



Security Authorization Process Guide

Office of the Chief Information Security Officer
(CISO)

Version 10

[June 6, 2013]

TABLE OF CONTENTS

1.0	Introduction.....	7
1.1	Background	7
1.2	Purpose	8
1.3	Scope	9
1.4	References	Error! Bookmark not defined.
2.0	Roles and Responsibilities	11
2.1	Security Authorization Team	11
2.2	Security Assessment Team.....	12
2.3	DHS inventory team.....	13
2.4	Information System Security Officer (ISSO).....	14
2.5	System Owner	14
2.6	Program Manager	14
2.7	Technical staff	14
2.8	Security Control ASSESSOR (SCA)	15
2.9	Authorizing Official (AO).....	15
2.10	Business Owner.....	15
2.11	Chief Information Security Officer (CISO)/ Information System Security Manager (ISSM).....	15
2.12	Chief Security officer (CSO)/Facility Security Officer (FSO)	15
2.13	Privacy Office	15
2.14	DHS Document Review Team (DR).....	15
3.0	IACS Basics	Error! Bookmark not defined.
4.0	Tasks Throughout the SELC.....	16
4.1	Markings.....	16
4.2	Publishing documents	16
4.3	Section 508 Compliance.....	16
4.3.1	DHS Section 508 Compliance Checklist	16
4.3.2	DHS Section 508 Compliance Upload	17
4.4	MOU/MOA/ISA.....	17
4.4.1	ISA Template	17

4.4.2	ISA Library	18
4.4.3	MOA Template	19
4.4.4	MOA Library	19
4.4.5	MOU Template	20
4.4.6	MOU Library	21
4.5	General Information (View and Publish the SP, RTM, etc.)	22
4.5.1	RTM.....	22
4.5.2	Project Personnel	23
4.5.3	Manage Project Artifacts	24
4.5.4	Published Documents.....	24
4.5.5	Financial DesignATION/Investment Information.....	25
4.5.6	Project Information Detail	25
5.0	Creating a Project (System or Program)	26
6.0	Categorize	27
6.1	Categorize Information System.....	27
6.1.1	Project Definition.....	27
6.1.2	Security Regulations	28
6.1.3	Project Personnel	28
6.1.4	ISSO Designation Letter	29
6.1.5	ISSO Designation Letter Extensible	29
6.1.6	System Users.....	30
6.1.7	System Boundary	31
6.1.8	System Data Flow	31
6.1.9	System Interfaces/Interconnections	32
6.1.10	System Environment.....	33
6.1.11	Project Milestones.....	35
6.1.12	System Data Types	35
6.1.13	Requirements Questionnaire.....	36
6.1.14	System Security	37
6.1.15	E-Authentication.....	37
6.2	Initial privacy threshold analysis.....	38

6.3	Final Privacy Threshold Analysis	38
6.3.1	DHS Privacy Checklist	38
6.3.2	Complete Privacy Threshold Analysis.....	38
6.3.3	Privacy Threshold Analysis Extensible	39
6.4	Privacy Documentation	39
6.4.1	PIA Upload	39
6.4.2	SORN Upload.....	40
7.0	Select.....	40
7.1	Select Security Controls.....	41
7.1.1	Organizationally Defined Requirements.....	41
7.1.2	System Security Requirements	41
7.1.3	RTM.....	41
8.0	Implement	42
8.1	Implement Security Controls	42
8.1.1	Equipment Group.....	43
8.1.2	Equipment Inventory	44
8.1.3	Manage Software	46
8.1.4	Controls Implementation	47
8.1.5	Review System Users	48
8.1.6	Review System Boundary.....	48
8.1.7	Review System Data Flow.....	48
8.1.8	Review System Interfaces/Interconnections	48
8.1.9	Review System Environment.....	49
8.1.10	Ports, Protocols, and Services.....	49
8.1.11	Security Plan References	50
8.1.12	Security Plan	50
8.1.13	Security Plan Extensible	50
8.2	Contingency Plan	51
8.2.1	ConTINGENCY PLAN (SECTIONS 1-2).....	52
8.2.2	Contingency plan (section 3-5).....	52
8.2.3	contingency Plan (section 6-7).....	52

8.2.4	Contingency Plan Extensible	52
8.3	Contingency Plan Test	52
8.3.1	Contingency Plan Test	53
8.3.2	Contingency Plan Test Extensible	53
8.4	Configuration Management Plan	53
8.4.1	Configuration Management Plan	54
8.4.2	Configuration Management Plan Extensible	54
9.0	Assess.....	54
9.1	Self-Assessment	55
9.1.1	Project Test Matrix	55
9.1.2	RTM.....	56
9.1.3	Security Assessment	56
9.1.4	Security assessment Plan	58
9.1.5	Security Assessment Plan Extensible	58
9.2	Security Assessment.....	59
9.2.1	Project Test Matrix	59
9.2.2	Security Assessment	60
9.2.3	Requirements Traceability Matrix (RTM).....	60
9.2.4	Security Assessment Report	60
9.2.5	Security Assessment Report Extensible.....	61
9.2.6	Vulnerability/Penetration Test Report	61
9.3	Risk Analysis.....	62
9.3.1	Analyze Risk Elements	63
9.3.2	Requirements Traceability Matrix (RTM).....	64
9.3.3	Risk Assessment (RA)	64
9.3.4	Risk Assessment Extensible	65
9.3.5	Security Assessment Report	65
9.3.6	Security Assessment Report Extensible.....	66
9.3.7	System risk level.....	66
10.0	Authorize.....	66
10.1	POA&M	67

10.1.1	POA&M Elements	68
10.1.2	POA&M Report Extensible	69
10.2	Component Document Review	69
10.2.1	Published Documents.....	70
10.2.2	Security Authorization Package Transmittal Letter.....	70
10.2.3	Security Authorization Package TRANSMITTAL LETTER Extensible.....	71
10.3	ATO Decision	71
10.3.1	Published Documents.....	71
10.3.2	Project Accrediation.....	72
10.3.3	ATO Letter.....	73
10.3.4	ATO Letter Extensible.....	73
10.4	DHS Document Review	74
10.4.1	Published Documents.....	74
11.0	Monitor	74
11.1	System Documentation	75
11.1.1	Project Definition.....	75
11.1.2	Project Information Detail	75
11.1.3	Project Milestones.....	76
11.1.4	System Boundary	77
11.1.5	System Environment.....	77
11.1.6	System Interfaces/Interconnections	79
11.1.7	System Data Flow	80
11.1.8	Manage Software	81
11.1.9	Controls Implementation	82
11.1.10	Equipment Groups.....	83
11.1.11	Equipment inventory	84
11.1.12	System Users	86
11.1.13	Project Personnel.....	87
11.1.14	Security Assessment.....	88
11.1.15	Analyze Risk Elements	89
11.1.16	POA&M Elements	91

11.1.17	Requirements Traceability Matrix (RTM)	93
11.1.18	Security Assessment Report.....	93
11.1.19	Security Plan	94
11.1.20	Security Plan Extensible.....	94
11.1.21	Contingency Plan	95
11.1.21.1	ConTINGENCY PLAN (SECTIONS 1-2).....	96
11.1.21.2	Contingency plan (section 3-5).....	96
11.1.21.3	contingency Plan (section 6-7)	96
11.1.22	Contingency Plan Test	96
11.1.23	Published Documents	97
11.2	Monitor POA&M.....	97
11.2.1	Analyze Risk Elements	98
11.2.2	POA&M Elements	99
11.2.3	POA&M Report Extensible	101
11.3	Change Log	101
11.3.1	Relevant Change Report	101

1.0 INTRODUCTION

Under the authority of the Department of Homeland Security (DHS) Chief Information Officer (CIO), the Chief Information Security Officer (CISO) bears the primary responsibility to ensure compliance with Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB), and all applicable laws, directives, policies, and directed actions on a continuing basis. This document sets forth the overall methodology for the Security Authorization process of information systems operated within the Department.

1.1 BACKGROUND

Security authorization (SA) is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. The Authorizing Official (AO) accepts security responsibility for the operation of an assessed system and officially declares that it is authorized to operate.

Security authorization involves comprehensive testing and evaluation of security features (also known as controls) of an information system. It addresses software and hardware security safeguards; considers procedural, physical, and personnel security measures; and establishes the extent to which a particular design (or architecture), configuration, and implementation meets a specified set of security requirements throughout the life cycle of the information system. It also considers procedural, physical, and personnel security measures employed to enforce information security policy.

An information system must be granted an Authority to Operate (ATO) before it first becomes operational, and must be re-authorized at least every three (3) years and whenever changes are made that affect the potential risk level of operating the system. “Operational” is generally defined as whenever an information system begins processing real or live data. An information system must be assessed and authorized in an Accreditation Decision Letter prior to passing the Key Decision Point 3 milestone in the development life cycle.

AOs may grant an Interim Authorization to Operate (IATO) for information systems that are undergoing development testing or are in a prototype phase of development. The AO may grant an IATO for a maximum period of six (6) months and may grant a single six (6) month extension. IATOs are not authorized for operational systems. IATOs are typically granted in the instance of a non-operational development information system testing with production data. In general, IATOs are not recognized within DHS.

The process for conducting a re-authorization is the same used to conduct the initial Security Authorization. The primary difference is that an initial Security Authorization should be started early in the System Engineering Life Cycle (SELC) process while re-authorization will usually begin four (4) to six (6) months before the current ATO expires. The four (4) to six (6) month timeframe assumes that resources are available to start the security authorization process. Additional lead time may be needed for contracting or otherwise obtaining resources needed to conduct the security authorization.

1.2 PURPOSE

The security authorization process applies the Risk Management Framework (RMF) from NIST Special Publication (SP) 800-37. This includes conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. This process helps ensure that managing information system-related security risks is consistent with the DHS mission/business objectives and overall risk strategy established by the department and components; integrates information security, including security controls, are integrated into the DHS enterprise architecture and SELC process; and supports consistent, well-informed security authorization decisions throughout the life-cycle of the information system.

The purpose of this document is to provide practical guidance for conducting a security authorization within DHS. Components may tailor this guide to meet their individual requirements as long as they remain consistent with this guide, NIST guidance, OMB guidance and directives, DHS security policies, guidance and directives, and all applicable laws, directives, policies, and directed actions.

1.3 SCOPE

All unclassified systems, including General Support Systems (GSSs) and Major Applications (MAs), in the DHS FISMA inventory must be assessed and authorized in accordance with the process identified in this guide. All sub-systems and minor applications must be documented in the security authorization package of an associated GSS or MA.

The process for assessing and accrediting National Security Systems (NSS) is outside the scope of this guide.

1.4 ONGOING AUTHORIZATION

As stated in NIST 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, “initial system authorization is based on evidence available at one point in time, but systems and environments of operation change.” To address the needs of constantly changing environments, DHS is implementing OA, which involves shifting from periodic to ongoing assessments and facilitates a continual state of awareness.

