NORTHROP GRUMMAN

Northrop Grumman's 2022 DIBCAC Joint Assessment Journey

High Level Overview Brief

Global Cyber Policy
Chief Information Office
June 2023

Presenter Biographies

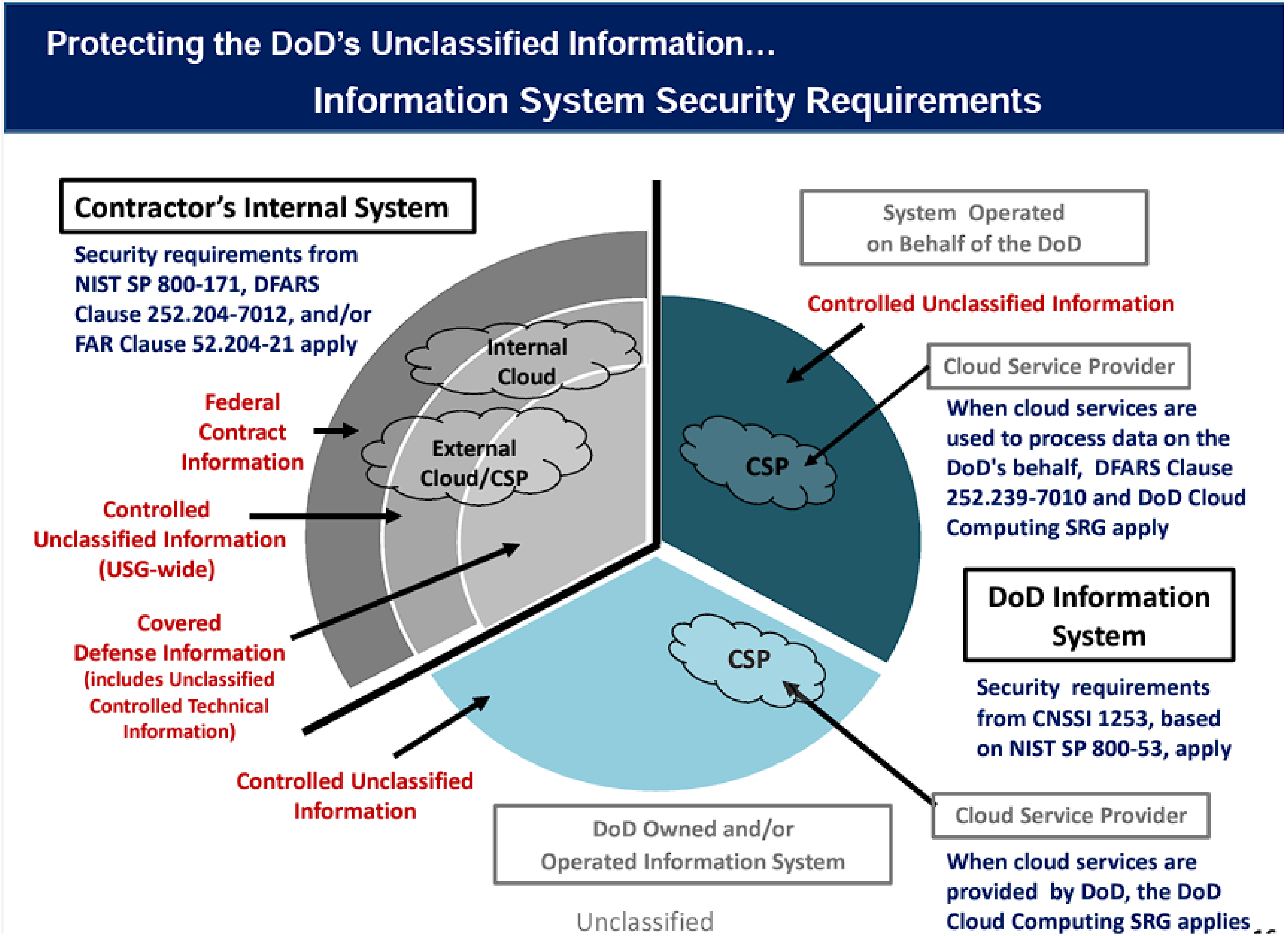
Dr. Thomas Autry has been working in the IT industry since 1996 at a variety of organizations from small businesses (<10 people) to large, Fortune 500 companies across several industries such as telecommunications, defense, retail, and financial encompassing a variety of roles (mechanical engineer, system engineer, project/program manager, virtualization engineer, system administrator, system implementer, cybersecurity engineer). He is currently a Staff Cyber Systems Engineer at Northrop Grumman. He obtained a BS and MS in Mechanical Engineering from the University of Oklahoma, MBA with an IT management focus from Western Governors University, and a Doctorate of IT in Information Assurance and Cybersecurity from Capella University. He has many industry certifications including CISSP, CCSP, CCSK, GSEC, PMP, ITIL, CCP, several cloud certifications (AWS, Azure) and numerous other technical certifications (UNIX, Linux, Solaris, AIX, VMWare). He is an active member of several external working groups and programs such as the Defense Industry Base Cybersecurity (DIB CS) program, the National Defense Industry Sharing and Analysis Center (NDISAC), and the DIB Sector Coordinating Council (DIB SCC). He also actively engages with other defense partners in the industry to identify and share best practices and lessons learned. He is also a volunteer with the Teaching Education and Learning Support (TEALS) program helping teach high school students introduction to Computer Science and Cybersecurity.

