

Cyber Compliance: Lessons Learned



2022 Technology and Compliance Conference



1



Background

- Cyber compliance is a disorganized mess.
- Every vendor has their own questionnaire and requirements.
- Different federal, state, and local government agencies have their own requirements, too.



2

US DoD's 1st Solution (2017):

NIST SP 800-171

- Introduced via DFARS 252.204-7012
- Required contractors handling "Controlled Unclassified Information" ("CUI") to do gap assessments and create POA&Ms to address the gaps.



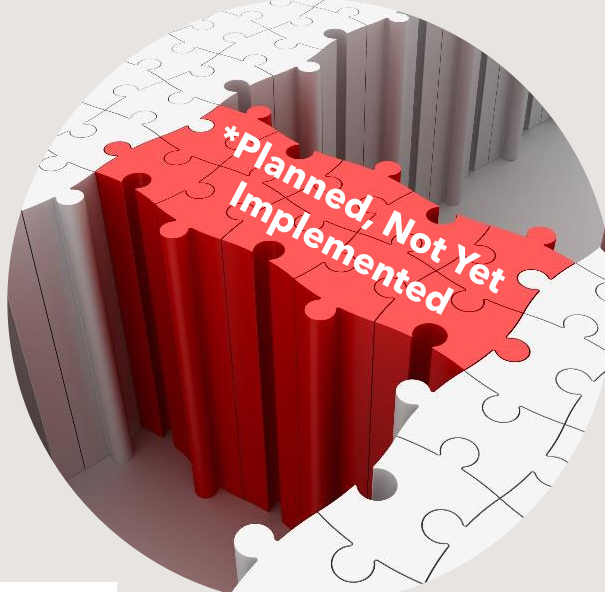
3



Super idea!



- Creates consistency across one of the government's largest agencies
- Serves as a testbed for other agencies
- Can be leveraged by SLED and commercial organizations
- Single compliance question

4



Lessons Learned


- Contractors don't know whether they are handling CUI.
- Contractors didn't remediate the gaps they identified, despite creating POA&Ms, because remediation isn't explicitly required.



5

US DoD's 2nd Solution (2019):

CMMC and DFARS -7019 and -7020



- DFARS 252.204-7019 - Contractors handling CUI must calculate a score based on their compliance with 800-171 ("low assurance") and submit to SPRS.
- DFARS 252.204-7020 - DCMA's DIBCAC team can conduct spot-checks against contractors' systems and conduct medium and high assurance compliance audits.
- DFARS 252.204-7021 - "CMMC" - For those handling CUI, Authorized 3rd Parties must perform an assessment against 800-171 and issue certification.
- Contracts with -7021 in them will require essentially all contractors handling CUI to be certified.

6

Contractors' Response to DFARS -7019

- DoD estimates 80,000 contractors handle CUI
- Only roughly 20,000 have submitted scores to SPRS
- Of those submitting scores, 75% have given themselves perfect scores