DHS implements OA in **three layers**, which collectively ensure constant control assurance.

- Layer 1: Common and Inherited Controls and Reciprocity
- Layer 2: Continuous Monitoring
- Layer 3: Event-Driven Monitoring

Event-Driven Monitoring (Layer 3) involves evaluating and testing controls when security events or “triggers” occur that may have an impact on the system’s security status. Following an event, a review is conducted to determine the impact on the status of controls and risk to the system. Some key **process highlights** include the following:

- An Operational Risk Management Board (ORMB), composed of various subject matter experts, evaluates security triggers and makes risk-based recommendations.
- Following ORMB review, the CISO prepares a formal recommendation to the Authorization Official (AO) about whether or not to maintain the authorization.

Security triggers are to be reported in the Component’s Trigger Accountability Log (TRAL) and provided to DHS on a monthly basis.

To qualify for OA, the following **prerequisites** must be met (see section 1.6 for more detail):

- The system must have a valid ATO.
- The information system must have a Control Allocation Table (CAT).
- The Component should have a Common Control Catalog in place.
- The Component must have a robust Continuous Monitoring program.
- The Component must assign an OA Manager.
- The Component must establish an ORMB.
- The Component must offer an OA training program.

The Component must accept and sign the DHS OA Memorandum of Agreement (MOA).

For more information about ongoing authorization, please refer to the Ongoing Authorization Methodology guide.

1.5 REFERENCES

- DHS Sensitive Systems Policy Directive 4300A
- DHS 4300A Sensitive Systems Handbook
- DHS Ongoing Authorization Methodology
- Attachments to DHS 4300A, particularly:
 - Attachment B, "*Waivers and Exceptions Request Form*"
 - Attachment C, "*Information Systems Security Officer (ISSO) Designation Letter*"
 - Attachment D, "*Type Accreditation*"
 - Attachment F, "*Incident Response and Reporting*"
 - Attachment G, "*Rules of Behavior*"
 - Attachment H, "*Plan of Action and Milestones (POA&M) Process Guide*"
 - Attachment K, "*IT Contingency Plan Template*"
 - Attachment N, "*Preparation of Interconnection Security Agreements*"
- NIST SP 800-53, "*Recommended Security Controls for Federal Information Systems and Organizations*"
- DHS CISO NIST SP 800-53 Security Controls tri-fold
- DHS FISMA System Inventory Methodology
- DHS Information Security Performance Plan
- DHS Security Authorization Process Guide
- DHS Document Review Methodology
- Document Review Checklists
- Security Authorization Document Templates
- FIPS-199 Workbook and Instructions

- Privacy Threshold Analysis (PTA) Template

Additional references that may be useful when conducting a Security Authorization include:

- Component specific guidance
- DHS Information System Security Officer (ISSO) Guide
- Telos Exacta User Guide and In-application Help
- Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*
- Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST Special Publications (SPs) in the 800 series, but especially:
 - SP 800-18, "*Guide for Developing Security Plans for Federal Information Systems*"
 - SP 800-30, "*Guide for Conducting Risk Assessments*"
 - SP 800-34, "*Contingency Planning Guide for Information Technology Systems*"
 - SP 800-37, "*Guide for Applying the Risk Management Framework to Federal Information Systems*"
 - SP 800-39, "*Managing Information Security Risk: Organization, Mission, and Information System View*"
 - SP 800-53A, "*Guide for Assessing the Security Controls in Federal Information Systems*"
 - SP 800-60, "*Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*"

2.0 ROLES AND RESPONSIBILITIES

Within DHS guidelines, each Component, organization and system determines its own internal procedures for conducting a security authorization. In some cases, security authorizations are conducted by ISSOs. In other cases, a system may use contractors hired specifically to conduct the security authorization or Components may provide a dedicated security authorization group for use within the Component. The following sections list personnel who have a key role in the security authorization process and briefly describe their duties.

2.1 SECURITY AUTHORIZATION TEAM

The security authorization team has primary responsibility for conducting security authorization activities. This includes collecting data, developing documents and preparing the Security Authorization Package (SAP) for the Security Control Assessor (SCA)/AO review. The security authorization team may also conduct the SAP depending on the need for separation of duties. The security authorization team needs access to the DHS security authorization Information Assurance Compliance System (IACS) tool.

Figure 1 illustrates the different stakeholders that must be engaged in order to conduct an efficient security authorization.

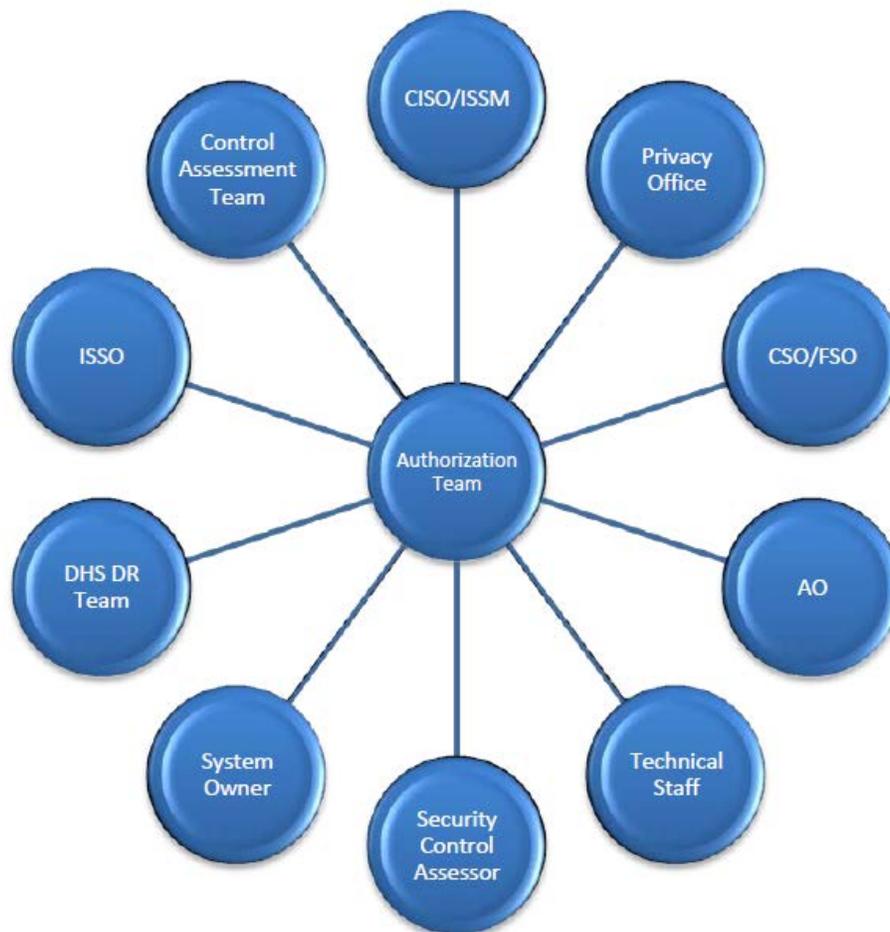


Figure 1: The Security Authorization Team Stakeholders

2.2 SECURITY ASSESSMENT TEAM

The Security Assessment Team tests the security controls documented in the Requirements Traceability Matrix (RTM). The RTM is created in RMS, and the controls are tested to ensure they have been implemented properly and are operating as intended. The Security Assessment is usually conducted using the Security Assessment Plan developed by the Security Authorization Team. Members of the Security Assessment Team should not be on the Security Authorization Team to avoid conflict of interest but do not need to be independent for systems categorized as Low-Low-Low, confidentiality, integrity, and availability security categories, as long as test results are reviewed by an independent source to validate their completeness, consistency, and veracity. The AO decides the required level of independence based on the criticality and sensitivity of the system and the ultimate level of risk.

veracity. The AO decides the required level of independence based on the criticality and sensitivity of the system and the ultimate level of risk.

Figure 2 illustrates the information flow among various stakeholders needed to complete the Security Authorization process.

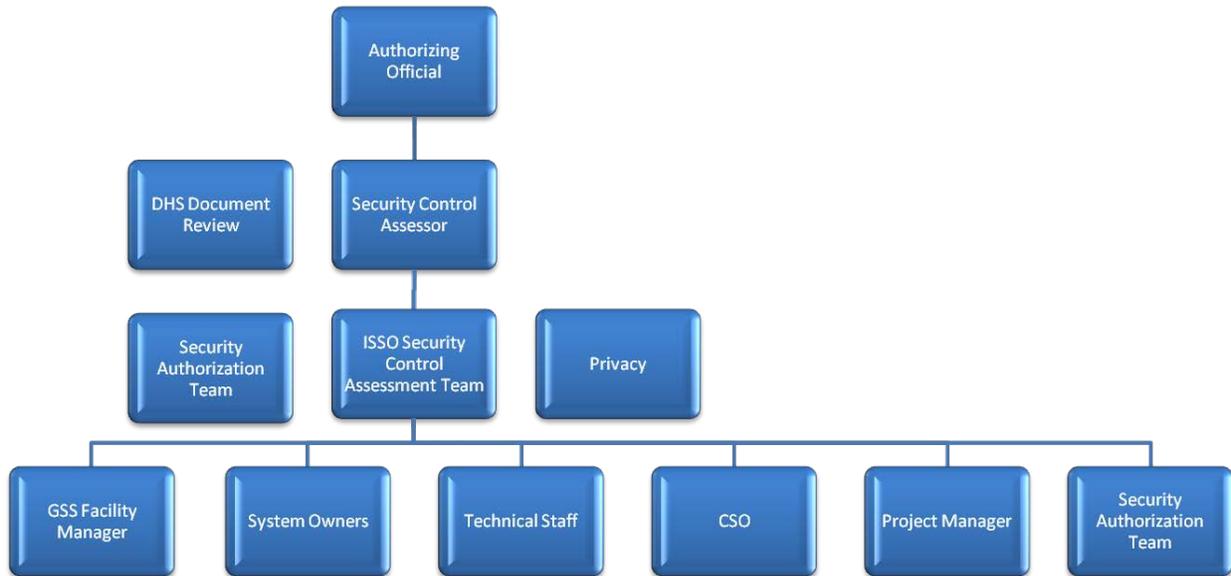


Figure 2: The Security Control Assessment Team

2.3 DHS INVENTORY TEAM

The Federal Information Security Management Act (FISMA) requires developing, maintaining, and updating an inventory of information systems operated by the DHS or under its control. This inventory also includes an identification of the interconnections between each system and all other systems or networks, including those not operated by or under the control of the Department. The DHS Information Technology (IT) system inventory is also used to support information resources management; IT planning, budgeting, and acquisition; the monitoring, testing, and evaluation of information security controls; and the preparation of the index of major information systems required pursuant to the Freedom of Information Act (FOIA). The DHS Chief Information Security Officer (CISO), and subsequently the Inventory Management (IM) Team within OCISO, is responsible for ensuring Department-wide oversight and compliance with FISMA to include developing and maintaining a Department IT system inventory.