Table of Contents

- Regulatory Overview and Background
- JSP Overview
- NGC’s DIBCAC JSP Journey
- Post Assessment Survey
- Lessons Learned and Recommendations
- Final Thoughts
- Resource, Definitions and Acronyms

Regulatory Overview and Background

Overview: Protecting DoD’s Unclassified Information



Protecting the DoD’s Unclassified Information…

Information System Security Requirements

Contractor’s Internal System

Security requirements from NIST SP 800-171, DFARS Clause 252.204-7012, and/or FAR Clause 52.204-21 apply

Federal Contract Information

Controlled Unclassified Information (USG-wide)

Covered Defense Information (includes Unclassified Controlled Technical Information)

Controlled Unclassified Information

System Operated on Behalf of the DoD

Controlled Unclassified Information

Cloud Service Provider

When cloud services are used to process data on the DoD's behalf, DFARS Clause 252.239-7010 and DoD Cloud Computing SRG apply

DoD Information System

Security requirements from CNSSI 1253, based on NIST SP 800-53, apply

Cloud Service Provider

When cloud services are provided by DoD, the DoD Cloud Computing SRG applies

DoD Owned and/or Operated Information System

Approved for public release; NG23-1538. © 2023 Northrop Grumman Systems Corporation

Protecting U.S. Government Information: FCI

What is FCI?

- **FCI** is any U.S. Government information that is “not intended for public release” that is provided by or generated for the U.S. Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments. (FAR 52.204-21)

Key Regulation?

- FAR 52.204-21: Basic Safeguarding of Covered Contractor Information Systems requires the basic safeguarding requirements and procedures to protect covered contractor information systems.

Definition: “Covered contractor information system” means an information system that is owned or operated by a contractor that processes, stores, or transmits FCI.

Key Documents?

- None, 15 FAR controls map to 17 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 controls
- CMMC Level 1 Self-Assessment Guide

Protecting U.S. Government Information: CUI

What is CUI?

- **CUI** is Information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. Source: E.O. 13556 (adapted)

Key Regulation?

- DFARS 252.204-7012: Safeguarding Covered Defense Information (CDI) and Cyber Incident Reporting requires contractors who handle CDI on non-federal systems in performance of contracts to implement adequate cybersecurity safeguarding controls (NIST SP 800-171), rapidly report cyber incidents to the federal government within 72 hours of discovery, and to flow these requirements to their subcontractors who receive or generate CDI on their internal system.

Protecting U.S. Government Information: CUI (cont'd)

DFARS 252.204-7012 invokes the NIST Special Publication 800-171 standard also known as "**Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations**."

