Executive Summary

CMMC / NIST SP 800-171 Readiness Assessment

Aegis Avionics LLC

1. Purpose & Scope

   This assessment evaluated Aegis Avionics' readiness against applicable NIST SP 800-171 requirements aligned with CMMC expectations. The review focused on systems and processes that store, process, or transmit Controlled Unclassified Information (CUI), including Microsoft 365, identify and access management, managed endpoints, and supporting administrative access paths.

   This engagement was conducted as a readiness assessment and does not represent a certification, audit or formal attestation.

2. Overall Readiness Posture

   Aegis Avionics demonstrates partial alignment with NIST SP 800-171 requirements. Core security capabilities – such as centralized identity management, multifactor authentication, and encrypted remote access – are in place. However, several controls are inconsistently implemented or lack formal documentation and enforcement.

   Based on the current state, Aegis Avionics likely will face challenges during a formal CMMC assessment without targeted remediation efforts.

3. Key Strengths

   The following strengths provide a solid foundation for remediation:

   - Centralized identity and access management through Microsoft Entra ID
   - Multifactor authentication enabled for most user accounts
   - Encrypted remote access and secure cloud-based collaboration tools
   - General awareness of CUI handling requirements among staff

   These capabilities significantly reduce the effort required to reach an acceptable compliance posture.

4. Key Risk Areas

   The most significant risk areas identified during the assessment include:

   - Lack of a documented and consistently executed user access review process
   - Excessive privileges granted to some users without formal justification
   - Inconsistent enforcement of endpoint session locking and timeout controls
   - Limited controls governing mobile device access to CUI
   - Gaps in documented authorization and oversight or privileged remote access

   If left unaddressed, these gaps increase the risk of unauthorized access to CUI and weaken audit defensibility.

5. Remediation Outlook (Next 60-90 days)

   Most identified gaps can be addressed withing 60-90 days through focused procedural improvements and configuration adjustments. Priority remediation efforts should focus on:

   - Formalizing access review and least privilege enforcement
   - Standardizing endpoint security configurations
   - Clarifying and enforcing mobile access restrictions
   - Documenting administrative access and privileged activity controls

   Successful execution of these actions will materially improve audit readiness and reduce compliance risk.

6. Final Assessment Statement

   With targeted remediation and continued leadership support, Aegis Avionics is well-positioned to achieve alignment with NIST SP 800-171 requirements. The organization's existing technical foundation enables efficient progress toward compliance without the need for extensive new tooling or significant operational disruption.