The DHS IM Team's role consists of two primary functions: 1) Perform routine change management; and 2) Conduct the Annual Refresh process.

DHS Components are required to submit a Change Request form to the IM Team any time the System Engineering Lifecycle (SEL) status or centrally managed data fields of a DHS

information system changes. It is the IM Team's responsibility to process change requests and update the Information Assurance Compliance System (IACS), reporting system as needed.

The IM Team also conducts an annual review of all DHS information systems called the FISMA Inventory Annual Refresh (Annual Refresh or Refresh). The Annual Refresh is an opportunity for Components to holistically review and update their inventory and for the ISO to clarify any discrepancies found through independent reviews.

2.4 INFORMATION SYSTEM SECURITY OFFICER (ISSO)

Information System Security Officers (ISSOs) are not always directly responsible for conducting a Security Authorization but they need to monitor and oversee the process at a minimum. ISSOs need to be aware of the status and expiration of the current ATO and initiate action early enough to ensure the Security Authorization process is completed before the system becomes operational or the current ATO expires. This entails working closely with the System Owner or program manager to ensure resources are available to both conduct and to participate in the Security Authorization process. Regardless of how the process is implemented, the ISSO plays a leading role to ensure documents are created in IACS and submitted to the SCA for DHS validation. ISSOs should coordinate closely with the SCA and the AO before and during the Security Authorization process to ensure they are aware of requirements, processes and expectations.

2.5 SYSTEM OWNER

The System Owner must ensure that adequate resources are budgeted for and allocated to the Security Authorization process. The System Owner will also serve as a primary source of input during data collection activities and should review the package for accuracy before it is forwarded to the SCA/AO. The System Owner must also be involved in POA&M planning to help determine resource availability and schedule. System Owners are ultimately accountable for the security of their systems and should be directly involved in the Security Authorization process.

2.6 PROGRAM MANAGER

The Program Manager may be a source of resources (e.g., if the Security Authorization process needs to be outsourced) and information input for areas where the System Owner is not knowledgeable (e.g., contracts).

2.7 TECHNICAL STAFF

A system's technical staff (e.g., system administrators, Data Base Administrators (DBAs), etc.) will be the primary source of input for describing and implementing most technical controls identified in the Security Plan. They may also have input to the system categorization process depending on system technology (e.g., wireless) and configuration. The technical staff should participate in the SAP to provide input to the SAP team and oversee the actual testing.

2.8 SECURITY CONTROL ASSESSOR (SCA)

The Security Control Assessor (SCA) assesses the effectiveness of the security controls based on the documentation submitted in the Security Authorization Package and makes a recommendation to the AO regarding whether or not to authorize the system. The Security Authorization Team should coordinate closely with the SCA throughout the process to ensure they understand and meet DHS and Component requirements.

The Component CISO is normally the SCA when no other person has been officially designated.

2.9 AUTHORIZING OFFICIAL (AO)

The Authorizing Official (AO) determines the degree of acceptable residual risk based on mission requirements, reviews the Security Authorization Package, and grants or denies ATO.

The DHS CIO serves as the AO for all Department-level enterprise systems or designates an AO in writing. The Component CIO serves as the AO for Component information systems or designates one in writing. The DHS Chief Financial Officer (CFO) serves as the AO for CFO Designated Systems managed at the DHS level. The Component CFO is the AO for only CFO Designated Systems managed by the Component.

2.10 BUSINESS OWNER

The business owner may provide input needed for the system categorization and section one (1) of the Security Plan. The business owner may also provide resources for conducting the Security Authorization or remediating weaknesses.

2.11 CHIEF INFORMATION SECURITY OFFICER (CISO)/ INFORMATION SYSTEM SECURITY MANAGER (ISSM)

The DHS Chief Information Security Officer (CISO) provides overall guidance for conducting a Security Authorization. The Component Chief Information Security Officer (CISO) / Information System Security Manager (ISSM) provides specific guidance for the Security Authorization Process within the Component and serves as the SCA unless someone else is designated.

2.12 CHIEF SECURITY OFFICER (CSO)/FACILITY SECURITY OFFICER (FSO)

The Chief Security Officer (CSO) and the Facility Security Officer (FSO) are often responsible for the implementation of some controls (e.g., physical access controls) and may provide input needed for personnel and physical controls for the system.

2.13 PRIVACY OFFICE

The DHS Privacy Office reviews PTAs and makes a determination regarding whether a Privacy Impact Assessment (PIA) or a System of Records Notice (SORN) is required.

2.14 DHS DOCUMENT REVIEW TEAM (DR)

The DHS Document Review (DR) Team reviews and validates Security Authorization Packages after they have been completed in IACS. Procedures for requesting a review can be found in the DHS Information Security Performance Plan at:

<http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Pages/comtech.aspx>

3.0 TASKS THROUGHOUT THE SELC

3.1 MARKINGS

Markings are the handling instructions on the header and footer of a published document. For most DHS information systems, “For Official Use Only” is the appropriate marking for the security authorization documentation. Please be mindful of the information included in the documentation as it may affect the overall classification or markings of the documentation. Classified information is not allowed in the Controlled Unclassified Information (CUI) IACS system and only information classified up to Secret is allowed in the Classified IACS environment.

3.2 PUBLISHING DOCUMENTS

Click on publish and select the appropriate markings on the pop-up screen. Typically, the systems will be For Official Use Only (FOUO); however, there are other markings used at DHS. They are:

- For Official Use Only (FOUO)
- Law Enforcement Sensitive
- Protected Critical Infrastructure Information (PCII)
- Sensitive Security Information (SSI)

3.3 SECTION 508 COMPLIANCE

Section 508 of the Rehabilitation Act of 1973 (as amended) requires all federal departments and agencies to ensure that their electronic information & technology (EIT) is accessible to people with disabilities. This task allows ISSOs and system owners to follow a checklist to determine if the system is 508 compliant.

3.3.1 DHS SECTION 508 COMPLIANCE CHECKLIST

This checklist is necessary for conducting a Section 508 Compliance process for the information system. To complete the checklist, click on the open icon and answer the questions.



Now the right hand column changes to display how many questions have been answered. Click on the open icon again to bring up the actual checklist.

Checklist Question Groups

Open	Section	Name	Status
	DHS Section 508 Compliance	DHS Section 508 Compliance	Incomplete (0/13)

Checklist Questionnaire

Number	Question	N/E	Yes	No	N/A	Notes
1.0	After answering the questions below, upload artifacts in the Section 508 Upload process step.					
1.1	Has the system been granted a National Security Exception for Section 508 Compliance? (Upload applicable artifact in the Section 508 Upload process step.)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
1.2	Has the system been granted an Undue Burden Exception for Section 508 Compliance? (Upload applicable artifact in the Section 508 Upload process step.)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
1.3	Has the system been granted a Fundamental Alteration Exception for Section 508 Compliance? (Upload applicable artifact in the Section 508 Upload process step.)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
1.4	Has the system been granted a Back Office Exception for Section 508 Compliance? (Upload applicable artifact in the Section 508 Upload process step.)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
1.5	Has the system been granted an Incidental to Contract Exception for Section 508 Compliance? (Upload applicable artifact in the Section 508 Upload process step.)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
1.6	Has the system been granted a Legacy System Exception for Section 508 Compliance? (Upload applicable artifact in the Section 508 Upload process step.)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
2.0	Has the system been assessed for 508 Compliance? (Upload applicable artifact in the Section 508 Upload process step.)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	

Rec/Page: 50 Records: 1-14 out of 14

3.3.2 DHS SECTION 508 COMPLIANCE UPLOAD

This step is for uploading and declaring artifacts in support of Section 508 compliance. Click on the paperclip icon to upload artifacts. Once all artifacts have been uploaded, answer the question.

Section 508 Upload

Completed: 

Have all of the system's Section 508 Compliance artifacts been uploaded?:

3.4 MOU/MOA/ISA

3.4.1 ISA TEMPLATE

This step is used to publish the ISA for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. (This is usually For Official Use Only (FOUO)).

ISA Template

View Template Properties Document Settings Publish

Completed:

Publishing Status: Never Published

This process step uses extensible publishing.



3.4.2 ISA LIBRARY

The ISA Library step includes all relevant ISA's pertaining to this project.

- Download the ISA template document from the ISA Template step.
- Fill out the provided template with the relevant information requested.
- Attach the populated document by clicking on the included documents button below.

ISA Library

Save All Document Settings Reset Publish

Completed:

The ISA Library step should include any relevant ISA's pertaining to this project.

- Download the ISA template document from the ISA Template step.
- Fill out the provided template with the relevant information requested.
- Attach the populated document by clicking on the included documents button below.

- Include this section in published document
- Start this section on new page
- Include 'List of Included Documents'

Included Document Title ▲	Properties	View	Delete
---------------------------	------------	------	--------

Remake Insert New Included Doc

Fill out the relevant information and include the document.

Add Included Document

Title*

Short Title:

Author:

Date*

Version:

File Location:

Add to References Appendix:

File*

Element	Description
Title	The title of the ISA.
Short Title	An extra field to add another title to the document.
Author	The author of the ISA.
Date	The date the ISA was completed.
Version	The version of the ISA.
File Location	The location of the file.
Add to References Appendix	This determines whether to add this ISA as a reference to the SP.
File	The document file to include.

3.4.3 MOA TEMPLATE

This step is used to publish the MOA for use outside of the IACS tool. Refer to the Publishing Documentation section for more information on markings.

3.4.4 MOA LIBRARY

The MOA Library step includes all relevant MOA's pertaining to this project.

- Download the MOA template document from the MOA Template step.
- Fill out the provided template with the relevant information requested.
- Attach the populated document by clicking on the included documents button below.

MOA Library

Completed:

- The MOA Library step should include any relevant MOA's pertaining to this project.
- Download the MOA template document from the MOA Template step.
 - Fill out the provided template with the relevant information requested.
 - Attach the populated document by clicking on the included documents button below.

Publishing Status: Never Published

1.0*

Memoranda of Agreement

There are no memoranda of agreement required or in force at this time.

Fill out the relevant information and include the document.

Add Included Document

Title*

Short Title:

Author:

Date*

Version:

File Location:

Add to References Appendix:

File*

Element	Description
Title	The title of the MOA.
Short Title	An extra field to add another title to the document.
Author	The author of the MOA.
Date	The date the MOA was completed.
Version	The version of the MOA.
File Location	The location of the file.
Add to References Appendix	This determines whether to add this MOA as a reference to the SP.
File	The document file to include.

3.4.5 MOU TEMPLATE

This step is used to publish the MOU for use outside of the IACS tool. Refer to the Publishing Documentation section for more information on markings..