- In total, 800-171 has 110 unique security requirements that are split among 14 broader sections, or "families."
- Considering the volume and specificity of these requirements, any organization performing under contracts (or subcontracts) with the Defense Department must make sure that they have the requisite information security knowledge, expertise and resources to comply with NIST SP 800-171. Non-compliance, after all, could spell the end of a contractor's relationship with the DoD.
- Department of Defense Controlled Unclassified Information (DoD CUI) previously known as Covered Defense Information (CDI) is one example of CUI. In explaining what steps must be taken to protect CUI, the NIST guidelines cover the protection of DoD CUI or CDI as mandated by the DFARS clause 252.204-7012

JSP Overview

Northrop Grumman’s 2022 DIBCAC Joint Assessment Journey

Overview: NGC's 2022 DIBCAC Joint Assessment Overview

The objective of this brief is to provide an overview of Northrop Grumman Corporation's (NGC) experiences with the 2022 Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) Voluntary Joint Assessment including internal lessons learned, recommendations, and preparation guidance. These lessons learned, recommendations, and preparation guidance are for informational purposes only and are not a guarantee of success for other organizations.

Note: The information in this briefing is informational only and not a recommendation for other organizations on how to pass an assessment as each organization will have individual needs and requirements.

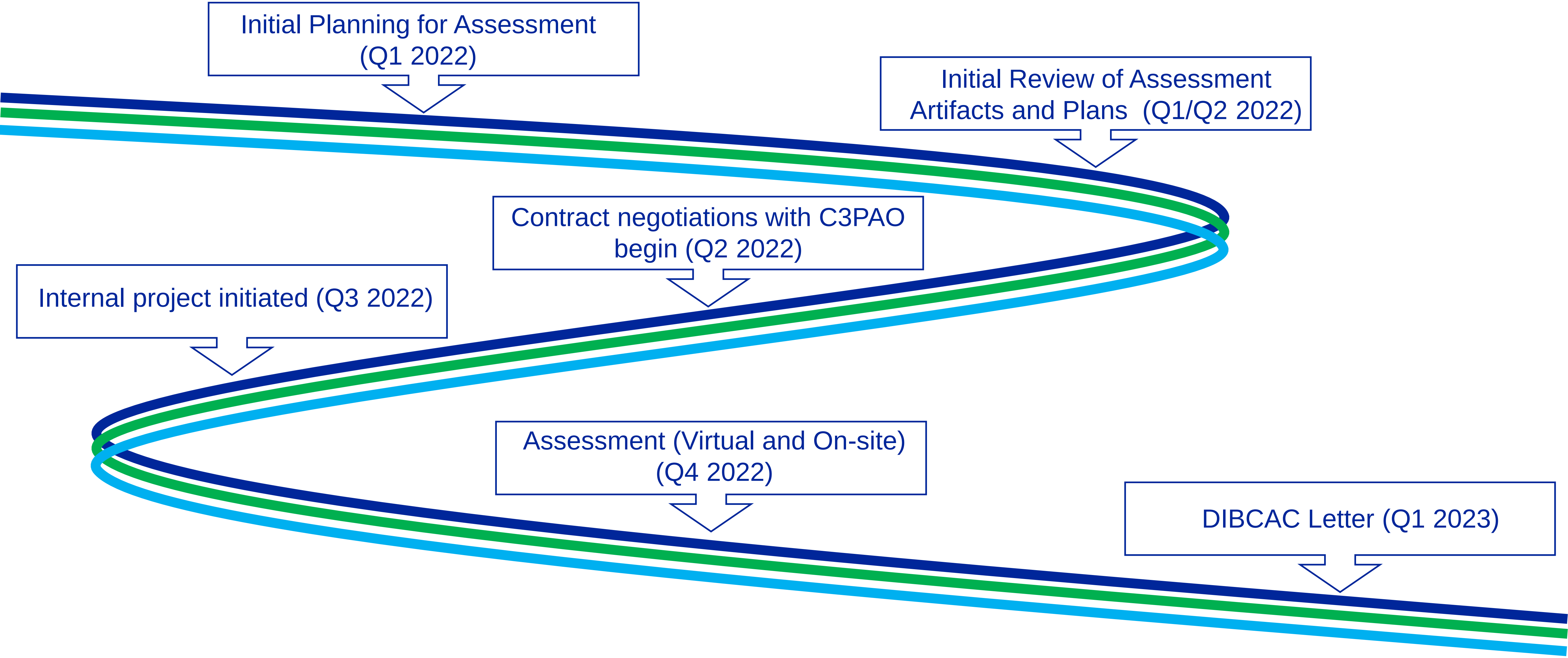
DIBCAC JSVAP (aka JSP) Background Information

