University of Dayton Research Institute

SUBCONTRACTOR CERTIFICATION – PART 2 FORM

NIST 800-171 DoD Assessment Requirements

Effective 30 November 2020, three new DFARS regulations further define DoD contractor obligations to protect Department of Defense (DoD) Controlled Unclassified Information (CUI):

- DFARS 252.204-7019, Notice of NIST SP800-171 DoD Assessment Requirements
- DFARS 252.204-7020, NIST SP800-171 Assessment Requirements
- DFARS 252.204-7021, Cybersecurity Maturity Model Certification Requirements

DFARS 252.204-7019 and DFARS 252.204-7020 require that all contractors have and maintain a current assessment score (less than three years old, using the DCMA assessment methodology) in the DoD Supplier Performance Risk System (SPRS). ***The regulations also require that, prior to awarding subcontracts involving CUI, prime contractors must confirm that subcontractors have a current assessment score in SPRS. In addition, the DFARS 252.204-7021 clause officially implements DoD's adoption of the Cybersecurity Maturity Model Certification (CMMC).*** The purpose of this questionnaire is to understand the capabilities and the depth of understanding of a supplier's information system(s) Cyber Security. Ref. NIST SP 800-171 & CMMC V1.02

Requested Actions

To avoid disruptions to future business and subcontracting actions with its subcontractors / suppliers the University of Dayton Research Institute (UDRI) requests that your organization answer the questions below and return this completed certification. Please respond considering all the information system(s) utilized in support of UDRI prime contracts.

Subcontractor Company Information

Supplier Name:	
Supplier Street Address:	
City, State, Zip:	
Date of this survey:	
SPRS Registration Complete?	YES □ NO □
Date of Complete Registration:	
CAGE Code used in Registration:	
Assessment Score:	
Confidence Level:	

Controlling Documents: NIST SP 800-171 & CMMC V1.2		YES	NO
1.	Is the supplier CMMC certified? If not, when is the Planned Certification Date? Details:	□	□
2.	Does the supplier have a System Security Plan (SSP) and Plan of Action and Milestones (POAM) in place? Details:	□	□
3.	Has the supplier notified the DoD of their status and do they have a plan to notify in the event of an incident? *(Notified DoD and have copy of DoD letter* *Incident-handling procedure in place for CUI spills, including participants)* Details:	□	□
4.	Does the supplier have a structured ITS support? *(e.g. Internal personnel or outsourced - domestic, team/individual for: network support, server support, DBA, log monitoring, etc.?)* Details:	□	□
5.	Does the supplier perform employee and contractor background checks and drug testing? (*Random or initial hire)* Details:	□	□
6.	Does the supplier have employee security training? *(New Employee Orientation, Email and Internet usage)* Details:	□	□

Controlling Documents: NIST SP 800-171 & CMMC V1.2		YES	NO
7.	*3.1.1* Does the supplier limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)? *(Examples: via MFA (Multi-Factor Authorization e.g. password and token), no shared/group passwords, access is monitored, access promptly removed for terminated employees or contractors, no Guest or Anonymous accounts)* Details:	□	□
8.	*3.1.2* Does the supplier limit information system access to the types of transactions and functions that authorized users are permitted to execute? *(One method of achieving this is defining access privileges by account or system account type. System account types include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, temporary, etc.)* Details:	□	□
9.	*3.1.6* Does the supplier use privileged and non-privileged accounts or roles to limit access between secure and non-secure functions - Staff or contractors with privileged accounts all have non-privileged accounts as well, that are used for non-privileged commands or activities? *(Example of privileged, or security functions: installing/removing software, disabling security controls changing system configuration, viewing/deleting activity logs, or accessing restricted directories. When not performing these tasks, the owner of a privileged account would use their non-privileged account, to avoid allowing an attacker to hijack their session and use the privileges to pivot into the network or install malware)* Details:	□	□
10.	*3.1.12* Does the supplier allow, monitor, and control remote access sessions? What endpoint security measures are in place? *(This would be access of the supplier's network via VPN, either using a client or using a browser to access the VPN portal on the supplier's network.)* Details:	□	□