MOU Template 

[View Template Properties](#) [Document Settings](#) [Publish](#) Completed:  [Prev](#)

Publishing Status: Never Published

This process step uses extensible publishing.  EXT PUB

3.4.6 MOU LIBRARY

The MOU Library step includes all relevant MOU's pertaining to this project.

- Download the MOU template document from the MOU Template step.
- Fill out the provided template with the relevant information requested.
- Attach the populated document by clicking on the included documents button below.

MOU Library 

[Save All](#) [Document Settings](#) [Reset](#) [Publish](#) Completed:  [Prev](#) [Next](#)

 The MOU Library step should include any relevant MOU's pertaining to this project.

- Download the MOU template document from the MOU Template step.
- Fill out the provided template with the relevant information requested.
- Attach the populated document by clicking on the included documents button below.

Publishing Status: Never Published

1.0* **Memoranda of Understanding**
There are no memoranda of understanding required or in force at this time.

Fill out the relevant information and include the document.

Add Included Document

Title*

Short Title:

Author:

Date*

Version:

File Location:

Add to References Appendix:

File*

Element	Description
Title	The title of the MOU.
Short Title	An extra field to add another title to the document.
Author	The author of the MOU.
Date	The date the MOU was completed.
Version	The version of the MOU.
File Location	The location of the file.
Add to References Appendix	This determines whether to add this MOU as a reference to the SP.
File	The document file to include.

3.5 GENERAL INFORMATION (VIEW AND PUBLISH THE SP, RTM, ETC.)

This task contains general information about the system. All steps in this task are repeated throughout the process but are important enough to be open in this task for updates and review.

3.5.1 RTM

The Requirements Traceability Matrix (RTM) relates requirements from requirement source documents to the security authorization process. It ensures that all security requirements are identified and investigated. Each row of the matrix identifies a specific requirement and provides the details of how it was tested or analyzed and the results.

This is a published document for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen.

Requirements Traceability Matrix (RTM)

[View Template Properties](#) [Document Settings](#) [Publish](#)

Completed:  

 The Requirements Traceability Matrix (RTM) relates requirements from requirement source documents to the security certification process. It ensures that all security requirements are identified and investigated. Each row of the matrix identifies a specific requirement and provides the details of how it was tested or analyzed and the results.

Publishing Status: **Published** 03/28/2013 20:02:57

This process step uses extensible publishing.



3.5.2 PROJECT PERSONNEL

This task defines and documents all individual personnel who have the roles and responsibilities (this is not restricted to security personnel) for the information system. This section allows for more fined grained definition of roles (e.g. system administrators, alternate information system security officers, etc.) than defined in section 2.0. DHS teams, such as the DHS Inventory team or the DHS Document Review team should not be included as they are defined by DHS already.

Project Personnel

[New](#) [Copy From](#) [Import from LDAP Server](#)

Completed:  [Prev](#) [Next](#)

 This step is used to list all personnel who participate in the assessment of the system, based on their assigned role. To create a new personnel record, click the "New" button under the page title.

Auto-copy from assigned project users:

Name ▲	Role	Organization	Office	Properties	Copy	Delete
--------	------	--------------	--------	------------	------	--------

Element	Definition
Role Name*	This field is a drop-down list of the roles available in IACS.
Title	The field is for the title of the person. This may be the official title of the person or a title related to the activities of the system.
First Name*	The first name of the person.
Middle Initial	The middle initial of the person.
Last Name*	The last name of the person.
Personnel Type	This field is a drop-down list to determine if the person is a contractor, military, or federal civil employee.
Office	The office of the person.
Office Designation	The office designation of the person.
Organization	The organization of the person.
Street Address	The address of the person's workplace.
Address Continued	

City	
State/Province	
ZIP/Postal Code	
Citizenship*	The person's citizenship status.
Phone	The phone of the person.
Secure Phone	The secure phone (if applicable) of the person.
Fax	The fax of the person.
Email*	The email of the person.

3.5.3 MANAGE PROJECT ARTIFACTS

The documents produced in support of the security authorization are referred to as "artifacts" in IACS. Each information system contains its own artifact library, which is found on the artifact page, and a site-level artifact library is available for global artifact management. Artifacts can be used to manage reference/evidence information or other activities deemed important by the ISSO and/or System Owner. As users attach documents to process steps within the project, those references will automatically be added to the information system artifact library.

Manage Project Artifacts 

Completed: 

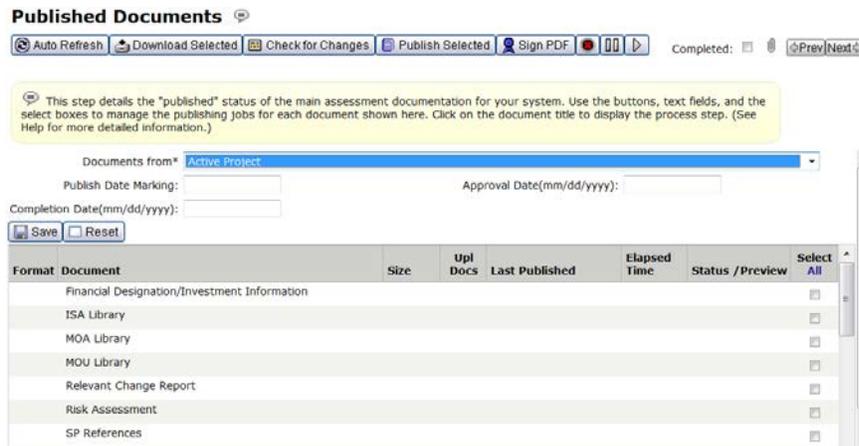
 The documents found on this page are referred to as "artifacts" in Assessment Engine. Each project contains its own artifact library, which is found on this page, and a site-level artifact library is available for global artifact management. Use this page to manage your reference/evidence information. As users attach documents to process steps within the project, those references will automatically be added to this project artifact library.

Show* -All-

File Name 	Description	Links	Date	Size (bytes)	View	Properties	Delete	Select
<div style="text-align: right; margin-bottom: 5px;">Filter: <input type="text"/> Filter History   </div>								

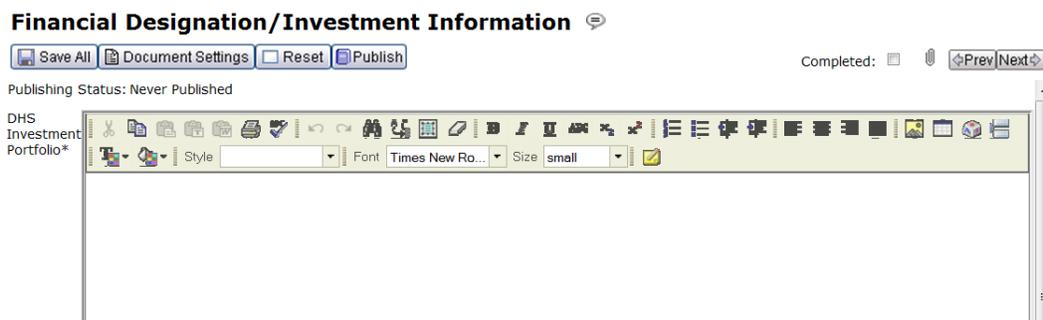
3.5.4 PUBLISHED DOCUMENTS

This step details the publishing status of the main assessment documentation for your system. It allows you to publish, track, view, and download multiple documents. The list of documents to be published is shown here along with the document size, uploaded documents, last published date, and the preview icon to view a previously published document. Use the buttons, text fields, and the select boxes to manage the publishing jobs for each document. This step is commonly used in more than one task. This allows users to create draft versions of the documents (or sections of the documents) as the project progresses, and to create final versions once the project is complete. The completed document status will be indicated on this step, as well as, the actual document page.



3.5.5 FINANCIAL DESIGNATION/INVESTMENT INFORMATION

This step is for entering DHS portfolio information for the information system. Each section is a separate text field. The capabilities of the text fields allow Microsoft Word compatible formatting.



3.5.6 PROJECT INFORMATION DETAIL

The Project Information Detail page allows the application to collect detailed project information that will be used in reporting.

Project Information Detail

Completed:  

 The Project Information Detail page allows the application to collect detailed project information that will be used in the IC IT Registry report. The information entered on this page will directly impact the IC IT Registry report.

SSP Name: Test 3-28-2013

IT Project Name:

Project ID:

Agency/Organization* Department of Homeland Security Headq

Reporting Authority* Department of Homeland Security Headq

Point of Contact:

IT System Type* Not Specified

System Location* Not Specified

System Operational:

Highest Information Category: No Marking

Lowest User Clearance: No Marking

Element	Description
SSP Name	The FISMA Name of the information system (e.g. IACS)
IT Project Name	Holds Investment Name
Project ID	Holds both OMB Exhibit & UII Code.
Agency/Organization	The component responsible for the information system.
Reporting Authority	The component responsible for the information system.
Point of Contact	The person responsible for coordinating the security activities for the information system (usually the ISSO).
IT System Type	Determines whether the system is CFO designated, financial, mixed financial, or a non-financial system
System Location	[Unknown]
System Operational	Determines whether the system is operational (granted an authority to operate).
Highest Information Category	The highest category of information contained in the system.
Lowest User Clearance	The lowest classification required for users to the system.

4.0 CREATING A PROJECT (SYSTEM OR PROGRAM)

A project is a container for a system or program in DHS. The previous tool allowed a separate container for a site. In the new IACS a site is attached to (or rather a part of) a system or program in terms of physical locations for equipment. Projects are created in IACS by the DHS Inventory Team and more information may be found at the IACS portal or the DHS Infosec helpdesk at 202-357-6100.

5.0 CATEGORIZE

5.1 CATEGORIZE INFORMATION SYSTEM

When categorizing the information system, great time and care must be invested. Important tasks are required in this section including:

- Defining the high level characteristics;
- Setting the security categorization for the confidentiality, integrity, and availability;
- Identifying and verifying
 - the personnel responsible for activities and maintenance of the system;
 - the system interfaces;
- Determining if the system contains personally identifiable information (PII) and;
- And Documenting
 - the system users;
 - the system boundary;
 - the system environment;

5.1.1 PROJECT DEFINITION

This step defines all the processes involved in the initial setup of the project in IACS.

Project Definition ⓘ

Completed:

ⓘ The project definition step prompts you to enter fundamental high-level information about the system being assessed. The information entered here will automatically appear in Section 1 of the SSP documentation.

Project Name: DHS Test System 03212013

IT System Category*

System Type*

Acronym:

Version:

Definition:

This section contains the project name, IT system category, system type, acronym, version, and a high level description of the system or program. This section is maintained by the DHS Inventory team and any changes go through the DHS Inventory change request process.