- In early 2022, DCMA (Defense Contract Management Agency) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) and the CMMC Accreditation Body (Cyber AB) announced the DIBCAC Joint Surveillance Voluntary Assessment Program (JSVAP) (aka JSP)
- Allowed companies to be assessed against NIST SP 800-171 using the DIBCAC Scoring Methodology in a joint effort by the DIBCAC and an authorized Cybersecurity Maturity Model Certification (CMMC) Third Party Assessment Organization (C3PAO)
- Considered a DIBCAC High per the scoring methodology with the assessment score populated in the Supplier Performance Risk Management (SPRS) system
- Scores above 88/110 (80%) per the scoring methodology will be awarded a CMMC Level 2 (L2) certification upon final rulemaking
- The DIBCAC JSVAP started assessing organizations in August of 2022
- Northrop Grumman went through the DIBCAC JSP in Q4 of 2022

NGC’s DIBCAC JSP Journey

2022 DIBCAC Joint Assessment

NGC DIBCAC JSP Journey Highlights



Initial Planning for Assessment (Q1 2022)

Initial Review of Assessment Artifacts and Plans (Q1/Q2 2022)

Contract negotiations with C3PAO begin (Q2 2022)

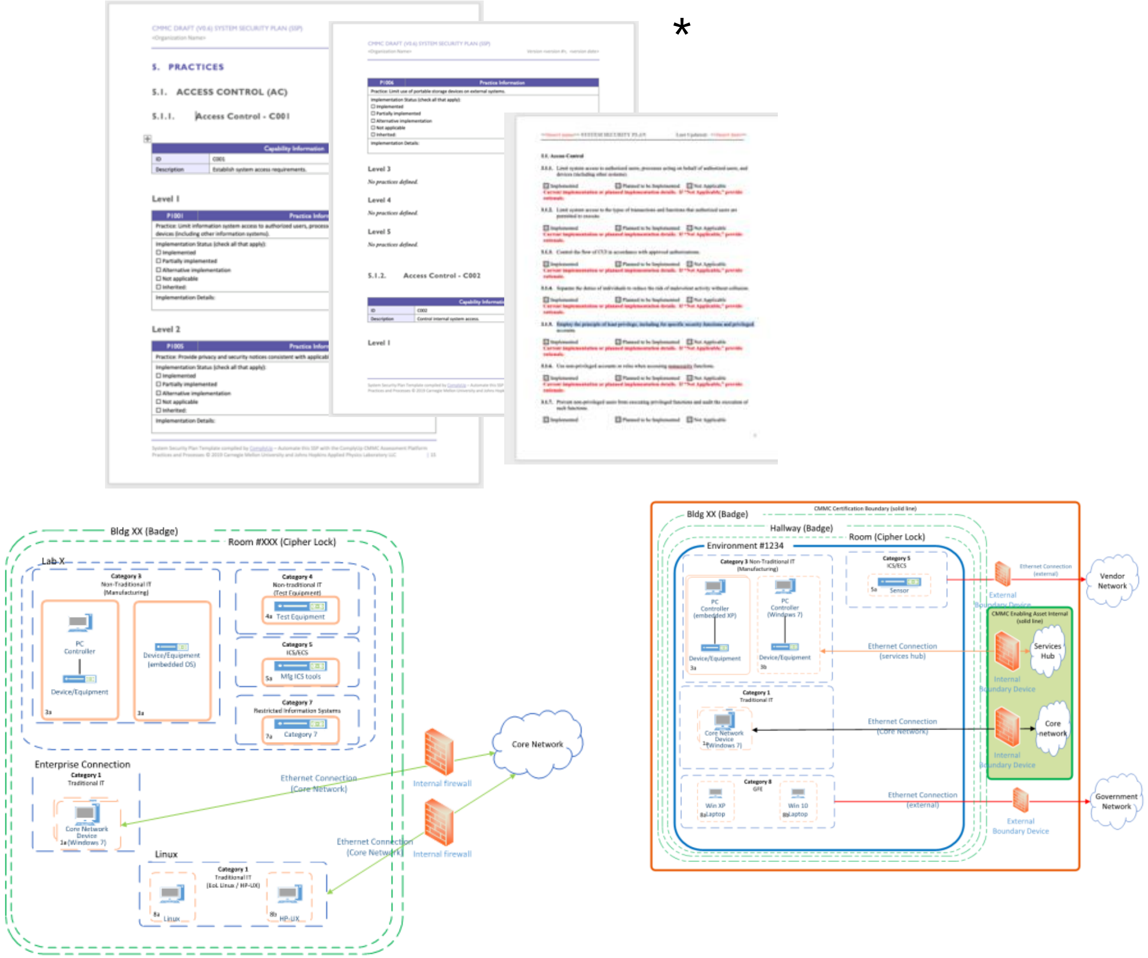
Internal project initiated (Q3 2022)

