

NIST 800-171 Requirements, Updates & CMMC Planning

July 12, 2023



As featured in:

**DEFENSE
SYSTEMS**

SECURITY
MANAGEMENT
A PUBLICATION OF ASIS INTERNATIONAL

KMOX
NewsRadio 1120
The Voice of St. Louis

CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

ST. LOUIS
BUSINESS JOURNAL



Our Presenters Today



Elizabeth Niedringhaus
President and CEO



Charlie Sciuto
Vice President Technology
and Security



Bob Duffy
Vice President of Network and
Cybersecurity Services

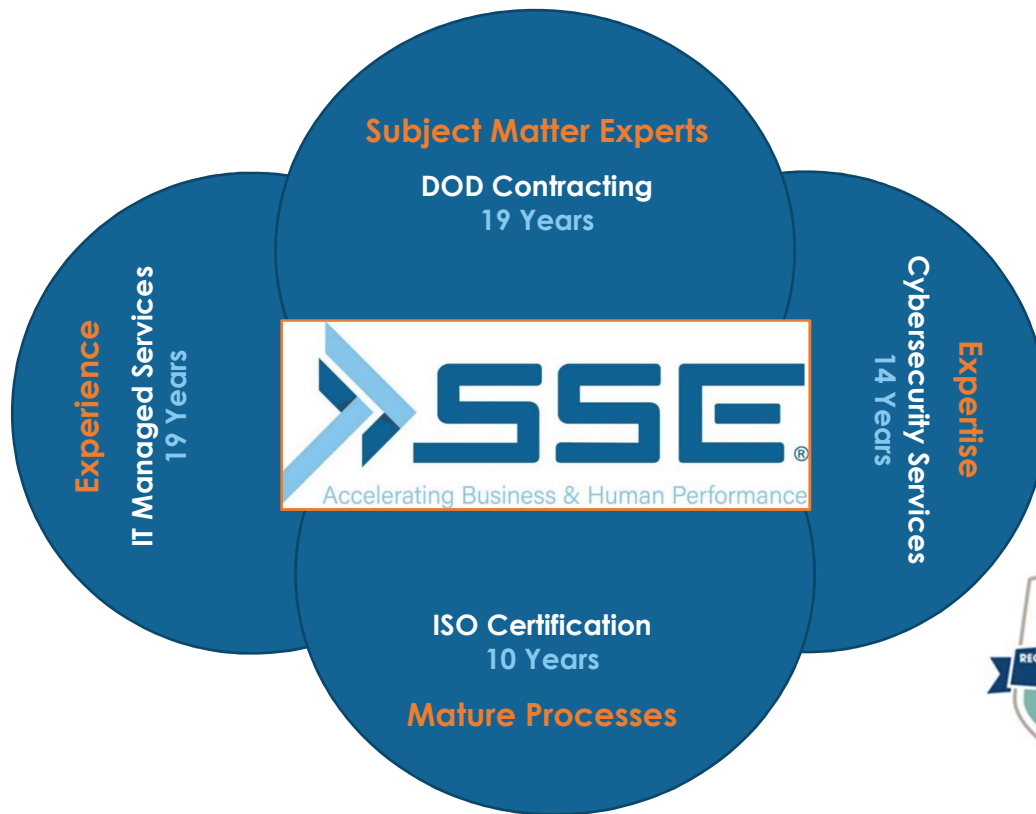
SSE Background



- Founded by Susan S. Elliott in 1966
- Grown and evolved since 1983
- Leader in training and IT services
- Developed cybersecurity expertise in 2009
- Supporting DoD clients across multiple industries
- Quality management system since 2013; ISO 9001:2015



Why SSE?



- NIST 800-53 compliant since 2009
Cage 1FGP5 - STL
Cage 64SV4 – JAX
- NIST 800-171 compliant since 2017
- Certifications:
 - 15 Certifications in SSE Tech Stack
 - 14 Certifications in general IT
 - 10 Certifications in IT/cybersecurity
 - **2 Registered Practitioners (RP) by CMMC Accreditation Body**
 - **3 Certified CMMC Professionals (CCP)**
 - **Registered Provider Organization (RPO) by CMMC Accreditation Body...now the Cyber AB**

Agenda

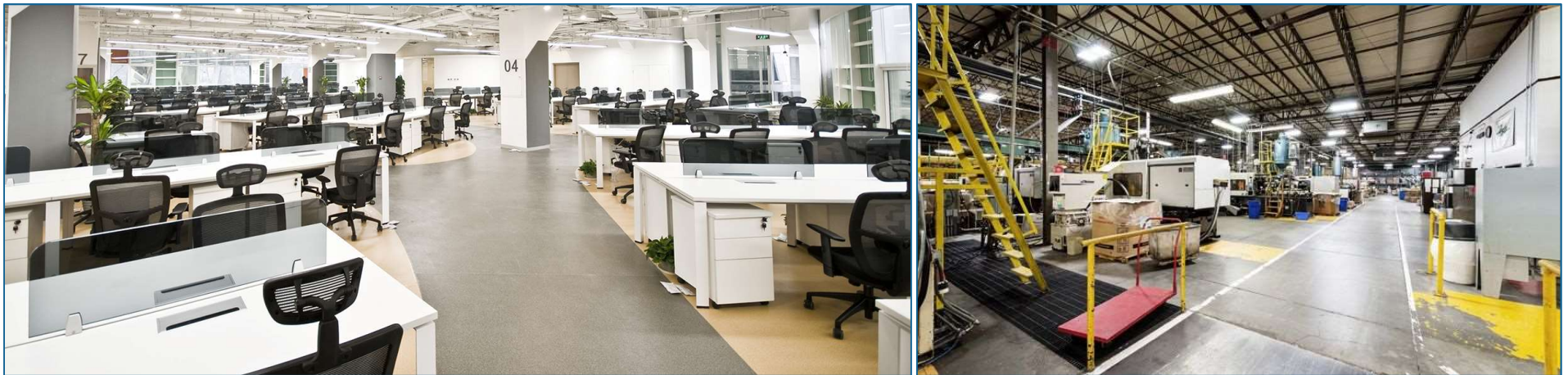


- NIST 800-171
 - What is required **NOW**
 - What is changing/being added with DRAFT Rev 3
- Risks of non-compliance
- CMMC timeline and latest updates
- SSE Solution Set
- Questions and Answers

NIST 800-171... Waiting is NOT an Option



- Applies to **ALL** DoD contractors and subcontractors (excluding COTS)
- Has been law since 2017
- DoD is starting to enforce requirements... and planning to add MORE requirements!