Element	Description
Project Name*	This is the Federal Information Security Management Act (FISMA) name of

	the system or program.
System Type*	The type of the system. Currently IACS only contains general support systems (GSS) and major applications (MA) which are reportable to the Office of Management and Budget (OMB) through the FISMA process.
Acronym	The common used acronym of the system or program (e.g. IACS).
Version	This is an optional field for setting the version number of the system (e.g. IACS 2.0).
Definition	This field contains a high level description of the purpose, mission, and/or scope of the system or program and Operating Location

5.1.2 SECURITY REGULATIONS

This section contains the security regulations which determine the baseline of controls for the project. This section cannot be modified.

Security Regulations

Completed: 

 The Security Regulations step allows you to select the set of regulations that will be followed for this project. Each regulation contains a group of security requirements and those requirements are validated by associated test procedures.

Short Title	Full Title	Author	Date	Requirements	Use All
NIST 800-53 w/ DHS 4300A	Department of Homeland Security Sensitive Systems Policy Directive 4300A Version 9.1	Department of Homeland Security	17 July 2012	738	<input checked="" type="checkbox"/>

5.1.3 PROJECT PERSONNEL

This task is for defining and documenting all the personnel who have responsibilities to assess the system or program. To enter personnel, please press the “New” button. Import from LDAP is not available at this time.

Project Personnel

Completed: 

 This step is used to list all personnel who participate in the assessment of the system, based on their assigned role. To create a new personnel record, click the “New” button under the page title.

Auto-copy from assigned project users:

Name ▲	Role	Organization	Office	Properties	Copy	Delete
--------	------	--------------	--------	------------	------	--------

Element	Definition
Role Name*	This field is a drop-down list of the roles available in IACS.
Title	The field is for the title of the person. This may be the official title of the person or a title related to the activities of the system.
First Name*	The first name of the person.
Middle Initial	The middle initial of the person.

Last Name*	The last name of the person.
Personnel Type	This field is a drop-down list to determine if the person is a contractor, military, or federal civil employee.
Office	The office of the person.
Office Designation	The office designation of the person.
Organization	The organization of the person.
Street Address	The address of the person's workplace.
Address Continued	
City	
State/Province	
ZIP/Postal Code	
Citizenship*	
Phone	The phone of the person.
Secure Phone	The secure phone (if applicable) of the person.
Fax	The fax of the person.
Email*	The email of the person.

5.1.4 ISSO DESIGNATION LETTER

This task contains editable sections for the ISSO designation letter. This task is broken into four sections: Designated Person, Affiliation, Designating Official, Review and Approval, Comments, and Acknowledgement of Responsibilities. Click in each of these sections and modify as needed. Afterward, click on "Save All" to save changes.

5.1.5 ISSO DESIGNATION LETTER EXTENSIBLE

This task is for publishing the ISSO Designation letter for office use and printing. To publish this document, click on "Publish."

A pop-up window will now display to specify what markings should be specified for the document. Please refer to the markings section for more information. After doing this, a link with the published date will display on this task page. To view the published document, click on the link and follow the instructions.

Report Preferences

Classification Marking Font Size: 14

Classification Marking Location: Header and Footer

Use Document Marking:

Current Classification Marks are set to:

Classifications	SCI Control Systems	Codewords
<input type="checkbox"/> LAW ENFORCEMENT SENSITIVE: <input type="checkbox"/> FOR OFFICIAL USE ONLY: <input type="checkbox"/> Protected Critical Infrastructure Information (PCI):		
Programs	NickNames	

5.1.6 SYSTEM USERS

This task is for identifying and adding users with responsibilities of the system or program in regards to operation, administration, maintenance and security. These are not individual users but rather categories of users (i.e., system administrators, patch managers, etc.). This allows minimum qualifications to users in any of these categories to be documented. To create a new system user, click on “New”

Add System User

Category*

Min. Clearance / Investigation* - Select One -

Foreign Nationals* - Select One -

Position Designation* - Select One -

Description*

Element	Description
---------	-------------

Category	This is the category or type of user. For example a system administrator.
Min. Clearance/Investigation	This is the minimum clearance or investigation level required for the user.
Foreign Nationals	This setting determines whether foreign nationals are allowed.
Position Designation	This setting determines whether the position is critical/non-critical and sensitive/non-sensitive.
Description	A brief description of the position.

5.1.7 SYSTEM BOUNDARY

This task defines all computers and related equipment within a location(s), defined under the System Environment step, along with the internal and external connections (e.g., a router and all systems connected to its local-area ports). Graphical representations of the system boundary may also be uploaded here.

System Boundary

Completed:

 Define all computers and related equipment within the location(s), defined under the System Environment step, along with the internal and external connections (e.g., a router and all systems connected to its local-area ports).



5.1.8 SYSTEM DATA FLOW

This task defines the routes by which the data flows through the system (e.g., flow of information between database servers and application servers; local network connections for backup or system mirroring; flow of routine e-mail traffic, etc.). Select New to name and define the different types of data flows used by your system.

Element	Description
Name*	The name of the service or daemon.
Port	The port the service communicates with
Protocol	The protocol the service uses (e.g. TCP/UDP).
Description	The description of the service. This should be as descriptive as possible.

Add System Data Flow

Name*

Port:

Protocol:

Description:

5.1.9 SYSTEM INTERFACES/INTERCONNECTIONS

This task defines the physical and logical external connections, or system interfaces, used by your system. Explain how the system interacts with other systems or networks. The System Interfaces entered will appear in the SP documentation.

Add System Interface

Specify Interface*

Name*

Description:

Port:

Protocol:

Organization:

Interface Type:

Connection Agreement Type:

Connection Agreement Date (mm/dd/yyyy):

FIPS 199 Category:

System C&A Status:

Element	Description
Specify Interface	This is a drop-down menu to identify whether the interface is Cross Domain

	Solution or not.
Name	The name of the interface
Description	A detailed description of the interface.
Port	The port or port range of the interface.
Protocol	The protocol(s) used for the interface.
Organization	The organization of the interface. This is not the organization of the system but the interface the system connects with.
Interface Type	The type of the interface.
Connection Agreement Type	The type of agreement used between both parties (e.g. MOU).
Connection Agreement Date	The date the agreement was signed and went into effect.
FIPS 199 Category	The security impact level of the interface based on FIPS 199.
System C&A Status	The security authorization status of the other system in the agreement.

5.1.10 SYSTEM ENVIRONMENT

The System Environment task defines the environments or locations in which the system operates and to adjust the threat levels associated with each location/environment. A default location is provided as the "main location" of the system being assessed. This information is published in the Risk Assessment documentation.

To modify the default, click on the “Properties” icon.

Name ▲	Description	Category	SCIF Certified	TEMPEST Certified	Weight	View	Test	Default	Properties	Copy	Delete
Main Location	Main Location		No	No	Medium		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			

To create a new environment, click on the “New” icon.

Edit System Location 'Main Location'

General
Threats
Geography

Name*

Description:

Weight*

Include Location in Test Plan:

General
Threats
Geography

Name	Group ▲	Weight
Humidity	Environment Failure	Medium ▼
Power	Environment Failure	Medium ▼
Sand/Dust	Environment Failure	Medium ▼
Temperature	Environment Failure	Medium ▼
Vibration/Shock	Environment Failure	Medium ▼

General
Threats
Geography

Site:

Building:

Room:

City:

State:

Country:

Category:

SCIF Certified:

TEMPEST Certified:

Tab	Element	Description
General	Name	The name of the location or environment.
	Description	A detailed description of the environment.
	Weight	The risk impact of the environment.
	Include Location in	Determines whether or not to include this site in the

	Test Plan	security assessment (test) plan.
Threats	Multiple	Weight of threats by the impact level and likelihood of threats occurring.
Geography	Site	The name of the site where the information system is housed.
	Building	The name of the building where the information system is housed.
	Room	The room name and/or number of where the information system is housed. The purpose is to easily identify the location of the system.
	City	The city where the information system is located.
	State	The state where the information system is located.
	Country	The country where the information system is located.
	Category	This is a drop-down to select the category of the site or location.
	SCIF Certified	This determines if the location is a certified SCIF.
	TEMPEST Certified	This determines if the location is TEMPEST certified.

5.1.11 PROJECT MILESTONES

The Project Milestones task is used to create a plan or project schedule for the security assessment of the system. It should identify all major milestones that should be reached with either approximate or exact dates. This task is updated throughout the process. To make this task easier, there is a function to export and import from Microsoft Excel.

The suggested method for this task is to click on the export button, fill out the excel spreadsheet, and import it into IACS.

Project Milestones 

Completed: 

 Project Milestones are used to outline a plan or project schedule for assessing a system. Identify all major milestones that should be reached for your assessment and an approximation or exact date that the milestone will be reached. The information entered here can be updated throughout the assessment process.

Title	Start Date	Completion Date	Properties	Copy	Delete	Select
Kick-off	03/01/2013	03/01/2013				<input type="checkbox"/>
Risk Categorization	03/02/2013	03/10/2013				<input type="checkbox"/>
Control Selection	03/10/2013	03/10/2013				<input type="checkbox"/>
Implement Controls	03/11/2013	03/30/2013				<input type="checkbox"/>

5.1.12 SYSTEM DATA TYPES

This task is for categorizing system information types. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management), defined by the organization or, in some instances, by a public law, executive order, directive, policy, or regulation.

System Data Types

Completed:

An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management), defined by the organization or, in some instances, by a public law, executive order, directive, policy, or regulation. (See Help for more details.)

Name ▲	Description	Type	Confidentiality	Integrity	Availability	Properties	Copy	Delete	Select All
Survey People, Places, and Things - 1	Survey People, Places, and Things - 1		Moderate	Moderate	Moderate				

To add a data type click on new.

Add Data Type

Name*

Description:

Data Type*

Confidentiality*

Integrity*

Availability*

Privacy Act Data:

If a Data Type contains Privacy Act information, then the Confidentiality setting should be Moderate or High.

Element	Description
Name	The name of the data type
Description	The description of the data type
Data Type	A drop-down selection of data types for DHS
Confidentiality	The confidentiality value of the data type.
Integrity	The integrity value of the data type.
Availability	The availability value of the data type.
Privacy Act Data	Determines whether the data type is covered by the privacy act.

5.1.13 REQUIREMENTS QUESTIONNAIRE

This task contains questions about the system being assessed to determine if requirements are applicable or not. If no questions are listed on this page, then no further action is required. For

the questions listed, answer them by selecting Yes or No and then save. Throughout the assessment process, if changes are made to the project information, these questions may need to be reviewed again. The results of this questionnaire will help determine the requirement's applicability as shown on the System Security Requirements page and the Security Controls Compliance Matrix (SCCM).

Question ▲	Yes	No
⚠ Is this a CFO designated financial system?	<input checked="" type="radio"/>	<input type="radio"/>

5.1.14 SYSTEM SECURITY

The System Security task defines the information technology security parameters and the depth of testing that is to be performed on the components of the system being authorized based upon the FIPS 199 security categorization. This information is used to calculate the system's protection level, which determines the type and intensity of the testing that will be performed.

