CELERIUM™

CYBER DEFENSE SOLUTIONS

CMMC

October 4, 2021

Overview

1. Purpose and Intent of CMMC
2. Current Status
3. Key distinctions from previous DoD and current NIST Frameworks
    - DITSCAP/DIACAP/NIST 800-37/NIST 800-53/ NIST 800-171/172
    - CMMC Level 3
    - Differences between CMMC level 3 and NIST 800-171
4. Opportunities for Education and Training
    - Workforce Development
    - Evidence Based Program Evaluation and Research
        - Creating metrics
        - Evaluating your current cybersecurity implementation
        - Where can I find more information?

CELERIUM™

Purpose and Intent of CMMC

- DoD is migrating to the new CMMC framework in order to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB) sector.

- The CMMC is intended to serve as a verification mechanism to ensure that DIB companies implement appropriate cybersecurity practices and processes to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within their unclassified networks.

- Created to allow organizations a way to meet minimum-security requirements and address difficulties and missing items from the NIST SP 800-171 product.

CELERIUM™

Current Status of CMMC

- Interim Rule: The interim rule became effective on November 30, 2020. The public review and comment period for DFARS Case 2019-D041 ended on November 30, 2020. Due to its designation as a major rule change, the interim rule must also complete a Congressional Review.
- Version 1.0 was released Jan 2020, and 1.02 was released in March 2020.
- The CMMC-AB has been stood up, and a chairperson has been selected.
- The first set of provisional certifiers has been trained.
- Targeted assessments are ongoing
- Requirement should be included in some contracts soon.

CELERIUM™

Key Distinctions

Previous DoD and Current NIST Frameworks

- DITSCAP
- DIACAP
- NIST SP 800-37
- NIST SP 800-53
- NIST SP 800-171
- CMMC Level

CELERIUM™

Key Distinctions
Previous DoD and Current NIST Frameworks

CMMC Level 3 essential differences from NIST SP 800-171

CELERIUM™

Importance of workforce development

- # of attacks based on network users

Evidence-Based Program Evaluation and Research

- How to create metrics
  - Impartial assessment
  - Items that could be used to help create metrics:
    - NIST Practices/Controls
    - Key Performance Indicators (KPI)

Where can I find more information?

- CMMC Academy is a good start at understanding the CMMC and how it can be implemented. This is a great place to start if you want to work on government contracts, however it's also a great place to start if you do not have any sort of security program in place.

Training & Metrics

CELERIUM™

Q&A