For manufacturers...must consider front office and shop floor

**Required NOW:
NIST 800-171 & Scored
Self-Assessments**



NIST 800-171 is not NEW



Year	Month	DFAR	Requirement	Description
2005			NIST 800-53	Federal System Protection: NIST SP 800-53 requirement
2014		DFAR 252.204-7012	NIST 800-171	Non-Federal System Protection: NIST 800-171 requirement; to be met no later than 12/31/2017
2017		DFAR 252.204-7012	NIST 800-171	Non-Federal System Protection: NIST 800-171 Self Attestation required
2019		DFAR 252.204-7012	NIST 800-171	Dod Inspector General, DODIG-2019-105, Contractors not consistently implementing NIST 800-171
2020	Sept	DFAR 252.204-7012	NIST 800-171	Interim Final Rule released amending 252.204-7012, effective 11/30/2020
		DFAR 252.204-7019	NIST 800-171	NIST 800-171 Self Assessment Methodology for input into SPRS... REQUIRED NOW
		DFAR 252.204-7020	NIST 800-171	NIST 800-171 Self Assessment Methodology for input into SPRS with ability for DOD review
		DFAR 252.204-7021	CMMC	Introduced Cybersecurity Maturity Model Certification (CMMC)

NIST is NOW - DFARS 252.204-7019 & 7020



- Objective Basic NIST 800-171 Self Assessment of current NIST 800-171 implementation status
- Weighted assessment methodology and score reflects the net effect of security requirements not yet implemented
- Perfect score of 110, and it is very possible to have a negative score
- Required System Security Plan (SSP) and date by which implementation will be complete based on any Plans of Action and Milestones (POAMs) for valid assessment submission
- Must be submitted in DoD Supplier Performance Risk System (SPRS)

NIST 800-171 DOD Assessment Methodology:

https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html

What is needed to submit an assessment score?



- Procurement Integrated Enterprise Environment (PIEE) account
- SPRS “Cyber Vendor” role needs to be active (may be requested through PIEE)
- Date of the assessment
- Summary level score (e.g., 95 out of 110, not the value for each requirement)
- Scope of the assessment – Commercial and Government Entity (CAGE) code(s)
- Plan of Action Completion Date – **date that a score of 110 is expected to be achieved**

SSE has detailed instructions for SPRS submission... contact us for help!

NIST 800-171 DOD Assessment Methodology:

https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html

**DRAFT NIST 800-171
Rev.3**



June 6 NIST Web Briefing



- A DRAFT Rev. 3 of SP NIST 800-171, Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations, was published in May of 2023, and it is available for **public comment through July 14: 800-171comments@list.nist.gov**
- Requirements are being updated to better align with NIST 800-53, Security and Privacy Controls for Information Systems and Organizations
- Addition of 3 “families”
- There are still likely to be 110 “controls”... but with more requirements (and likely more objectives when the assessment guide is updated) within those controls
- Final Rev 3 and an updated assessment guide are expected late 2023 – early 2024
- CMMC is still moving on its own track; updates to NIST 800-171 would also update CMMC Level 2 accordingly

Overview: Draft SP 800-171 Rev 3



Improved Readability

Streamlined “Introduction” and “The Fundamentals” sections

Updated Security Requirements

- Added, deleted, or changed security requirements to reflect controls & families in SP 800-53 Rev 5 and moderate baseline in 800-53B
- Eliminated distinction between basic & derived requirements
- Increased specificity & grouped requirements
- Introduced organization-defined parameters (ODPs)
- Removed outdated & redundant requirements

Significant Changes

Updated Tailoring Criteria

- Added new tailoring category, NA
- Recategorized selected controls from SP 800-53B moderate baseline

Added Supplemental Resources

- Developed *prototype* CUI Overlay using tailored controls in SP 800-53 Rev 5
- Created transition mapping tables & analysis of changes between SP 800-171 Revision 2 and Revision 3
- Developed an FAQ

Updated Security Requirements - #1



Number/Type of Changes:

Type of Change	Change Description	Number
No significant change	Editorial changes to requirement; no change in outcome.	18
Significant Change	Additional detail in requirement, including more comprehensive detail on and foundational tasks for achieving the outcome of the requirement.	49
Minor Change	Editorial changes. Limited changes in level of detail and outcome of requirement.	18
New Requirement	Newly added requirement in IPD SP 800-171 Rev 3.	26
Withdrawn Requirement	Requirement withdrawn.	27
New Organization-defined Parameter (ODP)	<i>Note: New ODPs can apply to all change types with the exception of withdrawn requirements. Each requirement includes one or more new ODPs.</i>	53
	Total Number of Security Requirements in Draft SP 800-171 Rev 3	138

Updated Security Requirements - #2



Added/Deleted Controls... and Added New Families of Controls:

Draft SP 800-171 Rev 3 Security Requirement Families			
Access Control (Added: 1, Withdrawn: 5)	Maintenance (Added: 0, Withdrawn: 3)	Security Assessment & Monitoring (Added: 3, Withdrawn: 1)	
Awareness & Training (Added: 0, Withdrawn: 0)	Media Protection (Added: 0, Withdrawn: 2)	System & Communications Protection (Added: 2, Withdrawn: 4)	
Audit & Accountability (Added: 0, Withdrawn: 0)	Personnel Security (Added: 0, Withdrawn: 0)	System & Information Integrity (Added: 1, Withdrawn: 3)	
Configuration Management (Added: 0, Withdrawn: 1)	Physical Protection (Added: 2, Withdrawn: 3)	New Families	Planning (Added: 4)
Identification & Authentication (Added: 1, Withdrawn: 4)	Risk Assessment (Added: 1, Withdrawn: 1)		System & Services Acquisition (Added: 2)
Incident Response (Added: 0, Withdrawn: 0)			Supply Chain Risk Management (Added: 4)

Updated Security Requirements - #2 cont.



