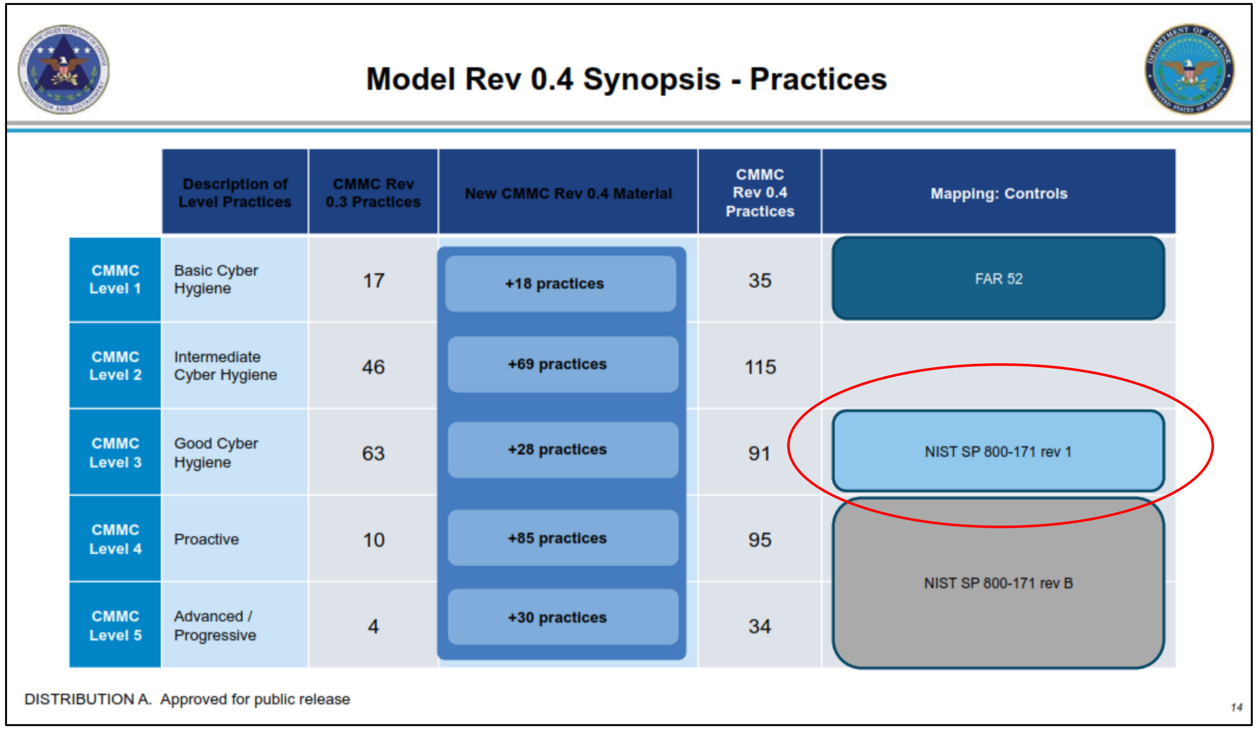
Sera-Brynn Reality Check	DOD IG Audit of Protection of DoD CUI on Contractor-Owned Networks and Systems
• Lack of MFA (3.5.3) • Untrained users (3.2.1) • Poor patch management (3.11.3) • Lack of Audit Logs (3.3.1)	• Contractors did not always mitigate the vulnerabilities on their networks and systems (3.11.3 Patches, 3.14.5 Scans) • Multifactor authentication was not consistently used (3.5.3) • Password lengths were susceptible to password attacks (3.5.7 Pwd Complexity) • CUI on removable media was not protected (3.8.6)

Recent Changes

- Jul 2019 - Defense Contract Management Agency (DCMA) assessing contractor compliance with DFARS Clause 252.204-7012 and NIST SP 800-171 as part of review of contractor purchase systems
  - Reviewing procedures to assess compliance of their Tier 1 Level Suppliers
- Sep 2019 - Navy Marine Corps Acquisition Regulation Supplement (NMCARS) changes to enforce DFARS Clause 252.204-7012 compliance
  - KOs consider the right to reduce or suspend progress payments for contractor noncompliance
  - Reinforces, that "A contractor MUST make their SSP available to the contracting officer within 30 days of contract award and be ready to host the contracting officer for a review of the SSP at the contractor's facility."
    - Instance of subcontractor "let go" by prime on a recompete bid because no SSP or POAM

CMMC Anticipation

- Companies looking for clear guidance
  - Not sure what to do
  - Attending Listening Tour, Seminars/Speaking
  - Realize Gov't is "building the plane inflight"
- Some companies waiting until CMMC is final to do anything
  - Not aware of FAR 52 or DFARS 252.204-7012
- Some companies unaware of need for compliance
  - "We don't have any CUI…whatever that is"
  - Disconnect from Privacy Act and other PII protection regulations



Model Rev 0.4 Synopsis - Practices

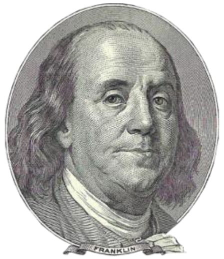
	Description of Level Practices	CMMC Rev 0.3 Practices	New CMMC Rev 0.4 Material	CMMC Rev 0.4 Practices	Mapping: Controls
CMMC Level 1	Basic Cyber Hygiene	17	+18 practices	35	FAR 52
CMMC Level 2	Intermediate Cyber Hygiene	46	+69 practices	115	
CMMC Level 3	Good Cyber Hygiene	63	+28 practices	91	NIST SP 800-171 rev 1
CMMC Level 4	Proactive	10	+85 practices	95	NIST SP 800-171 rev B
CMMC Level 5	Advanced / Progressive	4	+30 practices	34	

DISTRIBUTION A. Approved for public release

14

Recommendations for Businesses

- Dust off SSP and complete actions in POAMs to comply with 800-171
  - Best preparation for CMMC in Oct 2020
- Budget for cybersecurity
  - Labor, Vulnerability Scans, Pen Tests, internal/external audits
- Ensure cybersecurity is a team effort – Admin, Intel, Ops, and IT
  - Put your Cybersecurity Support POC on speed dial
- Run your Incident Response Plan w/Key Players – desktop exercise
- Treat Cybersecurity like you do ISO – monthly metric reviews, documentation reviews, internal audits



"An ounce of prevention is worth a pound of cure."
Benjamin Franklin

The State of Compliance

Sam Morthland
Executive VP, Federal Services
sam.morthland@sera-brynn.com
703-988-5764