There are three levels of assessments, according to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DoD Assessment Methodology[[1]](#endnote-1) (found at <https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171>), which are reflective of the depth and confidence level of each: Basic, Medium, and High. The High Assessment has virtual[[2]](#endnote-2) and on-site portions.

Please ensure that the items below are available to the assessment team in advance of the assessment. The DIBCAC will conduct a pre-assessment coordination meeting at least five weeks prior to the assessment to address any questions and to coordinate logistics information.

**Action Items Applicable to Medium and High Assessments**

* Perform a Basic (Self) Assessment of identified system security plan(s), in accordance with NIST SP 800-171 DoD Assessment Methodology.
* Provide Basic (Self) Assessment results to DIBCAC, to include the total score for each system/system security plan assessed (e.g., 105 out of 110), and the date that a score of 110 is expected to be achieved for each system security plan assessed (i.e., all requirements implemented).
  + Use Commercial and Government Entity (CAGE) Code Info (Enclosure 2) to provide the below information from your Basic Assessment to the DIBCAC prior to the pre-assessment coordination meeting.
    - System security plan (SSP) name and date
    - All CAGE Codes supported by the SSP
    - Date of your Basic Assessment
    - Summary level score
    - Date that a score of 110 is expected to be achieved for SSP assessed
  + Input the Basic Assessment score in the Supplier Performance Risk System (SPRS).
    - Go to the Procurement Integrated Enterprise Environment (PIEE) website: <https://piee.eb.mil/piee-landing/> to access SPRS.
    - Follow the link for Vendors to create an account if it does not already exist.
    - If your company has a PIEE account, work with your company Contractor Administrator (CAM) to add the appropriate “SPRS Cyber Vendor Role” required to input the SPRS Basic Assessment score data.
* Provide system security plan(s) and any associated Plan(s) of Action for any requirements “not implemented” per your Basic Assessment, to enable DIBCAC to assess compliance with NIST SP 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.” The SSP must be able to clearly address how each of the 110 security requirements found in the NIST SP 800-171 are implemented within your enterprise, and demonstrate that the company correctly understands each of the security requirements. Based on the elements to make a system security plan successful, it should include:
  + General system description
  + Description of system boundaries
  + System environments of operation
    - Major applications
    - General support systems
    - Minor applications
  + Description of how each of the 110 security requirements are implemented
    - Simply copying/pasting the requirement verbiage from the NIST SP 800-171 would not be acceptable
    - If a policy or technology/tool is referenced, there should be an explanation of how it ties directly to the requirement
    - For Medium Assessments (SSP review only), if the SSP does not clearly demonstrate how a requirement is met, that requirement will be scored as “Not Implemented”
    - For High Assessments, supporting documentation referenced in the SSP should be made available to the Assessment Team.
  + Relationships with/or connections to other systems (including other mission partners)
  + Revision history

**Action Items Applicable to High Assessments Only**

* Provide a detailed Network Topology Diagram/Network Enterprise Overview Briefing (to include a high-level operational concept graphic, or OV-1), and diagram of the corporate enterprise network unclassified system that has Controlled Unclassified Information (CUI) traversing it, to aid in the DIBCAC’s understanding of how enterprise services protect CUI. This diagram must depict the network topology and security posture of the enterprise information systems or network enclave that processes CUI data. The drawing/overview briefing must clearly delineate (as applicable):
  + Security boundaries
  + Cybersecurity stack
  + Security event information management
  + Connections to other systems/networks
  + Cloud interconnections/data flow
  + Wireless (Institute of Electrical and Electronics Engineers (IEEE) standard 802.11)
  + Dedicated point-to-point connections
  + Multi-Protocol Label Switching (MPLS) clouds
  + High-level Internet Protocol (IP) address schema
  + Critical network enterprise services
  + Vulnerability scanning methodology
  + Authentication methodology
  + Enterprise logging
  + Remote access
  + How a remote user browses the web (web content filtering)
  + Domain Name Service
  + VoIP (Voice over Internet Protocol)
  + Video
  + Any other relevant information to allow the assessors to determine if your corporation is truly protecting CUI as a single (or more than one) enterprise enclave
* Provide artifacts for requirements that are met by a document such as a policy, process, or manual log.
* Demonstrate how the organization manages contractual (lower level) SSPs. DIBCAC will assess the organization’s ability to protect CUI at an enterprise level to cover as many contracts as practicable which inherit NIST SP 800-171 requirements from the enterprise. Since the DFARS clause 252.204-7012 requires covered contractor information system(s) to be subject to the security requirements in NIST SP 800-171, DIBCAC will need to understand how the corporation provides governance over this process, and will use a sample of contracts to ensure the enterprise mechanisms, policies, procedures and requirements flow down to the contract level.
* DIBCAC requests access to the following:
  + Members of the policy team tasked with maintaining policies which ensure cybersecurity compliance of DFARS clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting.*
  + Internal audit members tasked with responsibilities in cybersecurity, specifically DFARS clause 252.204-7012 compliance
  + Internal audit records showing governance associated with DFARS clause 252.204-7012
  + A trace from the enterprise SSP to individual contracts
  + Policies and procedures for implementing DFARS clause 252.204-7012 when the contract uses isolated networks or labs
  + Artifacts to support governance at the contract level
* In addition to the NIST SP 800-171 requirements of the DFARS clause 252.204-7012, DIBCAC will need to verify compliance with the additional requirements of the clause (cloud computing, cyber incident reporting, and cyber incident damage assessment activities).
* Recommend Subject Matter Experts who can demonstrate implementation and answer questions; they should be available for the interviews for each security family. Examples of positions/personnel:
  + Network Administrator/Engineer
  + Employees with audit and accountability responsibilities
  + Cybersecurity/Information Technology policy oversight
  + Account Management
  + Personnel with information security responsibilities
  + System Developers
  + Personnel with access enforcement responsibilities
  + Risk Assessment Team
  + Cyber Net Defender/Incident Response
  + Senior Information Security Officer
  + Personnel/Human Resources Specialist
  + Physical Security Specialist
  + Configuration Management
  + Enterprise Services Lead
  + Active Directory Administrator
* **(Virtual portion)** Ensure access and capability to utilize the agreed upon method of screen share. If the contractor has a collaboration tool preference, identify the tool before the pre-assessment coordination call.