The values are calculated via two modes—auto and manual. In auto mode, the values are determined by the system data types from the “System Data Types” task. In manual mode, the values may be changed. If the values are changed, a reason must be entered to justify the change.

Confidentiality:	<input type="text" value="Moderate"/>	<input type="text"/>
Integrity:	<input type="text" value="Moderate"/>	<input type="text"/>
Availability:	<input type="text" value="Moderate"/>	<input type="text"/>

5.1.15 E-AUTHENTICATION

This task defines the e-authentication level of the system. The determination of the e-authentication level is performed outside of the tool via the e-authentication workbook. Enter the value from the workbook here and upload the workbook itself as an artifact.

Please select the eAuthentication Assurance Level as determined after completing the eAuthentication Workbook. Upload the completed workbook on this page as an artifact.:

5.2 INITIAL PRIVACY THRESHOLD ANALYSIS

The privacy threshold analysis (PTA) is a document used to determine if privacy identifiable information (PII) data is stored or processed in the system. In the past, the PTA was a separate document; however, now it is captured by the tool.

Initial Privacy Threshold Analysis

Completed: 

Please use the whiteboxes below to fill out the Privacy Threshold Analysis (PTA) form.

Publishing Status: Never Published

Summary Information*

Project or Program Name:	<i>[Enter Text]</i>		
Component:	Department of Homeland Security Headquarters (DHS HQ)	Office or Program:	<i>[Enter text]</i>
FISMA Name:	Test 3-28-2013	FISMA Number:	[FISMA Number Not Specified]
Type of Project or Program:	<i>[Enter text]</i>	Project or Program Status:	Operational

Click on each individual section and fill out as appropriate. When finished, click on save all at the top of the page.

5.3 FINAL PRIVACY THRESHOLD ANALYSIS

5.3.1 DHS PRIVACY CHECKLIST

The DHS Privacy Checklist is a checklist which determines the privacy documents that are required.

Minimum Security Checklist Questionnaire

Number ^	Question	N/E	Yes	No	N/A	Notes
1.0	Is this a Privacy Sensitive System?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
2.0	Please identify the category of system by answering the questions below:					
2.1	Is this an IT System?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	

5.3.2 COMPLETE PRIVACY THRESHOLD ANALYSIS

This task defines the final portion of the PTA. The DHS privacy reviewer enters the information in this task.

PIA Upload

Completed: 

Has this system's PIA been uploaded?:

5.4.2 SORN UPLOAD

Select whether a PIA has been uploaded. Click on the paperclip to upload the PIA.

SORN Upload

Completed: 

Has the system's SORN been uploaded?:

6.0 SELECT

Once a system has been defined and categorized, control selection takes place. The activities during the **Select Security Controls** task include:

- **Identify applicable controls/requirements.** The controls available for selection and implementation are based upon the FIPS 199 security categorization levels and other requirements (i.e. CFO designated system) identified during the Categorize Information System task.
- **Generate relevant draft documentation.** Once the full set of applicable requirements has been selected for the system, the draft Requirements Traceability Matrix (RTM) is published.

The responsibility for completing this task belongs to the ISSO role who has been assigned read and write access to the task.

The Select Security Controls task is approved by the ISSO.

The ISSM and the ISSO will receive notifications in their inboxes when the task is approved or ready for approval as well as when the task is activated or not approved.

To approve the Select Security Controls task, the ISSO should first ensure all data in the task is accurate and complete. Each process step should be marked as completed. When the task is ready to be approved, click the approval icon, provide any necessary notes and click Save.

At this point, any necessary notifications will be sent out and the next task, RATC Approval, will become available.

6.1 SELECT SECURITY CONTROLS

6.1.1 ORGANIZATIONALLY DEFINED REQUIREMENTS

This step defines the requirement assignment questions that are used to collect specific information that vary from organization to organization (e.g., number of login attempts allowed, how often a plan is updated). All of the questions on this page are based on DHS guidance (e.g., 3 attempts, 90 days). The answers are added automatically to the associated requirement, identified by the paragraph number in the brackets at the end of the question. The answers replace existing text, such as [Assignment: organization-defined time period].

Organizationally Defined Requirements

Completed:

ⓘ This step contains requirement assignment questions that are used to collect specific information that vary from organization to organization (e.g., number of login attempts allowed, how often a plan is updated). Answer all of the questions on this page, based on your organization's guidance (e.g., 3 attempts, 90 days). The answers will be added automatically to the associated requirement, identified by the paragraph number in the brackets at the end of the question. The answers replace existing text, such as [Assignment: organization-defined time period]. Note: Only questions associated to applicable requirements are displayed on this page.

Question	Answer
⚠ According to which conditions does the organization re-screen individuals (where re-screening is so indicated, indicate the frequency of such re-screening)? [provide a list (e.g., individual entering an SCIF, etc.)] [PS-3]	Every five years for high risk posi
⚠ At least how many number of characters must be changed before the information system allows the creation of new passwords? [provide a number (e.g., 4)] [IA-5(1)]	
⚠ How long does it take the organization to initiate the transfer or re-assignment actions? [provide a time period (e.g., one day)] [PS-5]	At least one year
⚠ How long does it take the organization to mediate legitimate vulnerabilities? [provide a time period (e.g., within 24 hours)] [RA-5]	Within 60 days
⚠ How long does the organization prevent the reuse of user or device identifiers? [provide a time period (e.g., 30 days)] [IA-4]	
⚠ How long does the organization retain audit records to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements? [provide a time period (e.g., one year)] [AU-11]	90 days online and 7 Years in tota
⚠ How long does the organization retain individual training records? [provide a time period (e.g., 1 year)] [AT-4]	For the lifetime of the information
⚠ How many number of password generations must pass before the information allows the reuse of a password? [provide a number (e.g., 5)] [IA-5(1)]	0

6.1.2 SYSTEM SECURITY REQUIREMENTS

The System Security Requirements task displays the security requirements that have been selected for the assessment of your system. The requirements are derived from regulations that were selected in Manage Regulations. These may include international and government security regulations, policies and practices, as well as locally defined security requirements. Requirements may be added with justifications.

System Security Requirements

Completed:

ⓘ The System Security Requirements step displays the security requirements that have been selected for the assessment of your system. The requirements are derived from regulations that were selected in Manage Regulations. These may include international and government security regulations, policies and practices, as well as locally defined security requirements.

Regulation:

Regulation	Paragraph/ReqID	Requirement	Security Category	IC	View	Notes	OvLy	Lock	Appl
NIST 800-53 w/ DHS 4300A	AC-1	Access Control Policy and Procedures	Access Control Policy and Procedures					<input type="checkbox"/>	<input checked="" type="checkbox"/>
NIST 800-53 w/ DHS 4300A	AC-2	Account Management	Account Management					<input type="checkbox"/>	<input checked="" type="checkbox"/>

6.1.3 RTM

The Requirements Traceability Matrix (RTM) relates requirements from requirement source documents to the security authorization process. It ensures that all security requirements are identified and investigated. Each row of the matrix identifies a specific requirement and provides the details of how it was tested or analyzed and the results.

This is a published document for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. Please refer to the markings section for more information.

Requirements Traceability Matrix (RTM)

[View Template Properties](#) [Document Settings](#) [Publish](#)

Completed:  

 The Requirements Traceability Matrix (RTM) relates requirements from requirement source documents to the security certification process. It ensures that all security requirements are identified and investigated. Each row of the matrix identifies a specific requirement and provides the details of how it was tested or analyzed and the results.

Publishing Status: Published 03/28/2013 20:02:57

This process step uses extensible publishing.



7.0 IMPLEMENT

Once security controls are selected, it is necessary to implement them for the information system. This formalizes plans and expectations regarding the overall security of the information system. The description of the security control implementation includes planned inputs, expected behavior, and expected outputs where appropriate, typically for those technical controls that are employed in the hardware, software, or firmware components of the information system. At a minimum, the security control address the, what, where, who and how often questions. That is, what is the process for implementing and ensuring the control is in place and effective. Where is the process taking place (both physically and logically within the system). Who is involved in the process (i.e. a system administration applying patches to a system), and how often is this performed to ensure the control remains effective (e.g. patches are applied monthly). Documentation of security control implementation allows for traceability of decisions prior to and after deployment of the information system. The level of effort expended on documentation of the information system is commensurate with the purpose, scope, and impact of the system with respect to organizational missions, business functions, and operations.

7.1 IMPLEMENT SECURITY CONTROLS

Once a system has been granted an RATC, control implementation can occur in order to prepare for testing.

The activities you will encounter during the **Implement Security Controls** task include:

- **Identify equipment and software.** Once the applicable control set has been determined, IACS generates the test plan used to validate the controls.
- **Determine implementation status of control.** The implementation status of each of the applicable controls will be evaluated. The status of each control can be either “Planned”

or “Inherited.” Additionally the application allows for the status of a control to be inherited from another system and/or project.

- **Review system information.**
- **Generate SP documentation.** Modify the SP and publish a new draft using the extensible publishing step.

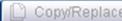
The responsibility for completing this task belongs to the ISSO. The task is approved by the ISSO.

To approve the task the ISSO should ensure all data is accurate and complete. When ready to be approved, the ISSO will click the approval icon, provide any notes and click Save.

7.1.1 EQUIPMENT GROUP

Equipment groups should be defined for each location within the project. It is important to define the equipment groups, before importing the equipment, to both provide a process for grouping the equipment inventory during the import and for easily categorizing the components of the information system. The ISSO can use the default set of groups provided here or simply add/modify the equipment groups to best fit the individual system environment.

Equipment Groups 

 New  Copy/Replace  Delete Selected

Completed:  

 A default set of the basic equipment groups is defined here. Equipment groups should be defined for each location within the project. It is important to define the equipment groups, before importing the equipment, to provide a process for grouping the equipment inventory during the import. You can use the default set of groups provided here or simply add/modify the equipment groups to best fit your system environment.

Group Name ▲	Location	Description	Equipment To Test	Properties	Copy	Delete
Mainframes	Main Location		0/0			
Networking Equipment	Main Location		0/0			
Unix Servers	Main Location		0/0			
Unix Workstations	Main Location		0/0			
Windows Laptops	Main Location		0/0			
Windows Servers	Main Location		0/0			

To add a new equipment group, click on new. To modify an existing equipment group, click on properties.

Add Equipment Group

 Save  Reset  Close

Group Name* OS X Servers

Description: OS X Servers.

Manufacturer: Apple

Model:

OS: 10.8.3

Location* Offsite

Weight* Medium

Host Name Display Pattern* {\$name}

Equipment To Test

Name ▲	Sele
	All

Name	Description
Group Name	The name of the group. This should be as general as possible.
Description	A description of the equipment group.
Manufacturer	The manufacturer of the equipment group.
Model	The model (usually model number) of the group.
OS	The operating of the equipment group if applicable.
Location	The physical location of the equipment group. The locations are created in the categorize phase.
Weight	The risk weight of the equipment group.