New Families	Planning (Added: 4)
	System & Services Acquisition (Added: 2)
	Supply Chain Risk Management (Added: 4)

Planning

- Added rigor and ODPs around frequency with which policies and procedures, the system security plan and rules of behavior will be reviewed and updated.

System & Services Acquisition

- Added application of system security engineering in selection of software/services and need to have process to monitor compliance

Supply Chain Risk Management

- Added plan to mitigate supply chain risk with management plan, acquisition strategies, controls & processes

Updated Security Requirements - #3



Organization-defined Parameters (ODPs) = Variable part of a control that is defined/instantiated by organization during tailoring process by either assigning an organization defined value or selecting from a predefined list provided as part of the control

- Intended to increase flexibility and help organizations better manage risk
- 53 total ODPs added

Family	SP 800-171 R2 SORT-ID	SP 800-171 R2 Identifier	SP 800-171 R2 Security Requirement	Summary of Change(s)
Access Control	R2-03-01-08	3.1.8	Limit unsuccessful logon attempts.	New security requirement title Aligned with SP 800-53, Rev 5 Added new ODP: number of consecutive invalid login attempts Added new ODP: time period

Overview: Draft SP 800-171 Rev 3

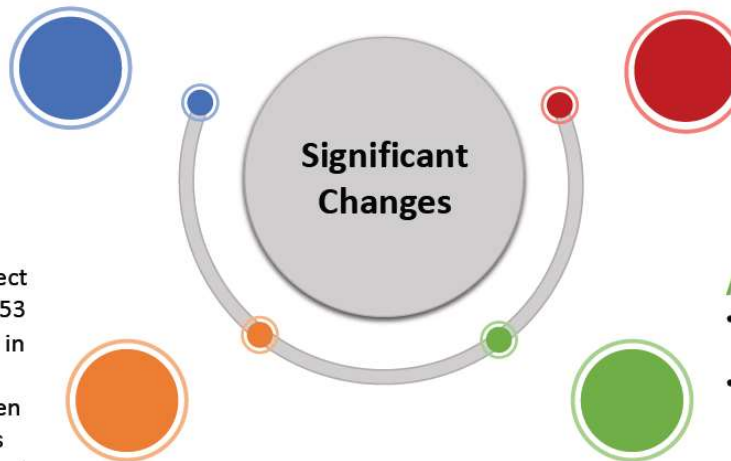


Improved Readability

Streamlined “Introduction” and “The Fundamentals” sections

Updated Security Requirements

- Added, deleted, or changed security requirements to reflect controls & families in SP 800-53 Rev 5 and moderate baseline in 800-53B
- Eliminated distinction between basic & derived requirements
- Increased specificity & grouped requirements
- Introduced organization-defined parameters (ODPs)
- Removed outdated & redundant requirements



Updated Tailoring Criteria

- Added new tailoring category, NA
- Recategorized selected controls from SP 800-53B moderate baseline

Added Supplemental Resources

- Developed *prototype* CUI Overlay using tailored controls in SP 800-53 Rev 5
- Created transition mapping tables & analysis of changes between SP 800-171 Revision 2 and Revision 3
- Developed an FAQ

Updates Tailoring Criteria



Tailoring = The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.

- Added NA As Tailoring Criteria

Overlay Summary:

Control overlay for protecting the confidentiality of Controlled Unclassified Information (CUI) based on SP 800-53 Revision 5 and SP 800-53. Serves as an alternative method to capture the security requirements in IPD SP 800-171 Revision 3 and provides a detailed analysis of the tailoring decisions at the control item (or requirement item)-level between SP 800-53 and SP 800-171. The tailoring symbols and tailoring criteria used for the Prototype CUI Overlay are identified below:

NCO: Not directly related to protecting the confidentiality of CUI

NFO: Expected to be implemented by nonfederal organizations without specification

FED: Primarily the responsibility of the Federal Government

CUI: Directly related to protecting the confidentiality of CUI

NA: Not Applicable. *Note that controls in the (SP 800-53 Rev 5/SP 800-53B) PM and PT families are considered NA since they are not included in the moderate baseline. The PM and PT controls are not included in the Prototype CUI Overlay.*

Overview: Draft SP 800-171 Rev 3

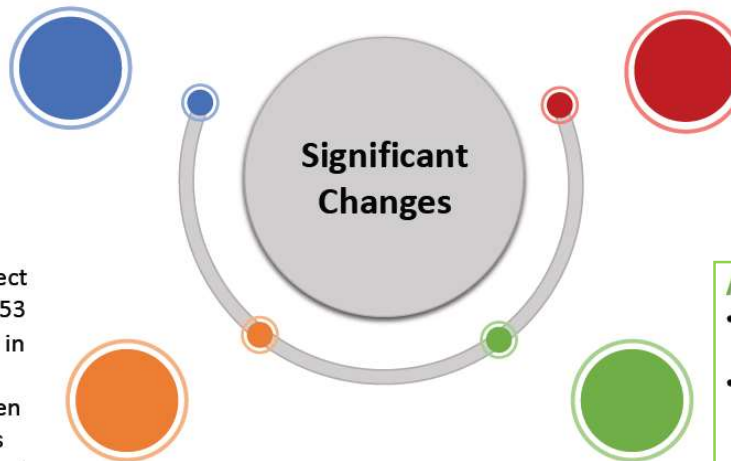


Improved Readability

Streamlined “Introduction” and “The Fundamentals” sections

Updated Security Requirements

- Added, deleted, or changed security requirements to reflect controls & families in SP 800-53 Rev 5 and moderate baseline in 800-53B
- Eliminated distinction between basic & derived requirements
- Increased specificity & grouped requirements
- Introduced organization-defined parameters (ODPs)
- Removed outdated & redundant requirements



Updated Tailoring Criteria

- Added new tailoring category, NA
- Recategorized selected controls from SP 800-53B moderate baseline

Added Supplemental Resources

- Developed *prototype* CUI Overlay using tailored controls in SP 800-53 Rev 5
- Created transition mapping tables & analysis of changes between SP 800-171 Revision 2 and Revision 3
- Developed an FAQ

Added Supplemental Resources



NIST Website - <https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/draft>

