OFFICE OF THE UNDER SECRETARY OF DEFENSE

3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION
AND SUSTAINMENT

MEMORANDUM FOR COMMANDER, UNITED STATES CYBER
COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES SPECIAL OPERATIONS
COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES TRANSPORTATION
COMMAND (ATTN: ACQUISITION EXECUTIVE)
DEPUTY ASSISTANT SECRETARY OF THE ARMY
(PROCUREMENT)
DEPUTY ASSISTANT SECRETARY OF THE NAVY
(PROCUREMENT)
DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE
(CONTRACTING)
DIRECTORS, DEFENSE AGENCIES
DIRECTORS, DEFENSE FIELD ACTIVITIES

SUBJECT: Supplier Performance Risk System for National Institute of Standards and Technology Special Publication 800-171 Department of Defense Assessment

Defense Federal Acquisition Regulation Supplement 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 in Nonfederal Systems and Organizations, when covered defense information resides on, or transits through, the contractor's or subcontractor's internal information system. Over the last year, the Defense Contract Management Agency's (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) has conducted over 70 Assessments of the Defense Industrial Base covering over 500 Commercial and Government Entity Codes with total contract value exceeding 1.5 trillion dollars.

The Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) memorandums, "Strategically Implementing Cybersecurity Contract Clauses," dated February 5, 2019, and, "Assessing Contractor Implementation of Cybersecurity Requirements," dated November 14, 2019, direct that assessment results be documented in the Supplier Performance Risk System (SPRS). A recent update to the assessment methodology, driven by the Department's response to COVID-19, is available at: https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf.

In May 2020, SPRS updated existing functionality designed to document, store, and retrieve summary results from the NIST SP 800-171 Department of Defense (DoD) Assessments. With this deployment, authorized representatives of the contractor may enter results for Basic (self) assessments. DCMA's DIBCAC may enter summary results for Medium and High assessments. DoD Components already have visibility into the results of these assessments. All Defense Components should use this enterprise information in assessing cyber security readiness for industry NIST 800-171 implementation. Detailed information for this module, as well as other capability deployed in SPRS, can be found at https://www.sprs.csd.disa.mil and in Attachment 1.

Please direct SPRS policy questions to my point of contact, Ms. Mae Bartley, at 703-697-4420 or mae.k.bartley.civ@mail.mil. Operational SPRS questions should be directed to John Duncan at john.c.duncan@navy.mil. Questions regarding NIST SP 800-171 DoD Assessments should be directed to Darren King at darren.j.king.civ@mail.mil. Questions regarding the NIST SP 800-171 DoD Assessment Methodology should be directed to Kevin Dulany at kevin.m.dulany.civ@mail.mil.

HERRINGTON.KIM.1507719313

Digitally signed by HERRINGTON.KIM.1507719313
Date: 2020.07.01 13:50:33 -04'00'

Kim Herrington,
Acting Principal Director,
Defense Pricing and Contracting

Attachment:
As stated

## Attachment 1 – SPRS Capabilities

The Supplier Performance Risk System (SPRS) uses contractor performance information (PI) from Department of Defense (DoD) components and federal agencies to provide acquisition professionals with timely and relevant information for acquisition decisions. Capabilities within SPRS include the following:

**Quality & Delivery Scores** – Contractors are scored by commercial and government entity (CAGE) code on their contract deliveries.

**Risk Tools** – SPRS provides risk analysis in three areas, item risk, price risk, and supplier risk.

- Price Risk – Calculates an item's average price paid and identifies risk for under-pricing and over-pricing.
- Item Risk – Flags items identified as "High Risk" due to critical safety use, increased risk of suspected counterfeiting or material failures, and other reasons identified by components.
- Supplier Risk – Scores over 63,000 vendors each day based on contract performance factors from various data sources.

SPRS aggregates risk analyses for different uses to include Procurement Risk, Market Research and Supplier Surveillance.

**National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DoD Assessments** – Displays "Basic" assessments as entered by contractors and "Medium and High" assessments conducted by the Defense Contract Management Agenc, including all CAGEs subject to a system security plan.

**Business Segment Structure** – Provides corporate hierarchies arranged by CAGE, declared by contractors.

**Vendor Threat Mitigation/Section 841** – Provides a common platform for vendor-vetting, using intelligence community threat assessments and combatant command threat ratings.

**National Security System (NSS) Restricted List** – Provides a list of contractors and covered products not authorized for use by DoD.

**Enhanced Vendor Profile** – Enables supply chain risk management/illumination environment using government and commercial data sources. Features Company Profile, Supply Chain mapping, Contract activity by sector, component, obligations, and News feeds of DoD actions.