Assessment (Virtual and On-site) (Q4 2022)

DIBCAC Letter (Q1 2023)

Critical Artifacts for Showing Compliance within Defined Scope and Boundary

- System Security Plan (SSP)
  - Security technologies
  - Asset inventories (devices, users, etc.)
  - Detailed assessment objective answers
- Diagrams
  - Architectural
  - Network
  - Data Flow
- Policies and Procedures
  - Data identification and management
  - User identification and management
  - Change management
  - Configuration management



*

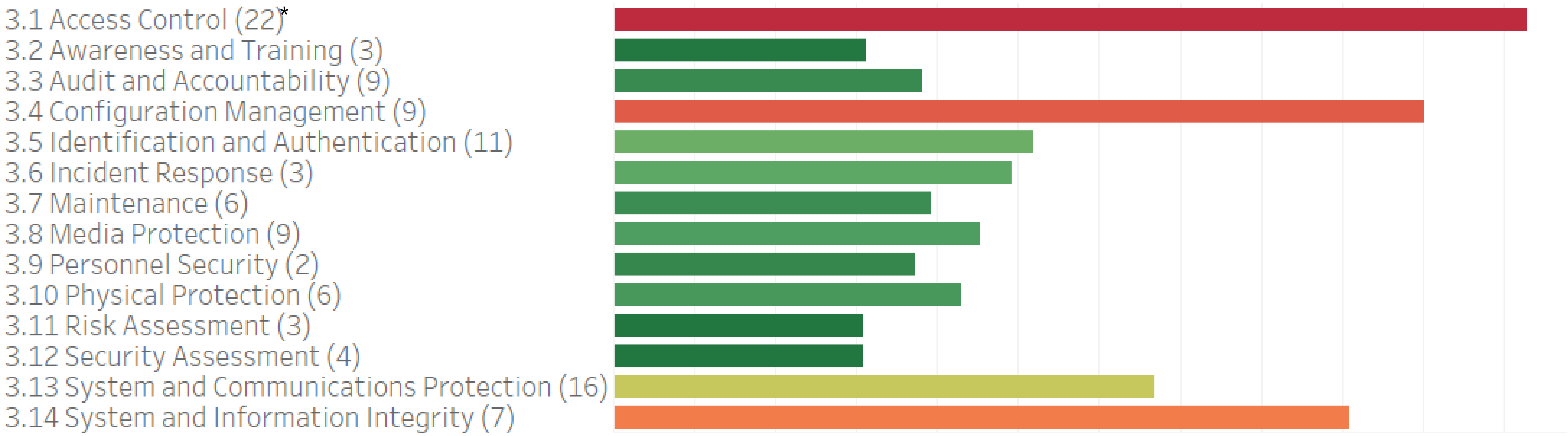
Figure 1: Generic Examples of Possible Artifacts

* NIST SSP and POAM Templates

Post Assessment Survey

2022 DIBCAC Joint Assessment

Time Spent by Control Family (Pre-Assessment)



*Number of Controls in domain

Time Spent by Task (Pre-Assessment)

