

<Organization Name>	Information Security Assessment and Authorization Policy	
Department Name	Policy #	Issue Date: September 13, 2013
Approved by:		

1. Purpose

<Organization Name> <Insert Organization Mission Here>. This policy establishes the Enterprise Security Assessment and Authorization Policy, for managing risks from inadequate security assessment, authorization, and continuous monitoring of company information assets through the establishment of an effective security planning program. The security planning program helps <Organization Name> implement security best practices with regard to enterprise security assessment, authorization, and continuous monitoring.

2. Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by <Organization Name>. Any information, not specifically identified as the property of other parties, that is transmitted or stored on <Organization Name> IT resources (including e-mail, messages and files) is the property of <Organization Name>. All users (<Organization Name> employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

3. Intent

The <Organization Name> Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a security assessment and authorization capability throughout <Organization Name> and its business units to help the organization implement security best practices with regard to enterprise security assessment, authorization, and continuous monitoring.

4. Policy

<Organization Name> has chosen to adopt the Security Assessment and Authorization principles established in NIST SP 800-53 "Security Assessment and Authorization," Control Family guidelines, as the official policy for this domain. The following subsections outline the Security Assessment and Authorization standards that constitute <Organization Name> policy. Each <Organization Name> Business System is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

- CA-1 Security Assessment and Authorization Procedures: All <Organization Name> Business Systems must develop, adopt or adhere to a formal, documented security assessment and authorization procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

<Organization Name>	Information Security Assessment and Authorization Policy	
Department Name	Policy #	Issue Date: September 13, 2013
Approved by:		

- CA-2 Security Assessments: All <Organization Name> Business Systems must:
 - Develop a security assessment plan that describes the scope of the assessment that includes:
 - Security controls and control enhancement under assessment.
 - Assessment procedure to be used to determine security control effectiveness.
 - Assessment environment, assessment team, and assessment roles and responsibilities.
 - Assess the security controls in the information asset on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
 - Produce a security assessment report that documents the results of the assessment.
 - Provide the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.
- CA-3 Information System Connections: All <Organization Name> Business Systems must:
 - Authorize connections from the information asset to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements.
 - Document, for each connection, the interface characteristics, security requirements, and the nature of the information communicated.
 - Monitor the information assets connections on an ongoing basis verifying enforcement of security requirements.
- CA-4 Plan of Action and Milestones: All <Organization Name> Business Systems must:
 - Develop a plan of action and milestones for the information asset to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.
 - Update existing action plans and milestones based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
- CA-5 Security Authorization: All <Organization Name> Business Systems must:
 - Assign a senior-level executive or manager to the role of authorizing official for the information asset.
 - Ensure that the authorizing official authorizes the information asset for processing before commencing operations.
 - Update the security authorization on an annual basis.

<Organization Name>	Information Security Assessment and Authorization Policy	
Department Name	Policy #	Issue Date: September 13, 2013
Approved by:		

- CA-6 Continuous Monitoring: All <Organization Name> Business Systems must establish a continuous monitoring strategy and implement a continuous monitoring program that includes:
 - A configuration management process for the information asset and its constituent components.
 - A determination of the security impact of changes to the information asset and environment of operation.
 - Ongoing security control assessments in accordance with the organizational continuous monitoring strategy.
 - Reporting the security state of the information asset to appropriate organizational officials on an annual basis.

DRAFT

<Organization Name>	Information Security Assessment and Authorization Policy	
Department Name	Policy #	Issue Date: September 13, 2013
Approved by:		

Appendix A – References

The following references illustrate public laws which have been issued on the subject of cyber security and should be used to demonstrate <Organization Name> responsibilities associated with protection of its cyber assets.

- a. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53 Recommended Security Controls for Federal Information Systems Revision 3, Management Controls, Security Assessment and Authorization Control Family, August 2009.
- b. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-37 “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach” Revision 1 February 2010.
- c. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-100 “Information Security Handbook: A Guide for Manager” October 2006.
- d. United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-115 “Technical Guide to Information Security Testing and Assessment” September 2008.

