Procure-to-Pay Capability Summary

PUBLICATION DATE: September 25, 2023

SUBJECT: Documenting DoD Cybersecurity Assessments in the Supplier Performance Risk System (SPRS)

BACKGROUND: Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, requires contractors and subcontractors to implement the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations, when covered defense information resides on, or transits through, the contractor's or subcontractor's internal information system.

The Defense Contract Management Agency's (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) conducts a limited number of moderate- and high confidence assessments of information technology (IT) system security plans (SSP). A majority of contrators will perform a low confidence (self-assessment) of their SSPs using the NIST SP 800-171 DoD Assessment Methodology. Assessments are valid for three (3) years. If the assessment score is less than 110, the contractor is required provide the date they estimate attaining a score of 110. Prime contractors are also mandated to verify that their subcontractors have also completed these assessments, if handling CUI.

Contracting officers are required to verify that current and prospective government contractors who will handle controlled unclassified information (CUI) have valid results of a NIST SP 800-171 cybersecurity assessment posted in SPRS prior to contract award or option exercise. Contracting officials search SPRS by CAGE during preaward activities. CAGEs covered by a valid assessment are eligible for award.

POLICY: DFARS clause 252.204–701 requires contractors to apply the security requirements of NIST SP 800– 171 to ‘‘covered contractor information systems.’’ DFARS 252.204–7019/7020 contains assessment requirements for prime contractors and subcontractors. DFARS 204 instructs contracting officers to verify cybersecurity assessment results in SPRS.

DATA STANDARDS: SPRS retains cybersecurity assessment results as entered by contractors or government employees from DCMA's DIBCAC. SSP documents are not uploaded into SPRS.

INFORMATION TECHNOLOGY INFRASTRUCTURE: NIST SP 800-171 DoD Assessment results are posted in SPRS and protected in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI). SPRS is centrally hosted at the Defense Information Systems Agency (DISA), leveraging a virtual operating environment. SPRS also leverages the single sign on capabilities of the Procurement Integrated Enterprise Environment (PIEE) platform to provide government and contractor personnel system access.

IMPACT: DoD Components may rely on NIST SP 800-171 DoD Assessment results posted in SPRS in lieu of including requirements to assess implementation of NIST SP 800-171 on a contract-by-contract basis.

CONTACT: Mae Bartley, OUSD (A&S)/DPC at 703-697-4420, mae.k.bartley.civ@mail.mil
John Duncan, NSLC-Portsmouth, NH at 207-438-6481, john.c.duncan3.civ@us.navy.mil