Security Assessment and Authorization Implementation Checklist

Policy and Documentation

- [ ] **CA-01**: Develop, document, and disseminate organization-level, mission/business process-level, and system-level assessment, authorization, and monitoring policy
- [ ] **CA-01**: Ensure assessment, authorization, and monitoring policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
- [ ] **CA-01**: Verify assessment, authorization, and monitoring policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
- [ ] **CA-01**: Document procedures to facilitate implementation of the assessment, authorization, and monitoring policy and associated controls
- [ ] **CA-01**: Designate an official to manage the development, documentation, and dissemination of assessment, authorization, and monitoring policy and procedures
- [ ] **CA-01**: Review and update assessment, authorization, and monitoring policy at least every 3 years or as required by federal or organizational policy changes
- [ ] **CA-01**: Review and update assessment, authorization, and monitoring procedures at least every 3 years or as required by federal or organizational policy changes

Control Assessment Planning and Execution

- [ ] **CA-02**: Select appropriate assessor or assessment team for the type of assessment to be conducted
- [ ] **CA-02**: Develop control assessment plan that describes controls and control enhancements under assessment
- [ ] **CA-02**: Develop control assessment plan that describes assessment procedures to be used to determine control effectiveness
- [ ] **CA-02**: Develop control assessment plan that describes assessment environment, assessment team, and assessment roles and responsibilities

- [ ] **CA-02**: Ensure control assessment plan is reviewed and approved by authorizing official or designated representative prior to conducting assessment
- [ ] **CA-02**: Assess controls in the system and its environment of operation at least annually
- [ ] **CA-02**: Determine extent to which controls are implemented correctly, operating as intended, and producing desired outcome with respect to security and privacy requirements
- [ ] **CA-02**: Produce control assessment report that documents results of the assessment
- [ ] **CA-02**: Provide results of control assessment to FedRAMP PMO and JAB
- [ ] **CA-02(01)**: Employ independent assessors or assessment teams to conduct control assessments

System Interconnections and Information Exchange

- [ ] **CA-03**: Approve and manage exchange of information between the system and other systems using appropriate agreements (interconnection security agreements, information exchange security agreements, memoranda of understanding or agreement, service level agreements, user agreements, nondisclosure agreements, or organization-defined type of agreement)
- [ ] **CA-03**: Document interface characteristics as part of each exchange agreement
- [ ] **CA-03**: Document security and privacy requirements as part of each exchange agreement
- [ ] **CA-03**: Document controls as part of each exchange agreement
- [ ] **CA-03**: Document responsibilities for each system as part of each exchange agreement
- [ ] **CA-03**: Document impact level of information communicated as part of each exchange agreement
- [ ] **CA-03**: Review and update agreements at least annually and on input from FedRAMP

Plan of Action and Milestones

- [ ] **CA-05**: Develop plan of action and milestones for the system to document planned remediation actions to correct weaknesses or deficiencies noted during control assessments
- [ ] **CA-05**: Develop plan of action and milestones to reduce or eliminate known vulnerabilities in the system
- [ ] **CA-05**: Update existing plan of action and milestones at least monthly based on findings from control assessments

- [ ] **CA-05**: Update existing plan of action and milestones at least monthly based on findings from independent audits or reviews
- [ ] **CA-05**: Update existing plan of action and milestones at least monthly based on findings from continuous monitoring activities

Security Authorization

- [ ] **CA-06**: Assign a senior official as the authorizing official for the system
- [ ] **CA-06**: Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems
- [ ] **CA-06**: Ensure authorizing official for the system accepts use of common controls inherited by the system before commencing operations
- [ ] **CA-06**: Ensure authorizing official for the system authorizes the system to operate before commencing operations
- [ ] **CA-06**: Ensure authorizing official for common controls authorizes use of those controls for inheritance by organizational systems
- [ ] **CA-06**: Update authorizations at least every three years or when a significant change occurs

Continuous Monitoring

- [ ] **CA-07**: Develop system-level continuous monitoring strategy in accordance with organization-level continuous monitoring strategy
- [ ] **CA-07**: Establish system-level metrics to be monitored as defined in the applicable FedRAMP and organization-defined continuous monitoring strategy
- [ ] **CA-07**: Establish continuous monitoring for malicious code protection mechanisms
- [ ] **CA-07**: Establish continuous monitoring for log record review
- [ ] **CA-07**: Establish continuous monitoring for account management activities
- [ ] **CA-07**: Establish continuous monitoring for remote access management activities
- [ ] **CA-07**: Establish continuous monitoring for verification of ongoing identification and authentication
- [ ] **CA-07**: Establish continuous monitoring for configuration settings
- [ ] **CA-07**: Establish at least annual assessment frequencies for all other control assessment activities

- [ ] **CA-07**: Conduct ongoing control assessments in accordance with the continuous monitoring strategy
- [ ] **CA-07**: Conduct ongoing monitoring of system and metrics as defined in the applicable FedRAMP and organization-defined continuous monitoring strategy
- [ ] **CA-07**: Perform correlation and analysis of information generated by control assessments and monitoring
- [ ] **CA-07**: Implement response actions to address results of the analysis of control assessment and monitoring information
- [ ] **CA-07**: Report security and privacy status of the system to FedRAMP PMO and JAB in accordance with the applicable FedRAMP and organization-defined continuous monitoring strategy
- [ ] **CA-07(01)**: Employ independent assessors or assessment teams to monitor controls in the system on an ongoing basis

Internal System Connections

- [ ] **CA-09**: Authorize internal connections of organization-defined system components or classes of components to the system
- [ ] **CA-09**: Document interface characteristics for each internal connection
- [ ] **CA-09**: Document security and privacy requirements for each internal connection
- [ ] **CA-09**: Document nature of information communicated for each internal connection
- [ ] **CA-09**: Terminate internal system connections after organization-defined conditions
- [ ] **CA-09**: Review at least annually the continued need for each internal connection

Key Timeframes Summary

- [ ] **Policy Review**: At least every 3 years or when federal/organizational policy changes occur
- [ ] **Control Assessments**: At least annually
- [ ] **System Interconnection Agreement Review**: At least annually and on input from FedRAMP
- [ ] **POA&M Updates**: At least monthly
- [ ] **Authorization Updates**: At least every three years or when significant change occurs
- [ ] **Continuous Monitoring**: Continuous for specific activities (malicious code protection, log review, account management, remote access management, identification and

authentication verification, configuration settings); at least annually for all other control assessment activities

- [ ] **Internal Connection Review**: At least annually