DOCUMENTATION

Publication:

- [SP 800-171 Rev. 3 \(Draft\) \(DOI\)](#)
- [Local Download](#)

Supplemental Material:

- [Comment template \(xls\)](#)
- [FAQ \(pdf\)](#)
- [Change analysis \(Rev. 2 to Rev. 3 ipd\) \(xls\)](#)
- [Prototype CUI Overlay \(xls\)](#)
- [Protecting CUI project \(web\)](#)
- [NIST news article \(web\)](#)

SSE's 3 Main Takeaways



1. What remains true is that DFARS -7012 contractually requires NIST 800-171 (current Rev 2) compliance NOW... and significant risk to non-compliance with the False Claims Act and contractual consequences for failing to comply.
2. What DoD contractors should focus on NOW is the implementation of NIST 800-171 as it exists today... with an eye to meeting or upgrading to Rev. 3 requirements when they are incorporated in contracts in the future
3. If DoD contractor is focused on when third party auditors (C3PAOs) may begin CMMC certification audits, they are missing the point and putting their business at risk

For additional info and resources:

<https://csrc.nist.gov/Projects/protecting-CUI>

Risks of Non-Compliance

Recent Study of DoD Contractors (CyberSheath/Merrill Research)



Survey of 300 defense contractors seeking CMMC compliance...

- Only 60% have a System Security Plan (SSP)
- Only 53% have Plans of Action and Milestones (POAMs)
- 80% lack a Vulnerability Management solution
- 79% lack Multi-Factor Authentication (MFA)
- 70% have not deployed Security Information and Event Management (SIEM)

“This is a huge concern and problem. Why are companies so behind? Where is our patriotism? Why are we giving our intellectual property away to our adversaries? Please pay attention to your cyber and physical security!!!!”

~Stacy Bostjanick
CMMC Director and DoD CIO
(12/5/22)

Risks of Non-Compliance



Risk Background:

- Since October 2016, under 252.204-7008 solicitation clause, contractors represent they **“will implement”** NIST 800-171 by 12/31/2017.
- And, under 252.204-7012 clause, agree they **“shall implement”**...**“as soon as practical, but not later than”** 12/31/2017.
- Under the November 2020 252.204-7019 clause: “In order to be considered for award” an offeror must **“verify”** a “current” NIST 800-171 self-scoring of its information systems, and include:
 - The system security plan (SSP) architecture
 - The **“expected”** completion date
- **CMMC 2.0 will require at least “affirmation” of compliance by a senior official.**

Risks of Non-Compliance



Contracts:

- Unable to secure next/additional contracts
- Termination for default/damages

Civil/Criminal Damages and Penalties:

- Knowing or reckless misstatements risk liability under the False Claims Act

DOJ Cyber Fraud Initiative launched in 2022... settlements of \$9M against a DoD manufacturer and \$300K for a sole proprietor!

- Knowing and willfully making a false claim or statement can be criminally prosecuted

DoD reviewing NIST 800-171 Assessment Submissions (Cyber-AB)



- Defense Contract Management Agency (DCMA) started sampling System Security Plans submitted by contractors on their compliance with NIST 800-171 during summer of 2022 to make sure companies were **“likely complying”**
 - 60K companies had submitted basic NIST 800-171 scored self assessment detail to SPRS as of Q2 2022 (Cyber-AB)
 - **26% of these companies dubiously reported a perfect score of 110 (Cyber-AB)**
- Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) now examining SPRS data and conducting medium assessments on companies that had submitted basic assessments
 - They found an average basic assessment score of 56, and an average medium assessment score of -57... **This represents a -113 point gap between “perception and reality”**

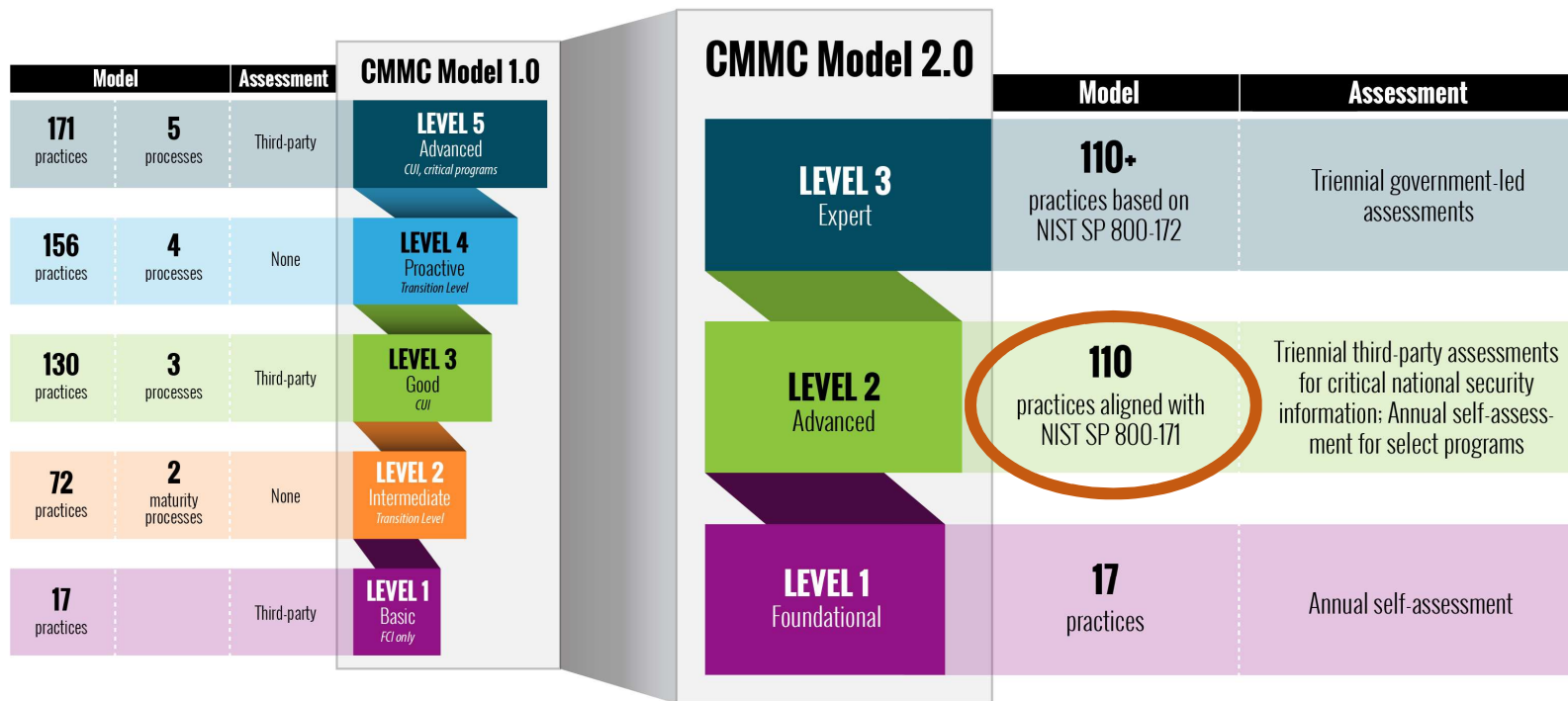
Challenge and significant risk...