\*NIST Special Publication 800-171A is a companion publication developed to support assessments of the CUI security requirements in NIST SP 800-171. As such, it is the primary and authoritative source of guidance for organizations conducting such assessments.

**Tentative Schedule for Pre- and Post-Assessment Items (High and Medium Assessments)**

* **5 Weeks Prior to Assessment:** DCMA pre-coordination call
* **14 Days Prior to Assessment Start:** DoD SAFE drop request sent
* **7 Days Prior to Assessment Start:** Material received by DCMA
* **NLT Assessment End Date:**  DCMA Out-Brief
* **14 Business Days After Assessment End Date:** Reclama period ends
* **NLT 60 Days After High Assessment End Date:** Results provided to company

**Tentative Schedule for High Assessments Only**[[3]](#endnote-3)

**Monday** 0800 – 0830 Arrival / In-processing security **(on-site)** and Connectivity Tests/ Troubleshooting **(virtual)**

0830 – 1000 Room 1 - DCMA / Company In-Briefs

1000 – 1200 Room 1 - System Security Plan & Additional Documentation Review

1200 – 1300 Lunch

1300 – 1600 Room 1 - System Security Plan & Additional Documentation Review

1600 – 1630 Afternoon Artifact Request and Hot Wash (daily summary)

**Tuesday** 0800 – 0805 Arrival **(on-site)** and Connectivity Tests/Troubleshooting **(virtual)**

0805 – 1200 Room 1 - 3.1, 3.3, 3.5 Requirements

Room 2 - 3.2, 3 9, 3.10, 3.11, 3.12 Requirements

Room 3 - 3.4, 3.7, 3.8 Requirements

1200 – 1205 Morning Artifact Request

1200 – 1300 Lunch

1300 – 1530 Room 1 - 3.1, 3.3, 3.5 Requirements

Room 2 - 3.2, 3 9, 3.10, 3.11, 3.12 Requirements

Room 3 - 3.4, 3.7, 3.8 Requirements

1530 – 1600 DCMA Internal Discussion

1600 – 1630 Afternoon Artifact Request and Hot Wash (daily summary)

**Wednesday** 0800 – 0805 Arrival **(on-site)** and Connectivity Tests/Troubleshooting **(virtual)**

0805 – 1200 Room 1 - 3.6, 3.13, 3.14 Requirements

Room 2 - 3.2, 3 9, 3.10, 3.11, 3.12 Requirements

Room 3 - 3.4, 3.7, 3.8 Requirements

1200 – 1205 Morning Artifact Request

1200 – 1300 Lunch

1300 – 1530 Room 1 - 3.6, 3.13, 3.14 Requirements

Room 2 - 3.2, 3 9, 3.10, 3.11, 3.12 Requirements

Room 3 - 3.4, 3.7, 3.8 Requirements

1530 – 1600 DCMA Internal Discussion

1600 – 1630 Afternoon Artifact Request and Hot Wash (daily summary)

**Thursday** 0800 – 0805 Arrival **(on-site)** and Connectivity Tests/Troubleshooting **(virtual)**

0805 – 1200 Room 1 - Requirements Follow-ups

Room 2 - Requirements Follow-ups

Room 3 - Requirements Follow-ups

1200 – 1205 Final Artifact Request (if required)

1200 – 1300 Lunch

1530 – 1600 DCMA Internal Discussion and/or Out-Brief Prep

1530 – 1630 Room 1 - DCMA Out-Brief and Discussion (Hot Wash if assessment not complete)

**Friday**   
*(if needed)* 0800 – 0805 Arrival **(on-site)** or Connectivity Tests/Troubleshooting **(virtual)**

TBD Room 1 - Alternate time for DCMA Out-Brief and Discussion

1. Current as of time of assessment [↑](#endnote-ref-1)
2. High Assessments require screen share capabilities through the use of an agreed-upon method of screen share such as the government’s MS Teams or the company’s virtual collaboration tools (i.e., ZoomGov, WebEx, etc.). Collaboration tools will be addressed during the pre-assessment coordination call and specifics will be provided to DCMA DIBCAC and/or the company prior to the assessment start. The Assessment Lead will schedule a time to test connectivity prior to the assessment start. [↑](#endnote-ref-2)
3. This Tentative Schedule applies to High Assessments only and is subject to change at the discretion of the Assessment Lead. [↑](#endnote-ref-3)