Controlling Documents: NIST SP 800-171 & CMMC V1.2		YES	NO
11.	*3.1.16* Does the supplier authorize wireless access prior to allowing such connections? *(Encryption is set to at least WPA2)* Details:	□	□
12.	*3.1.18* Does the supplier control connection of mobile devices? *(Example: passcode expiration, encryption via Wireless Access Points, using WPA2 or stronger encryption, or mobile devices, primarily cell phones and tablets, must access the network via a Mobile Device Management platform such as Airwatch, etc.)* Details:	□	□
13.	*3.1.20* Does the supplier verify and control/limit connections to and use of external systems? Describe the systems in place. *(External systems are generally Internet destinations or networks not controlled by the Supplier – e.g. Dropbox, Gmail, Facebook, Amazon, etc., especially where this could be a conduit for data exfiltration)* Details:	□	□
14.	*3.1.22* Does the supplier control information posted or processed on publicly accessible information systems? *(For example, only select individuals are authorized to post CUI onto publicly accessible systems and the content of such information is reviewed prior to posting to ensure that nonpublic information is not included.)* Details:	□	□
15.	*3.3.1* Does the supplier 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? *(Event types to be included in audit logs may include password changes, failed logons or failed accesses related to systems, administrative privilege usage, or third-party credential usage. As well as time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, filenames involved, and access control or flow control rules invoked etc.)* Details:	□	□

Controlling Documents: NIST SP 800-171 & CMMC V1.2		YES	NO
16.	*3.3.3* Does the supplier review and update logged events? *(A.I. software, consultant, ITS staff)* Details:	□	□
17.	*3.4.3* Does the supplier track, review, approve or disapprove, and log changes to organizational systems (e.g., through a formal change control/management program)? *(Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Processes for managing configuration changes to systems include review and approval of proposed changes to systems. Audit logs of changes include activities before and after changes are made to organizational systems and the activities required to implement such changes.)* Details:	□	□
18.	*3.4.7* Does the supplier restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services on IT systems? *(Disables or removes nonessential applications, services, etc. on workstations, and has a configuration template for servers that does similar functions and monitors the network via vulnerability scans or network logs to detect activity from these objects)* Details:	□	□
19.	*3.5.1 & 3.5.2* Does the supplier identify system users, processes acting on behalf of users, or devices and how do they authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational information systems? *(Device identifiers include Media Access Control (MAC), Internet Protocol (IP) addresses, or device-unique token identifiers. Typically, individual identifiers are uniquely assigned usernames associated with system accounts.)* Details:	□	□

Controlling Documents: NIST SP 800-171 & CMMC V1.2		YES	NO
20.	*3.5.7* Does the supplier enforce a minimum password complexity, change of characters, and frequency of change? *(Requirements may include a character minimum, encouraging use of passphrases (MyRobin58Pumpkin#) w/ upper and lower case, numbers, and special characters. Passwords expire every 30 days and cannot be re-used for the last 5 times. Controls in place block passwords such as 'password123', 'asdfghjkl', and similarly easy-to-guess passwords)* Details:	□	□
21.	*3.6.1* Has the supplier established an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities? *(System with published policy/procedure for incident-handling, opening a trouble-ticket, assigning support personnel, distributing status updates to stakeholders, conducting post-incident reviews. Operational incidents would be, for example: production file server is down, network link is broken, firewall is not passing traffic, remote users can't logon, etc.)* Details:	□	□
22.	*3.7.1* Does the supplier perform routine maintenance on organizational systems? (*This requirement addresses the information security aspects of the system maintenance program and applies to all types of maintenance to any system component (including hardware, firmware, applications) conducted by any local or nonlocal entity.)* Details:	□	□

Controlling Documents: NIST SP 800-171 & CMMC V1.2		YES	NO
23.	*3.8.1* Does the supplier protect (i.e., physically control and securely store) system media? *(Back up production systems regularly and the backup media are stored in a restricted-access area on-premises, or offsite with a data protection service. Disk drives, particularly on workstations, are encrypted. System media (e.g. disk drives) for decommissioned equipment are destroyed or else sanitized using DoD-approved wiping methods)* Details:	□	□
24.	*3.8.3* Does the supplier sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse? *(Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal.)* *(Sanitization of non-digital media includes destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document.)* Details:	□	□
25.	*3.10.1* Does the supplier limit physical access to organizational systems to authorized individuals? *(Maintains production systems in restricted-access locations on-premises. Only specifically authorized staff (e.g. system administrators) are allowed access. Access is controlled electronically and is logged)* Details:	□	□
26.	*3.10.3* Does the supplier escort visitors and monitor visitor activity? (*Example: audit logs can be used to monitor visitor activity.)* Details:	□	□