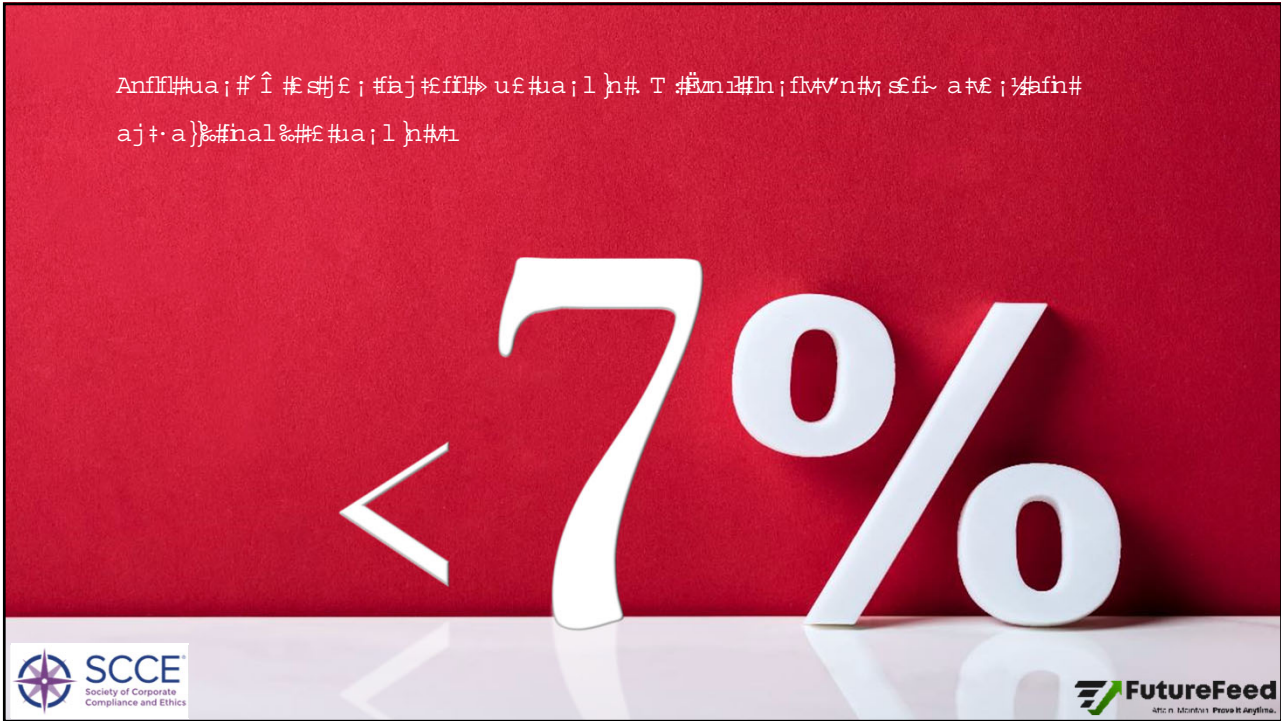
7

DIBCAC's Lessons Learned

- 75% of the companies giving themselves perfect scores are taking a rosy view of their compliance.
- Many miss several controls.






8



9

How About the Basics?

- 800-171 has 110 controls and over 300 objectives.
- FAR 52.204-21 only has 15, and they are the kind of things that everyone should do.



10



Frequent Internal Roadblocks

- Overly confident contractor employees/ service providers
- Programs built without a foundation
- Failure to identify the requirements
- Misunderstanding the requirements
- Lack of evidence
- One and done mentality



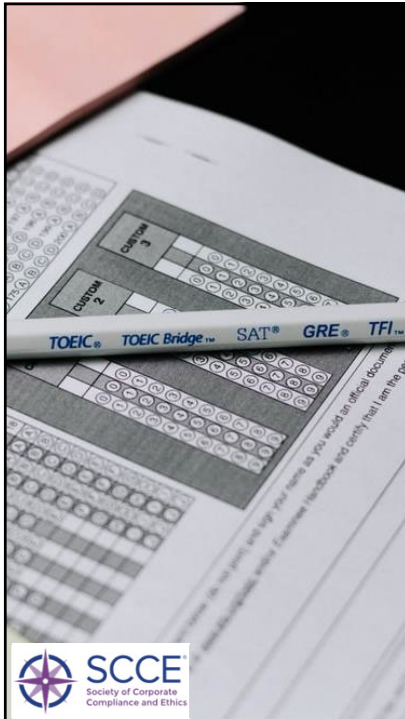
13

Employee Overconfidence

- Bring in a 3rd Party
- Penetration testers are a great start
- Also need to review:
 - *Policies, procedures, etc.*
 - *System configurations*
 - *Evidence*



14



Don't Make Stuff Up: Select an industry standard and build your program to that standard

- **Center for Internet Security Controls**
 - ~150 requirements
 - Good for most orgs
 - Widely adopted, but not well known
- **FAR 52.204-21**
 - 15 requirements
 - US Government demands this from all contractors
- **NIST SP 800-171**
 - Required of all government contractors handling CUI
 - Most companies have the same types of data as CUI (e.g., social security numbers, credit card info, client info, partner business plans, etc.)



15

Carefully Identify and Track the Requirements

- Use a contract manager
 - Even an Excel spreadsheet will work
- Track the requirements from each contract
 - Remember that not all requirements are technical (e.g., breach notification)
- Requirements may vary by enclave

Contracts

Title / Description	Start Date	End Date	Related CAGE Code	Standard / Level	DFARS Clauses				Export Control Restrictions		
					7012	7019	7020	7021	ITAR	EAR	
Title: <input type="text" value="Test Contract"/> Description: <input type="text"/>	<input type="text" value="Start Date"/>	<input type="text" value="End Date"/>	<input type="text" value="A234H"/>	<input type="text" value="CMMC v2.0 - Level 2"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Title: <input type="text" value="Contract"/> Description: <input type="text"/>	<input type="text" value="Start Date"/>	<input type="text" value="End Date"/>	<input type="text" value="None"/>	<input type="text" value="CMMC v1.0 - Level 3"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



16

AC.L2-3.1.3 Control CUI Flow

Control the flow of CUI in accordance with approved authorizations.

