System Security Plan (SSP)

1. System Identification

System Name: Logistics Operations Support System (LOSS)

Owner: Defense Logistics Agency (Simulated)

System Category: Moderate Impact (FIPS 199)

Environment: Azure Government Cloud

2. Control Implementation Summary

Control: AC-2 - Account Management

Implementation: Azure Active Directory is used to manage user identities, enforce multi-factor authentication (MFA), and apply role-based access controls. User accounts are reviewed bi-weekly, and inactive accounts are automatically disabled after 30 days.

Control: AC-17 - Remote Access

Implementation: All remote connections must pass through a VPN authenticated via DoD-issued PKI certificates. Remote access is monitored and logged via Microsoft Defender for Endpoint and Azure Sentinel.

3. Continuous Monitoring Strategy

Continuous monitoring is implemented through Microsoft Defender, Azure Monitor, and Sentinel. Vulnerability scans are performed weekly using Tenable Nessus. Patches are deployed within 15 days of vulnerability disclosure, and findings are tracked in a formal POA&M.