CMMC 2.0 Level 3 Compliance Checklist

The security requirements in CMMC Level 3 are selected from NIST SP 800-172, and where applicable, Organization-Defined Parameters (ODPs) are assigned.

Access control

- □ **AC.L3-3.1.2e:** Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.
- □ **AC.L3-3.1.3e:** Employ secure information transfer solutions to control information flows between security domains on connected systems.

Awareness and training

- □ **AT.L3-3.2.1e:** Provide awareness training upon initial hire, following a significant cyber event, and at least annually, focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat.
- □ **AT.L3-3.2.2e:** Include practical exercises in awareness training for all users, tailored by roles, to include general users, users with specialized roles, and privileged users, that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.

Configuration management

- □ **CM.L3-3.4.1e:** Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.
- □ **CM.L3-3.4.2e:** Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, remove the components or place the components in a quarantine or remediation network to facilitate patching, re-configuration, or other mitigations.
- □ **CM.L3-3.4.3e:** Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components.

Identification and authentication

- □ **IA.L3-3.5.1e:** Identify and authenticate systems and system components, where possible, before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.
- □ **IA.L3-3.5.3e:** Employ automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile.

CMMC 2.0 Level 3 Compliance Checklist

Incident repsonse

- □ **IR.L3-3.6.1e:** Establish and maintain a security operations center capability that operates 24/7, with allowance for remote/on-call staff.
- □ **IR.L3-3.6.2e:** Establish and maintain a cyber-incident response team that can be deployed by the organization within 24 hours.

Personnel security

- □ **PS.L3-3.9.2e:** Ensure that organizational systems are protected if adverse information develops or is obtained about individuals with access to CUI.

Risk management

- □ **RA.L3-3.11.1e:** Employ threat intelligence, at a minimum from open or commercial sources, and any DoD-provided sources, as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.
- □ **RA.L3-3.11.2e:** Conduct cyber threat hunting activities on an on-going aperiodic basis or when indications warrant, to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls.
- □ **RA.L3-3.11.3e:** Employ advanced automation and analytics capabilities in support of analysts to predict and identify risks to organizations, systems, and system components.
- □ **RA.L3-3.11.4e:** Document or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination.
- □ **RA.L3-3.11.5e:** Assess the effectiveness of security solutions at least annually or upon receipt of relevant cyber threat information, or in response to a relevant cyber incident, to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.
- □ **RA.L3-3.11.6e:** Assess, respond to, and monitor supply chain risks associated with organizational systems and system components.
- □ **RA.L3-3.11.7e:** Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan at least annually, and upon receipt of relevant cyber threat information, or in response to a relevant cyber incident.

CMMC 2.0 Level 3 Compliance Checklist

Security assessment

□ **CA.L3-3.12.1e:** Conduct penetration testing at least annually or when significant security changes are made to the system, leveraging automated scanning tools and ad hoc tests using subject matter experts.

System and communications protection

□ **SC.L3-3.13.4e:** Employ physical isolation techniques or logical isolation techniques or both in organizational systems and system components.

System and information integrity

□ **SI.L3-3.14.1e:** Verify the integrity of security critical and essential software using root of trust mechanisms or cryptographic signatures.

□ **SI.L3-3.14.3e:** Ensure that specialized assets including IoT, IIoT, OT, GFE, Restricted Information Systems, and test equipment are included in the scope of the specified enhanced security requirements or are segregated in purpose-specific networks.

□ **SI.L3-3.14.6e:** Use threat indicator information and effective mitigations obtained from, at a minimum, open or commercial sources, and any DoD-provided sources, to guide and inform intrusion detection and threat hunting.