- For companies that do not have a SSP but submitted a scored self-assessment
- Or, considering the documentation provided, submitted an incredibly high score

CMMC Updates

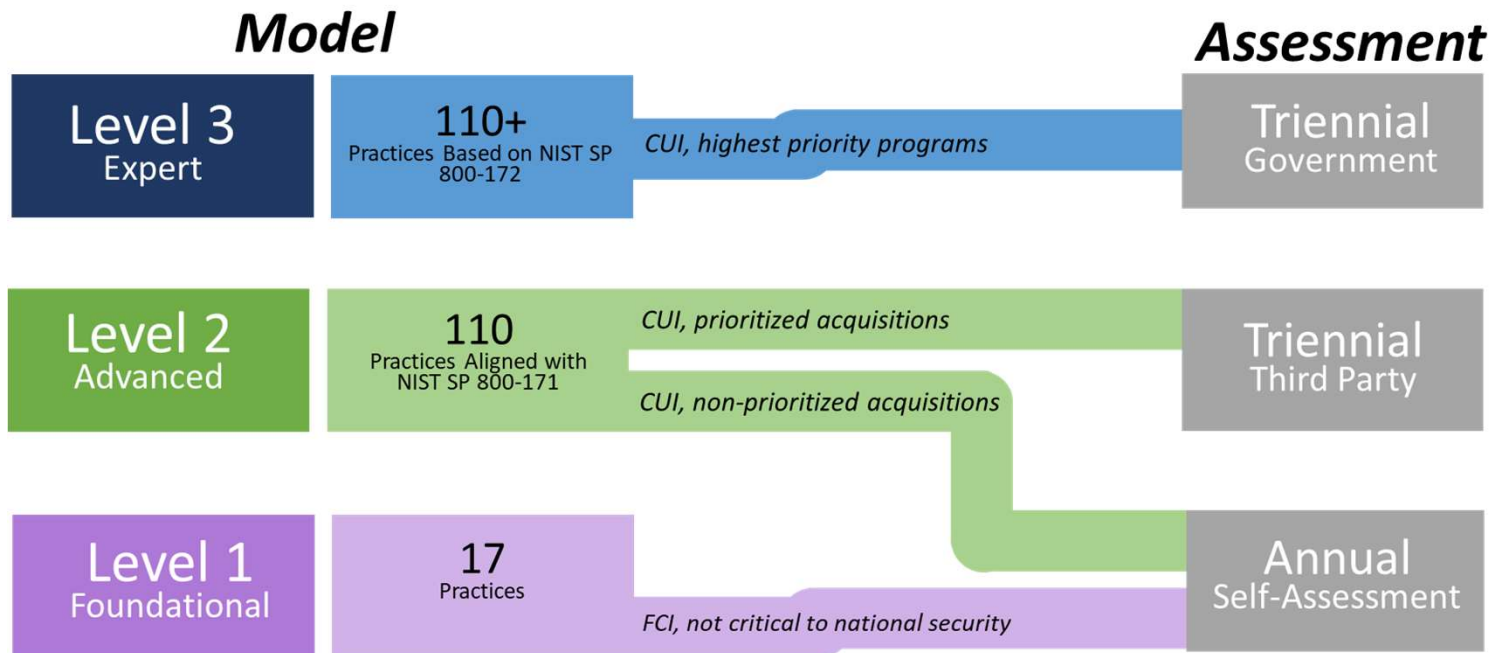


CMMC 1.0 vs 2.0 – Model Specifics



<https://www.acq.osd.mil/cmmc/about-us.html>

Assessment Requirements by Level



From 11/9/21 CMMC-AB Town Hall: The information in this presentation reflects the DoD's strategic intent with respect to the CMMC program. The DoD will be engaging in rulemaking and internal resourcing as part of implementation, and program details are subject to change during these processes.

Assessment Complexity

- **Level 1** = 17 controls; 54 page assessment guide
- **Level 2** = 110 controls (inclusive of Level 1)
 - **320 assessment objectives**
 - 270 page assessment guide!!
- Each control has the following:
 - Control definition
 - Assessment objectives
 - Potential assessment methods and objects
 - Discussion
 - Key references

AC.1.1-3.1.1 – Authorized Access Control

Access Control (AC)

AC.1.1-3.1.1 – AUTHORIZED ACCESS CONTROL

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

- [a] authorized users are identified;
- [b] processes acting on behalf of authorized users are identified;
- [c] devices (and other systems) authorized to connect to the system are identified;
- [d] system access is limited to authorized users;
- [e] system access is limited to processes acting on behalf of authorized users; and
- [f] system access is limited to authorized devices (including other systems).


POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine
[SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].

Interview
[SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].

Test
[SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management].

