Exploring the CMMC Framework

The CMMC is intended to serve as a verification mechanism to ensure that appropriate levels of cybersecurity practices and processes are in place to guarantee basic cyber hygiene as well as protect controlled unclassified information (CUI) that resides on the Department's industry partners' networks.

17 domains are key sets of capabilities for cybersecurity

5 SECURITY LEVELS DEFINED

1. Performed

Requires organization to perform a set of practices that correspond to basic safeguarding requirements.

2. Documented

Requires organization to establish and document practices and policies.

3. Managed

Requires organization to establish, maintain, and resource a plan demonstrating the management of activities for practice implementation. Focuses on protection of CUI.

4. Reviewed

Requires that an organization review and measure practices for effectiveness and take corrective action when necessary. Focuses on protection of CUI from Advances Persistent Threats and encompasses a subset of the enhanced security requirements as well as other cybersecurity best practices.

5. Optimizing

Requires an organization to standardize and optimize process implementation across the organization, increasing the depth and sophistication of cybersecurity practices.

STERLING