Top Task per Working Role

Control Family Leads

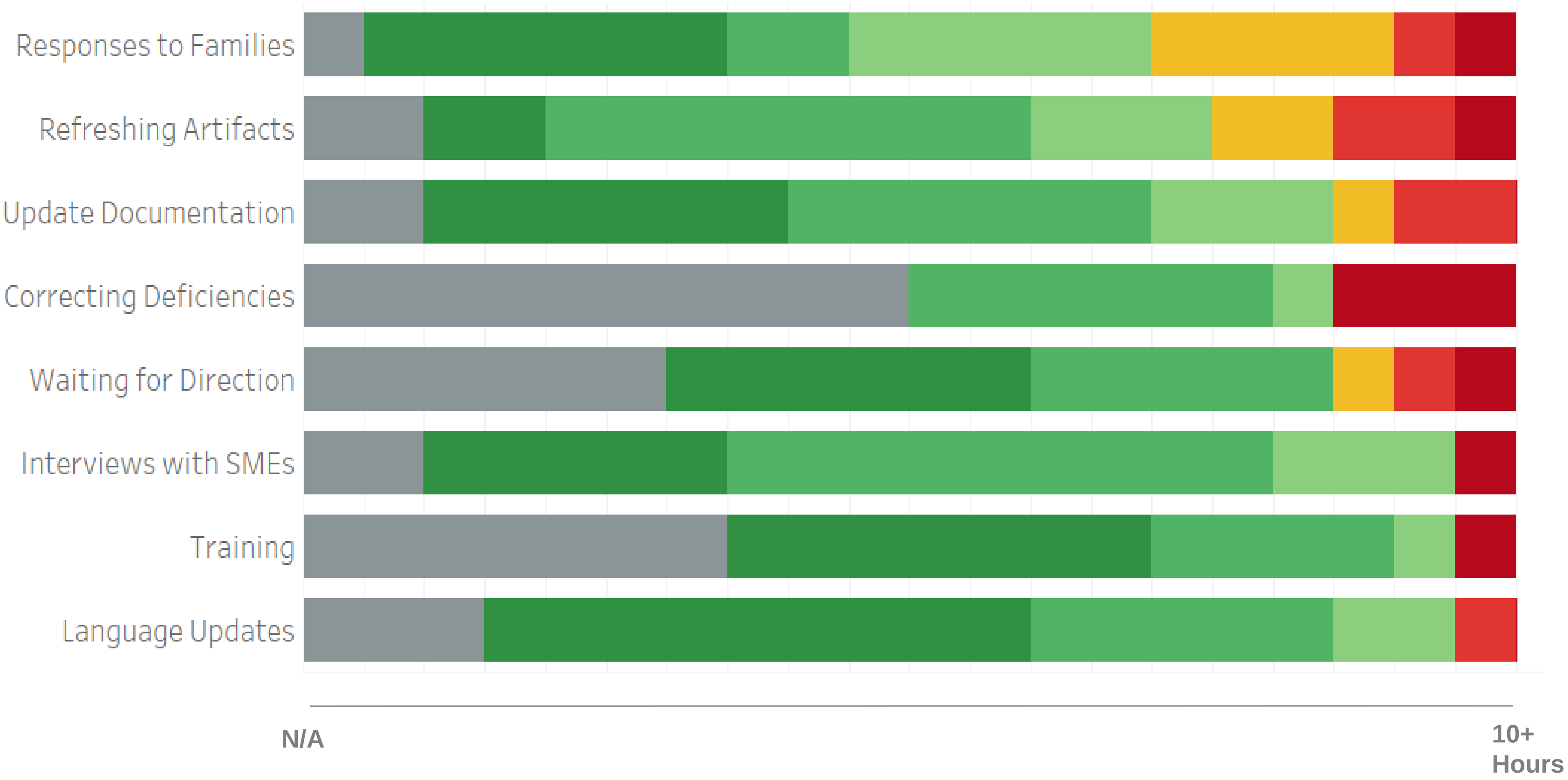
1. Refreshing Artifacts
2. Responses to Families
3. Updating Documentation