CDM: Self Assessment Guide - Level 1 - Version 2.0



<https://www.acq.osd.mil/cmmc/index.html>

The Evolution to CMMC



Required Now

What's Ahead

Year	Month	DFAR	Requirement	Description
2005			NIST 800-53	Federal System Protection: NIST SP 800-53 requirement
2014		DFAR 252.204-7012	NIST 800-171	Non-Federal System Protection: NIST 800-171 requirement; to be met no later than 12/31/2017
2017		DFAR 252.204-7012	NIST 800-171	Non-Federal System Protection: NIST 800-171 Self Attestation required
2019		DFAR 252.204-7012	NIST 800-171	Dod Inspector General, DODIG-2019-105, Contractors not consistently implementing NIST 800-171
2020	Sept	DFAR 252.204-7012	NIST 800-171	Interim Final Rule released amending 252.204-7012, effective 11/30/2020
		DFAR 252.204-7019	NIST 800-171	NIST 800-171 Self Assessment Methodology for input into SPRS... REQUIRED NOW
		DFAR 252.204-7020	NIST 800-171	NIST 800-171 Self Assessment Methodology for input into SPRS with ability for DOD review
		DFAR 252.204-7021	CMMC	Introduced Cybersecurity Maturity Model Certification (CMMC)
2021	March	DFAR 252.204-7021	CMMC	Initiated internal review of CMMC; 850 public comments
	Nov	DFAR 252.204-7021	CMMC	Suspended and announced CMMC 2.0 with timeline of 9-24 months
2022	July		CMMC 2.0	Rulemaking started
2023	March		CMMC 2.0	Anticipated Release of 2 Interim Rules
	May		CMMC 2.0	Requirement in DOD Contracts
	Sept		CMMC 2.0	Planned to issue 2 NEW Interim Proposed Rules
2024	FALL		CMMC 2.0	Planned to finalize rules

Latest from CYBER-AB Townhalls



- Implementation to follow, with requirements showing up in contracts
- Potentially a three-year rollout plan, but...

“On day one everyone will be required to do the self-assessment, the positive affirmation”

- Stacy Bostjanick, CMMC Director and DoD CIO

- Early adoption and voluntary assessments are being encouraged



Voluntary CMMC Assessments



- Now up to 44 approved C3PAOs ... 400+ in the application process
- Voluntary assessments have been a joint effort between DCMA Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) in collaboration with C3PAOs
- At least 14 voluntary assessments have been completed since starting in August
- Is there a benefit to early adopters?
Companies can be assessed now, and the assessment would convert to CMMC certification at the time CMMC is officially implemented



2023-2024 Compliance Planning

Initial Readiness Assessment



- Survey current environment and future needs using questionnaire
- Summary review of your existing SSP and POAMs (if possible)
- Summary review of existing IT Tools
- Discuss high-level budget and roadmap
- Overall estimation of current state readiness for CMMC; potential points at risk on NIST 800-171 Assessment

When? Schedule NOW... SSE complimentary service!

Gap Assessment



- Evidence collection and detailed assessment of current environment by CMMC Registered Practitioner
- Focus on NIST 800-171 and CMMC Level 2 – 110 Controls
- **Deliverables:**
 - Security Assessment Report “SAR”
 - + Detailed Compliance Traceability Matrix
 - + NIST 800-171 Assessment Score
 - + Information for SSP
 - + POAMs
- **Timeline:** 4 weeks



Why? Deliverables help fulfill the immediate documentation requirements for NIST 800-171 submissions AND planning for CMMC implementation

When? Schedule NOW for Q3-Q4; develop plan and budget for 2023-2024

Key Gap Assessment Deliverable: Information for SSP



- Implementation status per control
- Notes on implementation detail by objective
- Feeds directly into POAMs if not or partially met

CM.L2-3.4.1	Practice/Control Information
Practice: Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
Implementation Status (check all that apply): <input type="checkbox"/> Met <input type="checkbox"/> Partially Met <input checked="" type="checkbox"/> Not Met <input type="checkbox"/> Not Applicable	
Control Activity Name:	Control Activity Description:
N/A	N/A
Implementation Details: [a] A baseline configuration has not been formally defined; [b] informal baselines that exist only address hardware and software, not firmware, documentation, or configuration; [c] no formal review process exists for system baselines; [d][e] hardware/software inventory maintained in PDQ Inventory; [f] PDQ Inventory automatically rescans and updates the inventory on a regular, periodic basis.	
Objective Evidence:	

Key Gap Assessment Deliverable: Plans of Action & Milestones (POAMs)



- Designed and delivered as a working document
- Able to be updated with status and progress
- Vital in determining remediation scope and budget

Applicable Control Family	Applicable Control Name	Description	Milestones
Access Control	Access Enforcement (3.1.2)	The types of transactions users are permitted to execute has not been formally defined.	Develop, document, and implement a formal definition of the types of transactions that each type of user is permitted to execute.
Access Control	Information Flow Enforcement (3.1.3)	Policies and/or procedures describing how CUI is to be received, stored, and/or transmitted within, and without, the organization have not been developed or implemented.	Develop, document, and implement policies and/or procedures for the receipt, storage, and transmission of CUI both within and without the organization.
Access Control	Separation of Duties (3.1.4)	There are insufficient policies or procedures formally defining the separation of duties of the audit administrator from other system administrators. Additionally, access privileges do not adequately restrict the audit administrator from being able to execute privileged functions in certain areas, nor has system administrators' access been adequately restricted to prevent tampering or destruction of audit records.	Develop, document, and implement the mechanisms necessary to prevent malevolent activity without collusion., Develop, document, and implement policies and/or procedures formally defining the roles and responsibilities of the audit administrator.
Access Control	Least Privilege (3.1.5)	[a] There was insufficient evidence presented during the examination to ensure that privileged user accounts are readily identifiable as such. [c] There are insufficient policies or procedures formally identifying the security functions and the personnel assigned to execute them.	Develop, document, and implement procedures for the creation of privileged user accounts and the inclusion of some form of marking making such account readily identifiable as privileged., Develop, document, and implement policies and/or procedures formally identifying security functions and the personnel assigned to execute those functions.