Controlling Documents: NIST SP 800-171 & CMMC V1.2		YES	NO
27.	*3.10.4* Does the supplier maintain audit logs of physical access? *(Examples of audit logs are procedural, a written log of individuals accessing the facility, and automated, capturing ID provided by a PIV card.)* Details:	□	□
28.	*3.10.5* Does the supplier control and manage physical access devices? *(Includes keys, locks, combinations, and card readers)* Details:	□	□
29.	*3.12.1* Does the supplier periodically assess implemented security controls to determine if they are effective in their application throughout their life cycle? *(Organizations assess security controls in organizational systems and the environments in which those systems operate as part of the system development life cycle. By assessing the implemented security controls, organizations determine if the security safeguards or countermeasures are in place and operating as intended.)* Details:	□	□
30.	*3.13.1* Does the supplier monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems? *(Preserves firewall and IDS/IPS logs and forwards them to a SIEM. Alerts are sent to security personnel when unusual traffic is detected)* Details:	□	□
31.	*3.13.5* Does the supplier implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. *(Separated subnetworks, demilitarized zones (DMZ), are typically implemented with boundary control devices and techniques including routers, gateways, firewalls, virtualization, or cloud-based technologies.)* Details:	□	□

Controlling Documents: NIST SP 800-171 & CMMC V1.2		YES	NO
32.	*3.13.8* Does the supplier implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards, during storage and transfer of Data? *(Example of alternate physical safeguard is a protected distribution system (PDS) where the distribution medium is protected against electronic or physical intercept)* Details:	□	□
33.	*3.14.1* Does the supplier identify, report, and correct system flaws in a timely manner - system-patching policy in place, periodically runs vulnerability scans (or contracts a 3rd-person party to do them) and patches monthly, based on the results? Details:	□	□
34.	*3.14.2* Does the supplier provide protection from malicious code at appropriate locations within organizational information systems? *(Locations may include system entry and exit points such as, remote-access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Protection mechanisms include anti-virus signature definitions and reputation- based technologies.)* Details:	□	□
35.	*3.14.4* Does the supplier update malicious code protection mechanisms when new releases are available? *(Timely updates are preformed upon new releases to utilized protection mechanisms such as anti-virus signature definitions and reputation-based technologies.)* Details:	□	□

Controlling Documents: NIST SP 800-171 & CMMC V1.2		YES	NO
36.	*3.14.5* Does the supplier perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed? *(Periodic and real-time scans of files from external sources are used to detect malicious code that may be inserted into systems in a variety of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices)* Details:	□	□
37.	*3.11.1 e* Does the supplier subscribe to and analyze threat intelligence? a) If so, how frequently? *b)* Please list the source(s). *For example, US Cert (https://www.us-cert.gov/ics/alerts)* Details:	□	□
38.	*3.11.3* Does the supplier analyze and remediate vulnerabilities? *(When vulnerabilities are discovered the remediation level and effort are prioritized and executed with consideration to the related assessment of risk.)* a) If so, how frequently? *b)* Please list the tool(s) *(For example, NESSUS scanning)* Details:	□	□

Certification (signature) is required below by an authorized official verifying that your company has determined a basic assessment and submitted it in the DoD SPRS system per regulatory guidelines.

Survey completed by (name):	
Title:	
Email:	
Phone:	
Signature:	

Reference Websites and Addresses:	
Supplier Performance Risk System (SPRS)	https://www.sprs.csd.disa.mil/
DFARS 252.204-7008 through 252.204-7021	https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm
Cybersecurity Maturity Model Certification (CMMC)	https://dodcio.defense.gov/CMMC/
CMMC Model and Assessment Guides	https://dodcio.defense.gov/CMMC/Documentation/
NIST SP 800-171, Rev 2	https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

INTERNAL USE ONLY:

Eligible for CDI / CUI:	□ YES □ NO
Verification performed On-site or Virtually?	□ On-site □ Virtually
Review performed by:	
Date:	
COMMENTS:	