Leadership

1. Updating Documentation
2. Refreshing Artifacts
3. Interviews with SMEs

Subject Matter Experts

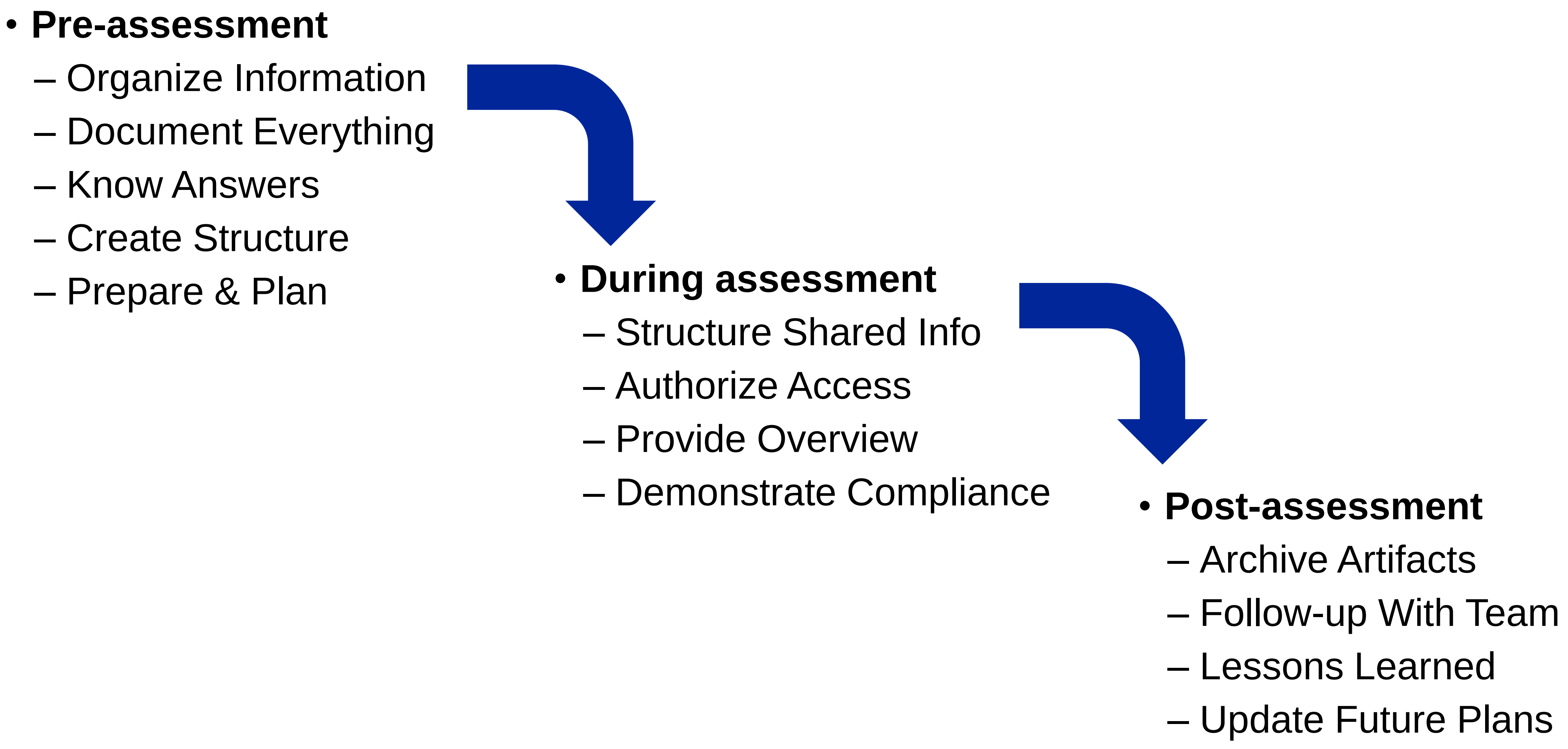
1. Updating Documentation
2. Responses to Families
3. Refreshing Artifacts



Lessons Learned and Recommendations

2022 DIBCAC Joint Assessment

Lessons Learned and Recommendations Summary



- **Pre-assessment**
  - – Organize Information
  - – Document Everything
  - – Know Answers
  - – Create Structure
  - – Prepare & Plan
- **During assessment**
  - – Structure Shared Info
  - – Authorize Access
  - – Provide Overview
  - – Demonstrate Compliance
- **Post-assessment**
  - – Archive Artifacts
  - – Follow-up With Team
  - – Lessons Learned
  - – Update Future Plans

Continual, consistent updates and engagement are critical for success.