Key Gap Assessment Deliverable: Basic NIST 800-171 Assessment Score



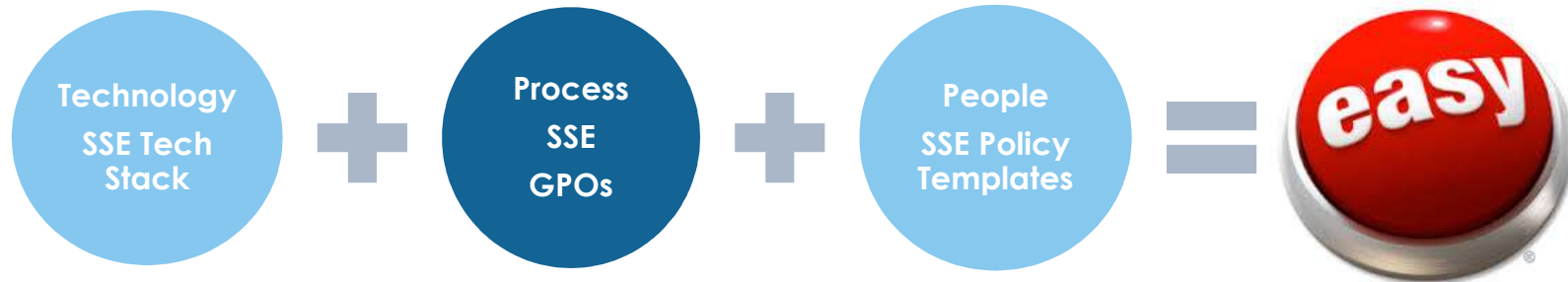
SSE		Appendix D - NIST 800-171 Scoring Assessment					
		Date: XX-XX-XXX		XYZ Company			
CMMC 2.0 Practice Number	NIST 800-171 Control Number	Met	Partially Met	Not Met	N/A	RISK LEVEL (H,M,L,O)	SCORE
AC.L1-3.1.1	3.1.1	1				H	0
AC.L1-3.1.2	3.1.2			1		H	-5
AC.L1-3.1.20	3.1.20			1		L	-1
AC.L1-3.1.22	3.1.22			1		L	-1
AC.L2-3.1.10	3.1.10			1		L	-1
AC.L2-3.1.11	3.1.11			1		L	-1
AC.L2-3.1.12	3.1.12			1		H	-5
AC.L2-3.1.13	3.1.13			1		H	-5
AC.L2-3.1.14	3.1.14	1				L	0
AC.L2-3.1.15	3.1.15			1		L	-1
AC.L2-3.1.16	3.1.16			1		H	-5
AC.L2-3.1.17	3.1.17	1				H	0
AC.L2-3.1.18	3.1.18	1				H	0
AC.L2-3.1.19	3.1.19			1		M	-3

- Evidenced based assessment and score
- Validated by SSP info and POAMs
- Primes are increasingly starting to require SPRS submissions, often to enable subcontractors to continue receiving CUI digitally

Total Number of Controls	110
Total Deductions	-197
NIST 800-171 Assessment Score	-87

Remediation Made Easy!

SSE Solution Set for DoD Contractors



SSE Tech Stack



IT Tools

- fully vetted to meet requirements
- tested and in production

Multi-Factor Authentication	Advanced CMMC Level 2
Intrusion Detection/Prevention	
System Information and Event Management	
Email Encryption	
Mobile Device Management	
Web Filtering	
Configuration Management	
Software Management	
Session Management	
VPN	
Harddrive Encryption	
Network Diagram	
Group Policy Objects	
Email Phishing & Cybersecurity Training	
Firewall	
Back-Up and Disaster Recovery	
Anti-virus	
Vulnerability Management	
Patch Management	
Network Access Control	
Ticketing System	SSE Management Tools
Remote monitoring	
Client Database	
Reporting	

- 90 point deduction from weighted NIST Assessment score without these!

SSE Group Policy Objects



“GPOs”

Fully tested and
in production

**-152 point
deduction
without IT Tools +
GPOs!**

CMMC Practice Requirement	Compliance Methodology
Provide privacy and security notices consistent with applicable CUI rules.	Logon Banner
Use non-privileged accounts or roles when accessing nonsecurity functions.	Employee separation of duties and removal of local administrative rights
Limit unsuccessful logon attempts.	enable account lock based on logon failures
Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	enable session lock after no more than 10 minutes of inactivity
Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	VPN uses approved encryption for all remote access.
Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	Audit information retained
Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	Network Time coordinated with NTP servers at NIST
Control and monitor user-installed software.	Prohibit use or installation of unauthorized software
Enforce a minimum password complexity and change of characters when new passwords are created.	Password policy
Prohibit password reuse for a specified number of generations.	Password policy
Allow temporary password use for system logons with an immediate change to a permanent password.	Temporary passwords are restricted to new employees and require password reset upon login
Control the use of removable media on system components.	Removable media not authorized on devices processing CUI data
Control and monitor the use of mobile code.	Prohibit use of mobile code, including on various web-browsers

SSE Model Policy & Procedure Templates



Ready for customization
to your environment!

- 313 point deduction
without IT Tools + GPOs
+ Policies!

Compliance Policies & Procedures	CLIENT POLICY INPUTS REQUIRED (as highlighted in SSE Provided Templates)	Compliance Policies & Procedures- Client Templates
AC_Access Control Policy	23	AC_Access Control Procedures AC_Access Control Appendix AC_Security Banner Configuration Procedure AC_Access Control List AC_New User Request Form
AT_Awareness and Training Policy	1	AT_Awareness and Training Procedures AT_Awareness and Training Appendix
AU_Audit and Accountability Policy	7	AU_Audit and Accountability Procedures AU_Audit and Accountability Appendix
CA_Security Assessment Policy	2	CA_Information Security Continuous Monitoring Pro CA_Security Assessment Appendix
CM_Configuration Management Policy	11	CM_Configuration Management Procedures CM_Configuration Management Appendix CM_Change Request Form
IA_Identification and Authentication Policy	7	IA_Identification and Authentication Procedures IA_Identification and Authentication Appendix
IR_Incident Response Policy	14	IR_Incident Response Plan IR_Incident Response Appendix IR_Incident Response Testing Plan IR_Incident Response Report
MA_Maintenance Policy	14	MA_Maintenance Procedures MA_Maintenance Appendix
MP_Media Protection Policy	6	MP_Media Protection Procedures MP_Media Protection Appendix MP_Authorized Access List
PE_Physical Protection Policy Template	6	PE_Physical Protection Procedures PE_Physical Protection Appendix PE_Visitor Access Log
PS_Personnel Security Policy Template	2	PS_Personnel Security Procedures PS_Personnel Security Appendix
RM_Risk Management Policy	3	RM_Risk Management Procedures RM_Risk Management Appendix RM_Equipment Decommission Checklist
SC_System and Communications Policy	16	SC_System and Communications Protection Procedu SC_System and Communication Protection Appendi
SI_System and Information Integrity Policy	10	SI_System and Information Integrity Procedures SI_System and Information Integrity Appendix
TOTAL	122	