7.1.2 EQUIPMENT INVENTORY

Define specific details of all computers, servers, printers that exist within the boundary of the information system. This step allows either manual entry of equipment or import an inventory list directly into the project, such as a Nessus scan file. Each individual piece of equipment can be characterized in detail, including hardware description, network address, operating system, information on installed software applications, and indication if the equipment will be tested. This information is used to build the appropriate equipment tests defined in the test plan for the system.

Equipment Inventory ⓘ

Completed: ⓘ

ⓘ Define specific details of all computers, servers, printers that exist within the boundary of your system. This step allows you to manually enter equipment or import an inventory list directly into the project, such as the Xacta Detect scan file. Each individual piece of equipment can be characterized in detail, including hardware description, network address, operating system, information on installed software applications, and indication if the equipment will be tested. This information is used to build the appropriate equipment tests defined in the test plan for the system.

Host Name (IP) ▲	Group Name	Last Updated	Test	Properties	Vulnerable	Copy	Delete	Se
1-DHS-Server	Windows Servers	04/11/2013 10:30:54	✓	ⓘ		📄	✖	

To add equipment inventory, click on new.

Edit Equipment '1-DHS-Server'

General	Detail	Installed Software	Vulnerabilities	Point of Contact 1	Point of Contact 2
Group* <input type="text" value="Windows Servers"/>					
Host Name* <input type="text" value="1-DHS-Server"/>					
Manufacturer: <input type="text" value="HP"/>					
Model: <input type="text" value="HP1XA001"/>					
IP Address: <input type="text" value="1.2.3.4"/>					
MAC Address: <input type="text" value="a1b2c3"/>					
Serial No: <input type="text" value="0000000-1"/>					
Visual ID: <input type="text" value="100000001"/>					
Agent Id: <input type="text"/>					
Test This Equipment: <input checked="" type="checkbox"/>					
Description: <input type="text" value="The main server."/>					
IA Enabled: <input checked="" type="checkbox"/>					
CC Eval Status: <input type="text" value="N/A"/>					
Function: <input type="text" value="The main server"/>					
Equipment Class* <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Any <input type="checkbox"/> Computer <input type="checkbox"/> Other <input type="checkbox"/> Printer <input checked="" type="checkbox"/> Servers 					

Tab	Element	Description
General	Group	The equipment group of the item.
	Host Name	The host name of the equipment.
	Manufacturer	The name of the company that manufactured the equipment.
	Model	The model (typically model number) of the equipment.
	IP Address	The IP address of the equipment.
	MAC Address	The MAC address of the equipment.
	Serial No.	The serial number of the equipment.
	Visual ID	An ID that can be used for equipment tracking (e.g. an asset ID tag).
	Agent Id	Asset Id
	Test This Equipment	Determines whether a test plan should be created in IACS for the equipment.
	Description	A description of the equipment and mission.
	IA enabled	[UNKNOWN]
	CC Eval Status	[UNKNOWN]
General	Function	A description of the equipment's function.
	Peripherals	A list of the peripheral equipment attached.
Detail	Select Property	A dropdown of the properties associated with the equipment.
Installed Software	Operating system	The operating system of the equipment. This is a drop-down list. The application list is populated from the managed software step.
Vulnerabilities	N/A	This page is populated from a scan.
Point of Contact 1	Title	The title of the contact.
	Name	The name of the contact
	Organization	The organization of the contact (e.g. Data Center)

	Location	The physical location of the contact.
	Phone	The phone number of the contact.
	Email	The email of the contact.
Point of Contact 2	Title	The title of the contact.
	Name	The name of the contact
	Organization	The organization of the contact (e.g. Data Center)
	Location	The physical location of the contact.
	Phone	The phone number of the contact.
	Email	The email of the contact.

7.1.3 MANAGE SOFTWARE

The Manage Software step is initially blank. When equipment is imported into the project, all the installed software (detected from the scan) will be displayed here along with the associated equipment count. A manual entry of software is also available in this step. Review the list of software applications and make any necessary modifications. Since software applications are directly linked to equipment inventory and test procedures, this ensures the appropriate test procedures are pulled on the Test Plan & Results step, under the Vulnerability Assessment and Testing task. This step is one instance of the same page – changes will appear in each instance under different tasks.

Manage Software

Completed:  

 The Manage Software step is initially blank. As equipment is imported into the project, all installed software, detected from the scan, will be displayed here along with the associated equipment count. Review the list of software applications and make any necessary modifications. Since software applications are directly linked to equipment inventory and test procedures, this ensures that the appropriate test procedures are pulled on the Test Plan & Results step, under the Vulnerability Assessment and Testing task. (See Help for more detailed information.) The Manage Software process step is one instance of the same page – changes will appear in each instance under different tasks.

-All-

		Filter:		Filter History					
Application ▲	Type	Category	Alias Count	Equip. Count	Approved	Publish All	Properties	Copy	De

To manually add software, click on new.

Add Software Application

General
Aliases

Name*

Vendor:

Version:

Type* Unknown

DADMS #:

FAM Status:

CC Eval Status:

Description:

IA Enabled?:

Admin Tool?:

Category:

Element	Description
Name	The name of the software
Vendor	The name of the software vendor
Version	The version number of the software.
Type	The type of software.
DADMS #	[UNKNOWN]
CC Eval Status	[UNKNOWN]
Description	A brief description of the software.
IA Enabled?	Determines if the software is IA enabled.
Admin Tool?	Determines if the software is used as an admin tool.
Category	The category of the software.

Once saved, clicking on the alias tab will let the ISSO enter alias information about the software.

7.1.4 CONTROLS IMPLEMENTATION

This step is used to define the implementation details for the NIST 800-53 and DHS 4300A controls. As changes and updates are made here, the information will automatically be populated in the appropriate SP sections.

NIST 800-53 w/ DHS 4300A											
Applicability Filter: Applicable Only										Filter: <input type="text"/>	
Paragraph/ReqID ▲	Title	Class	Type	Inheritance	Status	Priority	Responsible Entities	Implementation	Estimated Completion	View	Propertie
AC-1	Access Control Policy and Procedures	Technical			Implemented	P1	DHS CISO	This control may...			
AC-2	Account Management	Technical				P1					

Make updates by selecting the Properties icon for each requirement.

Edit Requirement 'AC-2 Account Management'

Type: System-Specific
Status: Implemented
Priority: P1

Responsible Entities:

Implementation:

Estimated Completion Date (mm/dd/yyyy):
Notes:

Element	Description
Type	The type of the control (system specific, hybrid, common, inherited & not specified.).
Status	The implementation status of the control.
Priority	The priority or sequencing of the control. Higher priority controls are to be implemented first.
Responsible Entities	The responsible entity field is used to store the control from the system it is inheriting from.
Implementation	The detailed description of the implementation of the control.
Estimation Completion Date	The estimated date when the control will be implemented.
Notes	Any extra notes or comments about the control implementation.

7.1.5 REVIEW SYSTEM USERS

Here, the ISSO can review and modify the system users identified in the categorization phase. Please refer to section 6.1.6.

7.1.6 REVIEW SYSTEM BOUNDARY

The ISSO can review the system boundary and make modifications if the boundary has changed from the categorization phase. Please refer to section 6.1.7 for more information..

7.1.7 REVIEW SYSTEM DATA FLOW

The ISSO can review the system data flow and make modifications if the data flow has changed from the categorization phase. Please refer to section 6.1.8 for more information..

7.1.8 REVIEW SYSTEM INTERFACES/INTERCONNECTIONS

The ISSO can review the system interfaces and interconnections and make modifications if they have changed from the categorization phase. Please refer to section 6.1.8 for more information..

7.1.9 REVIEW SYSTEM ENVIRONMENT

The ISSO can review the system environment and make modifications if they have changed from the categorization phase. Please refer to section 6.1.9 for more information.

7.1.10 PORTS, PROTOCOLS, AND SERVICES

This step identifies all the data ports, protocols, and services used by the information system.

The ISSO can either enter the data manually or import from the Excel spreadsheet provided by the export feature. To create a new entry manually, click on new.

Add Ports, Protocols and Services Item

Description/Service*

Reference:

Host:

Port:

Protocol:

Source Name/IP:

Destination Name/IP:

Direction:

Classification:

UTNP/CTNP:

Element	Description
Description/Service	The name or description of the service (e.g. SMTP)
Reference	A reference name to the service.
Host	The host of the service. The host name is preferred but the IP address can be used if the host name is unavailable.
Port	The port or port range the service uses.
Protocol	The name of the protocol the service uses.
Source Name/IP	The host name or IP of the source device.
Destination Name/IP	The host name or IP of the destination device.
Direction	The direction the service flows (inbound, outbound, or both).
Classification	The classification or markings associated with the protocol. Please keep in mind the environment of IACS to prevent security incidents from occurring.
UTNP/CTNP	Determines if UTNP/CTNP is used.

7.1.11 SECURITY PLAN REFERENCES

The SP References step contains a list of the regulations and/or checklists used for the assessment. These references are automatically pulled based on the selected regulations on the Manage Regulations step. Review the references listed here or add additional references to be included in the references table of the security plan.

7.1.12 SECURITY PLAN

This step is for entering the sections of the SP not associated with the controls. Each section is a separate text field. The capabilities of the text fields allow Microsoft Word compatible formatting.

Security Plan

Completed:

Publishing Status: Never Published

Document Change History*

Version	Date	Author	Description

Component's Address*

[DO NOT TYPE in the gray column. Provide response in the second column.]

Component's Address

7.1.13 SECURITY PLAN EXTENSIBLE

This step is used to publish the SP for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. Please refer to the markings section for more information.

Security Plan Extensible

 View Template Properties  Document Settings  Publish

Completed:  

Publishing Status: Never Published

This process step uses extensible publishing.



7.2 CONTINGENCY PLAN

This task is used to develop and publish the Contingency Plan (CP). The CP task stays open until the Authorize task is completed and ready for approval in order to ensure the system is updated and current just prior to receiving an ATO decision, allowing users to provide information security updates during the accreditation package development. Once the Authorize task is completed the Information Security Monitoring task will need to be approved first in order for the AO to make a decision. In the CP task, there is only one process step to complete before notifications are sent out. The ISSM and/or the ISSO are responsible for the task as each of their roles have read and write access to it.

Recall, The CP task stays open until the Authorize task is ready for approval in order to ensure the system is updated and current just prior to receiving an ATO decision. Once the Authorize task is completed the CP task will need to be approved first in order for the AO to make a decision.

The CP task is approved by either the ISSM or the ISSO and the Gov. only ISSM. This means two approvals are needed for this task. The ISSM, ISSO, and Gov. only ISSM will receive notifications in their inboxes when the task is approved or ready for approval as well as when the task is activated or not approved.