Final Thoughts

Foundational Questions To Ask

- Do you have a list of all users, groups, devices, and required functionality/services?
- Do you know how data flows within and outside of your environment?
- Do you perform change management and configuration management?
- Do you have an SSP and is it updated regularly?
- Do you use MFA?
- Do you use any encryption?
- Do you have a complete list of what is identified as CUI and other contractual requirements?
- Do you have a complete list of applications?
- Can all the previous questions be proven with documentation and demonstration?
- Is documentation (SSP, change management, config management, user lists, inventory) updated regularly?

Recommendations

- Make sure to identify and set assessment scope and boundary
- Start early, especially the contracting portions
- Run as a project for accountability, ownership, deliverables, and timeline
- Identify what services, technologies, and software are used in the environment
- Be prepared to document everything
  - Required to identify and prove how every assessment objective is met
- Develop overview briefing(s) describing the identified scope and boundary and how it is protected
- Make sure SSP is up to date and matches documentation
- Identify contractual regulations especially what is identified as CUI and deliverables
- Documentation and demonstration are key to being successful
  - users, inventory, diagrams, configurations, FIPS certificates, etc.

Resources, Definitions and Acronyms

NORTHROP GRUMMAN

Resources

- CMMC Official Site: https://dodcio.defense.gov/CMMC/
- Cyber AB: https://www.cyberab.org/
- DoD Procurement Toolbox FAQs: https://dodprocurementtoolbox.com/faqs/cybersecurity
- NARA CUI Registry: https://www.archives.gov/cui
- DoD CUI Program and Registry: https://www.dodcui.mil/
- NDISAC CyberAssist: https://ndisac.org/dibscc/cyberassist/
- NIST SP 800-171: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST Cryptographic Module Validation Program (CMVP) (FIPS): Cryptographic Module Validation Program | CSRC (nist.gov)
- DCMA DIBCAC: https://www.dcma.mil/DIBCAC/
- Supplier Performance Risk System (SPRS): https://www.sprs.csd.disa.mil/

Definitions and Acronyms

Acronym	Full Name	Definition
C3PAO	CMMC Third Party Assessment Organization	An Entity that is certified to be contracted to and OSC to provide consultative advice OR certified assessments.
CMMC	Cybersecurity Maturity Model Certification	Set of standards established by the DoD against which an OSC is to be assessed.
CUI	Controlled Unclassified Information	Information that requires safeguarding or dissemination control pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended. Source: NIST SP800-171 Rev 2
DCMA	Defense Contract Management Agency	Agency that provides contract administration services for the Department of Defense, other federal organizations and international partners, and is an essential part of the acquisition process from pre-award to sustainment. (DCMA.mil)
DFARS	Defense Federal Acquisition Regulation Supplement	The DFARS provides DoD implementation and supplementation of the Federal Acquisition Regulation (FAR). The DFARS contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on the public. (osd.mil)
DIBCAC	Defense Industrial Base Cyber Assessment Center	Leads the Department of Defense's (DoD) contractor cybersecurity risk mitigation efforts. DIBCAC assesses DoD contractors' compliance with the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 as well as, the DFARS clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements. (DCMA.mil)
FAR	Federal Acquisition Regulation	The Federal Acquisition Regulations System is established for the codification and publication of uniform policies and procedures for acquisition by all executive agencies. (acquisition.gov)
JSVAP / JSP	Joint Surveillance Voluntary Assessment Program (JSVAP) (aka JSP)	The DIBCAC JSVAP allows companies to be assessed against NIST SP 800-171 using the DIBCAC Scoring Methodology in a joint effort by the DIBCAC and an authorized Cybersecurity Maturity Model Certification (CMMC) Third Party Assessment Organization (C3PAO)
POAM /POA&M	Plan(s) of Action and Milestones	A document that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, milestones for meeting the tasks, and the scheduled completion dates for the milestones. (nist.gov)
RPO	Registered Provider Organization	An organization authorized to represent itself as familiar with the basic constructs of the CMMC Standard, with a CMMC-AB provided logo, to deliver non-certified CMMC Consulting Services. Signifies that the organization has agreed to the CMMC-AB Code of Professional Conduct.
SPRS	Supplier Performance Risk System	The authoritative source to retrieve supplier and product PI (performance information) assessments for the DoD acquisition community to use in identifying, assessing, and monitoring unclassified performance." (DoDI 5000.79)

Questions

NORTHROP
GRUMMAN