December 14, 2023

SUBJECT: Introducing Cybersecurity Compliance and Risk Assessment (CCRA)

Purpose: Introduces the concept of a common Cybersecurity Compliance and Risk Assessment (CCRA) for the Defense Industrial Base

The CCRA concept allows suppliers to complete ONE assessment which would be accepted on a reciprocal basis by DoD Prime contractors, or other companies who recognize the CCRA. This will introduce efficiencies and cost savings in contrast to current practices. As suppliers have observed, while the regulatory requirements for cybersecurity continue to grow and evolve, companies have resorted to developing proprietary assessments or using outdated questionnaires to capture compliance and risk information. This approach has introduced a significant burden to suppliers that are required to provide unique responses to assessment tools containing varying numbers of security requirements and inconsistent language.

The transition to the CCRA will introduce a consistent approach for acquiring cybersecurity compliance and risk information, will introduce a reduced set of required responses and introduce the efficiency of answering once and sharing with many who recognize the reciprocal value of the CCRA.

What is driving the change?

The primary drivers for this change include feedback from our suppliers who seek reduced administrative burden in documenting cybersecurity and risk information, coupled with supplier concern about meeting the DoD's compliance requirements. To address suppliers' input, the Defense Industrial Base (DIB) Sector Coordinating Council (SCC) Supply Chain Cybersecurity Task Force (SCCTF) created the CCRA Working Group to develop the CCRA as a common set of security requirements integrated into a single concise format to measure both risk and compliance.

What is the Cybersecurity Compliance and Risk Assessment?

The current version of the CCRA contains a maximum of 60 total questions and security requirements in a macro-enabled Excel file format. The file adjusts the number of required questions and security requirements based on responses in the compliance section of the CCRA. The risk assessment section is a subset of NIST SP 800-171 Rev 2 security requirements to ensure protection of sensitive information.

The CCRA is intended to be an industry-agnostic tool that will enable any company, regardless of size or scope, to effectively capture a baseline risk assessment for entities where sensitive data is shared. It should be noted, however, that completing the CCRA does not waive, or substitute for any DoD required assessments, or imply approval to host or process controlled unclassified information (CUI).

When will the CCRA be available?

The assessment will be available on December 14, 2023, from the National Defense Information Sharing and Analysis Center (ND-ISAC) website.

CCRA Deployment

Member companies who are part of the DIB SCC CCRA Working Group will begin piloting use of the CCRA following this general announcement.

Additional resources:

The National Defense Information Sharing and Analysis Center (ND-ISAC)[1] CyberAssist public website has information on the CCRA, FAQs and is the single source to download the CCRA.

Thank you for doing your part to help protect and secure the aerospace and defense industry and the customers who rely on us. Questions or feedback regarding the CCRA can be submitted to ccra@ndisac.org.

CCRA Working Group

LOCKHEED MARTIN

CENTURUM

L3HARRIS

leidos

NORTHROP GRUMMAN

RTX

COLLINS AEROSPACE | PRATT & WHITNEY | RAYTHEON

WIN-TECH INC

Additional Member Working Group companies: Accenture Federal Services, BAE Systems, Boeing, Booz Allen Hamilton, Frontgrade Technologies, Rolls Royce

[1] About the ND-ISAC: ND-ISAC is a non-profit, non-federal entity established and funded by its member companies to support their collective cybersecurity and resilience against all hazards through multiple lines of effort (e.g. secure cyber threat sharing, technical solution working groups, knowledge exchange events). The Defense Industrial Base Sector Coordinating Council (SIB SCC) designates ND-ISAC as its operational and administrative arm. To learn more about the DIB SCC or how to become a member company of the ND-ISAC please contact Info@ndisac.org.