Practice Guidance

Practice Satisfaction Summary

Confidence: 9

Summary Notes / Findings

Objectives

Objective	POAAM	NOT SET	MET	NOT MET
[a] Information flow control policies are defined.	1	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
[b] Methods and enforcement mechanisms for controlling the flow of CUI are defined.	+	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
[c] Designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.	+	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
[d] Authorizations for controlling the flow of CUI are defined.	1	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>


Make Sure Your Team Fully Understands the Requirements

- B a ; % # l a ; l a f l f l a " n # a ; # % f f n f l ~ n ; # B · v l n # v u # a l l v # ; a) # n a v) B a ; l # a l l v # ; a) # n > · v n ~ n ; # l
- - n # l · f n # # n " a } · a n # f ~ < } a ; j n # v u # u n # % f f n f l ~ n ; # B · v l n # ; l # # # · f l # u n # l a ; l a f l # # l n } a

SCCE Society of Corporate Compliance and Ethics

FutureFeed

17



Continuously Document What You're Doing

- Assessments are point-in-time evaluations
- HOWEVER, artifacts can demonstrate maturity
- Don't just look to pass today, be ready to prove compliance anytime

SCCE Society of Corporate Compliance and Ethics

FutureFeed

18

Interview: Key Personnel

- Identify employee(s) accountable/responsible for each requirement.
- Update as the org. changes.
- Be ready: assessors can interview anyone.



19

Examine: Identify Key Documents

- Define the program
 - *Policies - broad statement of intent*
 - *Procedures - checklist-style instructions for implementing the policy (simple risks)*
 - *Plans - structured approaches to collecting information for complex issues*
- Demonstrate continuous compliance
 - *Records of procedure completion*
 - *Completed worksheets*
 - *Records of review*



20

Test

- List the software, system(s), and equipment that should be reviewed
- Define suggested review (based on documentation)



21

Effective Communication with Stakeholders



- Establish consistency
- Use a single standard as your guide
 - *Even if your org is subject to other standards*
 - *Can be a hybrid of other standards*
- Stick to basic numeric scales (1-10, 1-50, 1-100)



22

Cybersecurity Assessment/Audit Preparation Process

1. Conduct Inventory
 1. Hardware
 2. Software
 3. Cloud services
 4. Information
2. Use inventory information to define "systems".
3. Create Diagrams
 1. Network diagram (illustrates the overall architecture).
 2. Data flow diagram (illustrates how data moves to/from the systems).
 3. Role-based org chart with information and system authorization.
4. Determine whether the environment should be managed under a single System Security Plan ("SSP").
 1. Does the nature of the work performed, or the workflow/information handled, suggest treating the environment as discrete systems with their own SSPs?
5. Collect policies, procedures, plans, and other documents relevant to the assessment scope, if they exist.
6. Perform a gap analysis against the standard(s), but don't bother collecting evidence.
7. Create POA&Ms (gap remediation plans) for open actions.
8. Close the gaps.
9. Perform a validation analysis – collect evidence that demonstrates your compliance with all the requirements defined in the assessment guide.



7Efi# ffin# n tavyll#nnø
u##<124j ~ ~ jvj ε ε ft % ~ ~ % " % ' %j ~ ~ jD a < D a < D j) n ; # n ; t a t n ~ n ; # x f j n f l a ; l D · n f t # ε ; j a v n %



23



Don't Forget Your Supply Chain

- Cybersecurity isn't just an internal issue.
- Third parties can send you infected software, documents, equipment.
- Third parties can bring infected items into your environment.
- Your clients can also be problematic.



24

Consistency is the Key

- Consistent approach to client engagement and service delivery from service providers.
- Consistent focus on a standardized set of requirements.
- Consistent use of terms.
- Consistent application of established practices.
- Consistent presentation of information.
- Consistent questions to those in your supply chain.



25

About the Presenter

James Goepel

- General Counsel and Director of Education and Content at FutureFeed
- Professor of Cybersecurity at Drexel University
- Published Cybersecurity Risk Management Author
- Co-Founder, CMMC Information Institute
- Author and Instructor of CMMC Accreditation Body's Registered Practitioner Training
- CMMC Provisional Instructor and Candidate CMMC Provisional Assessor
- Founding Director and Former Treasurer, CMMC Accreditation Body



26