Pretech™ Managed Services



- Network Monitoring, Administration and Maintenance
- User Support / Help Desk Services
- Network Health Reporting
- Technology Consulting / VCIO Services
- Project Services
- Workstation Builds

**Satisfies CMMC Level 1
Requirements**

Turn-key solution for small
businesses with FCI

Cybersecurity as a Service (CAAS)



- Outsourced management of SSE Tech Stack and GPOs
 - * Continuous monitoring and remediation/maintenance of IT Tools
 - * Audit/evidence collection to demonstrate compliance
 - * Plan of Action/Milestone identification and resolution
 - * Address Critical Alerts
 - * Monthly management reporting
- **Customizable and can layer on top of existing internal IT resources or MSP services**
- Support internal self-assessment (at least annually)

**Satisfies
CMMC
Level 2
Requirements**

What is Continuous Monitoring?



- CA (Security Assessment) L2-3.12.4:

Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls

- Sample Continuous Monitoring or “COMMON” schedule
- Significant time and resources necessary to manage internally
- Efficiently outsourced and managed by SSE

CMMC Domain	CMMC Level	CMMC Practice	NIST 800-171 Control	NIST 800-53 Control	Practice Requirement	Verification Method	Deliverable	Verification Frequency	Responsible Party
Access Control	1	AC.L1-3.1.20	3.1.20	AC-20, AC-20(1)	Verify and control/limit connections to and use of external information systems.	NAC report	Record of review and export.	Monthly	SSO
Access Control	1	AC.L1-3.1.22	3.1.22	AC-22	Control information posted or processed on publicly accessible information systems.	Review company website(s) and press releases for FCI/CUI.	Record of review and findings.	Quarterly	FSO
Access Control	2	AC.L2-3.1.9	3.1.9	AC-8	Provide privacy and security notices consistent with applicable CUI rules.	Verify that only approved notification messages or banners are displayed.	Record of review.	Annually	SSO
Access Control	2	AC.L2-3.1.21	3.1.21	AC-20(2)	Limit use of portable storage devices on external systems.	Pull user list of exceptions and review to confirm use is still needed.	Record of review and export.	Monthly	SSO
Access Control	2	AC.L2-3.1.5	3.1.5	AC-6, AC-6(1), AC-6(5)	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Within change management utility, export AD users to show which groups they hold memberships to along with who is an admin and review for accuracy.	Record of review and export.	Monthly	SSO
Access Control	2	AC.L2-3.1.6	3.1.6	AC-6(2)	Use non-privileged accounts or roles when accessing non-security functions.	Review IPS/IDS report and export.	Record of review and export.	Monthly	SSO
Access Control	2	AC.L2-3.1.8	3.1.8	AC-7	Limit unsuccessful logon attempts.	Review GPO and confirm settings.	Record of Review and screenshot.	Semiannually	SSO

Timeline & Case Studies



Potential Timeline



- Readiness Assessment: 1-2 weeks ---- **SSE complimentary service**
- Gap Assessment: 4 weeks
- Remediation Project: 2-3 months from Gap Assessment
(will vary by specific needs/situation)
- Ongoing Support: 1-2 months from Gap Assessment
(can usually be done concurrently w/Remediation)

Total time from start to compliance?

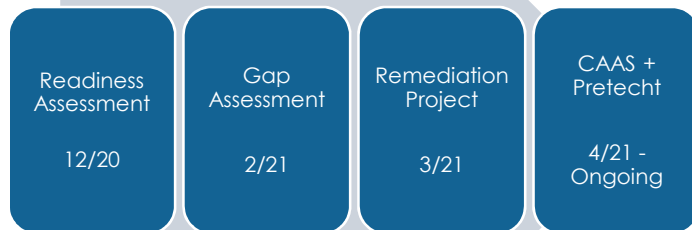
- 3-6 months for a mature IT environment
- 6-9 months for a non-mature IT environment

DoD Contractor Case Studies



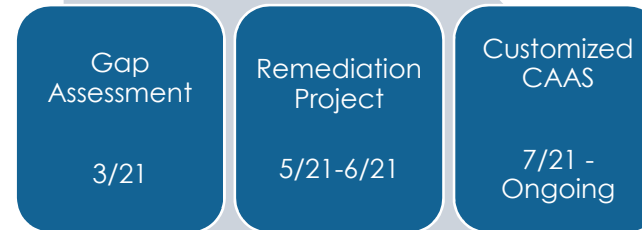
Company A

- 10-20 employees
- NIST Assessment score in negative triple digits (vs positive company submitted score)
- Hardware upgrade + policy project
- Comprehensive ongoing support



Company B

- 100+ employees
- Negative NIST Assessment score (vs positive company submitted score)
- Tailored remediation project with policy assistance
- Customized ongoing support



Thinking about DIY?

Key Findings from SSE Engagements



The average NIST 800-171 score based on SSE conducted assessments:

-94

The average discrepancy from a company scoring themselves vs after having an evidence-based assessment:

-108 points lower

The most common deficiency found during Gap Assessments:

Policy and procedure documentation

Submissions not done “in good faith” or completion dates not met are **risks** should a contract award be made with the submission on record

Wrap-Up and Q&A



- Do you have a System Security Plan (SSP)?
- Have you submitted a scored NIST 800-171 self-assessment to the DoD?
- Could you provide specifics supporting the above to your prime or the DoD if asked?
- Do you know when you need to be compliant/what you need to do to get there?
- Is your internal or external IT/cybersecurity support qualified or planning to become certified in these areas?
- Are you as a senior company official ready to affirm your compliance to NIST 800-171?

How do the recently announced draft changes to NIST 800-171 change what is required for my business and my compliance planning?

They don't.

Thank You

 9666 Olive Blvd, Ste 710
Saint Louis, MO 63132
 314-439-4769
 Robert.duffy@SSEinc.com