To approve the Information Security Monitoring task, the ISSM, ISSO, and Gov. only ISSM should first ensure the Information Security Monitoring is up to date, accurate, and complete. The CP process step should be marked as completed. When the task is ready to be approved, click the approval icon, provide any necessary notes and click Save.

At this point, notifications will be sent out and the AO can proceed with approving the Authorize task.

The CP task is divided into several steps which correspond to sections in the CP. Each section is a separate text field. The capabilities of the text fields allow Microsoft Word compatible formatting. The remake button will return the section to the original text.

7.2.1 CONTINGENCY PLAN (SECTIONS 1-2)

7.2.2 CONTINGENCY PLAN (SECTION 3-5)

Contingency Plan (Sections 3-5) 

    Completed:

 The Contingency Plan establishes procedures to recover the system following a disruption.

Publishing Status: Never Published

Damage Assessment Procedures*

Damage Assessment Procedures:
(Detailed procedures should be outlined to include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical status of physical infrastructure; status of information system equipment functionality and inventory, including items that will need to be replaced; and estimated time services to normal operations).

- Upon notification from the [SYSTEM OWNER/CONTINGENCY PLAN COORDINATOR], the DAT is to ...
- The [DAT] is to ...

Alternate

7.2.3 CONTINGENCY PLAN (SECTION 6-7)

7.2.4 CONTINGENCY PLAN EXTENSIBLE

This step is used to publish the CP for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. Please refer to the markings section for more information.

Contingency Plan Extensible 

   Completed:  

 The Contingency Plan establishes procedures to recover the system following a disruption.

Publishing Status: Never Published

This process step uses extensible publishing.


EXT PUB

7.3 CONTINGENCY PLAN TEST

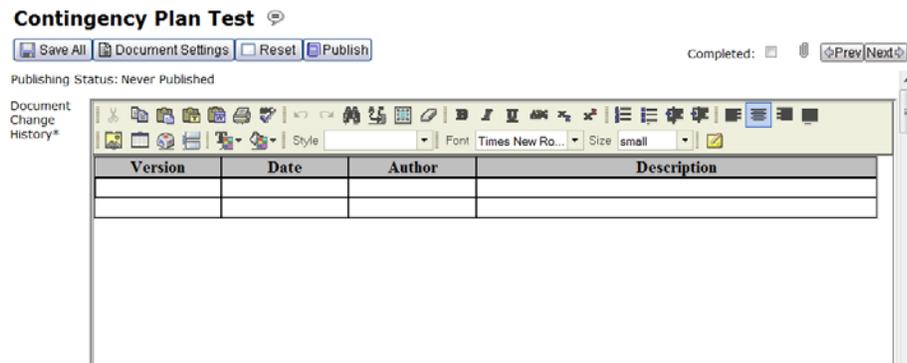
This task is used to develop and publish the Contingency Plan Test (CPT). The CPT task stays open until the Authorize task is completed and ready for approval in order to ensure the system is updated and current just prior to receiving an ATO decision, allowing users to provide

information security updates during the accreditation package development. Once the Authorize task is completed the CPT task will need to be approved first in order for the AO to make a decision. In the CPT task, there is only one process step to complete before notifications are sent out. The ISSM and/or the ISSO are responsible for the task as each of their roles have read and write access to it.

The CPT task ensures a contingency plan is tested and documented for the DHS security authorization package. A CPT is performed yearly and updated with the test results. If necessary, the CP and SP are also updated to reflect the findings from the CPT.

7.3.1 CONTINGENCY PLAN TEST

This step is for the ISSO to enter in the CPT results. The CPT step is divided into several sections which correspond to sections in the CPT. Each section is a separate text field. The capabilities of the text fields allow Microsoft Word compatible formatting. The remake button will return the section to the original text.



7.3.2 CONTINGENCY PLAN TEST EXTENSIBLE

This step is used to publish the CPT for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. Please refer to the markings section for more information.



7.4 CONFIGURATION MANAGEMENT PLAN

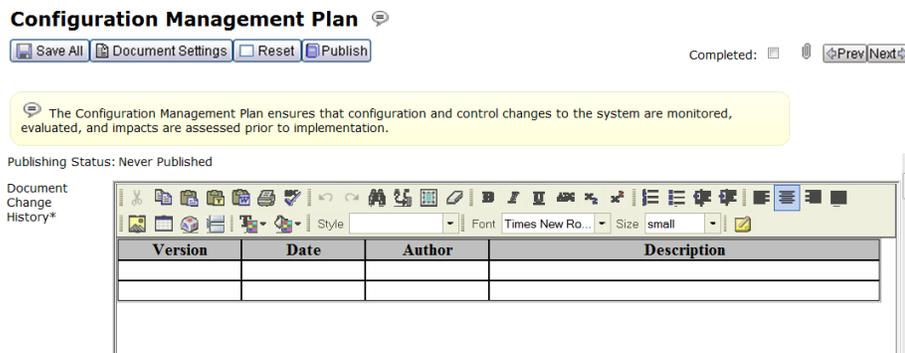
This task is used to develop and publish the Configuration Management Plan. The task stays open until the Authorize task is completed and ready for approval in order to ensure the system is updated and current just prior to receiving an ATO decision, allowing users to provide information security updates during the accreditation package development. Once the Authorize

task is completed the CPT task will need to be approved first in order for the AO to make a decision. In the CPT task, there is only one process step to complete before notifications are sent out. The ISSM and/or the ISSO are responsible for the task as each of their roles have read and write access to it.

The Configuration Management Plan task ensures a configuration management plan is developed and implemented for the DHS security authorization package. A configuration management plan should be examined and updated yearly. If necessary, SP and other relevant documentation should be updated to reflect the changes in the configuration management plan.

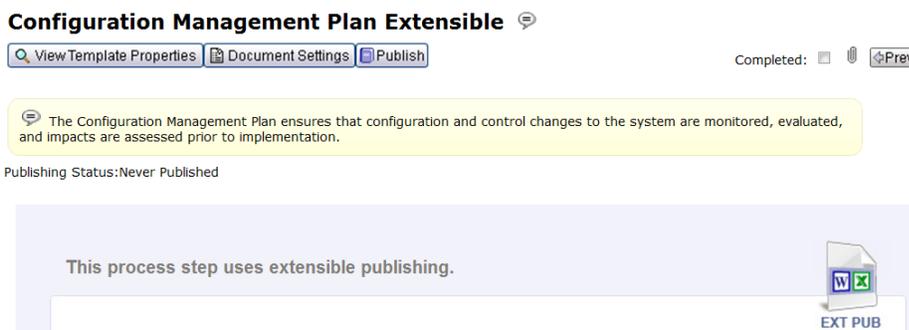
7.4.1 CONFIGURATION MANAGEMENT PLAN

The Configuration Management Plan ensures that configuration and control changes to the system are monitored, evaluated, and impacts are assessed prior to implementation. This step is divided into several sections which correspond to sections in the configuration management plan. Each section is a separate text field. The capabilities of the text fields allow Microsoft Word compatible formatting. The remake button will return the section to the original text.



7.4.2 CONFIGURATION MANAGEMENT PLAN EXTENSIBLE

This step is used to publish the configuration management plan for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. (This is usually For Official Use Only (FOU)).



8.0 ASSESS

Assessing the security controls using appropriate processes and procedures help to determine to the extent which the controls are implemented correctly, operating as intended, and producing the desired and expected outcome to meet the security requirements of the information system.

8.1 SELF-ASSESSMENT

Recall, we are now beginning the Assess Phase where we will assess the controls put in place in the Implementation phase 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. The first task we will encounter is the **Self-Assessment** task. The self-assessment is conducted as an initial test by the host to get a basic understanding of the system's security posture. When self-assessment is complete, security assessment is conducted.

In this task, the host will:

- Review the test matrix and requirement information to ensure the right controls are present and understand what needs to be tested.
- Perform the initial tests and analysis and enter the results.
- Create the Security Assessment Plan and Procedures (P&P), which outlines how and when the system should be tested and the resources required. This document will be referenced by the operational testing team during the Operational Testing task.

All roles have access to the task, but only the ISSO has read/write access. The task is primarily maintained by the ISSO. When this task is complete, a period of time is allotted for scheduling the tests. When the schedule is complete, operation testing begins.

The ISSO and the SCA will be notified when the task is approved or ready for approval. The ISSO and the SCA will also be notified when the task is activated or not approved.

At this point, the security assessment in the self-testing task will be complete. The test results in the security assessment will continue to be refined and updated during operational testing.

8.1.1 PROJECT TEST MATRIX

The project test matrix provides a detailed overview of the requirements and associated test procedures included in the test plan for the information system. This saves time and effort required to manually search through the test plan for this information. It provides a detailed summary of applicable test procedures and an explanation of those tests that are not applicable due to equipment type, equipment scope, etc.

Project Test Matrix



Completed: [Prev](#) [Next](#)

This test matrix provides a detailed overview of the requirements and associated test procedures included in the test plan for your system. This saves you the time and effort required to manually search through the Test Plan for this information. Take some time to review the information displayed here, which provides a detailed summary of applicable test procedures and an explanation of those tests that are not applicable due to equipment type, equipment scope, etc.

Total/Applicable Tests: 389 / 389 Total/Testable Locations: 2 / 0 Total System Tests: 390 Total Location Tests: 0
Total/Testable Equipment: 1 / 1 Total Equipment Tests: 0 Total Tests To Execute: 390

REQUIREMENT		TEST GRPS	TEST PROC	SUBJECTS			TOTAL	
Regulation	Paragraph/ReqID	Requirement	Assoc/Appl	Assoc/Appl	System	Location	TP/Equip	Tests
NIST 800-53 w/ DHS 4300A	AC-1	Access Control Policy and Procedures	2 / 2	6 / 3	3			3
NIST 800-53 w/ DHS 4300A	AC-2	Account Management	1 / 1	3 / 1	1			1
NIST 800-53 w/ DHS 4300A	AC-2[1]	Account Management	1 / 1	3 / 1	1			1

8.1.2 RTM

The Requirements Traceability Matrix (RTM) relates requirements from requirement source documents to the security authorization process. It ensures that all security requirements are identified and investigated. Each row of the matrix identifies a specific requirement and provides the details of how it was tested or analyzed and the results.

This is a published document for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen.

Requirements Traceability Matrix (RTM)

[View Template Properties](#) [Document Settings](#) [Publish](#)

Completed:

The Requirements Traceability Matrix (RTM) relates requirements from requirement source documents to the security certification process. It ensures that all security requirements are identified and investigated. Each row of the matrix identifies a specific requirement and provides the details of how it was tested or analyzed and the results.

ublishing Status: Published 03/28/2013 20:02:57

This process step uses extensible publishing.



8.1.3 SECURITY ASSESSMENT

This step displays the test plan developed for the information system based on the information provided in earlier steps. The test procedures shown are associated to the applicable requirements and ready to be executed. The ISSO enters the results of the testing/analysis by clicking the test title and entering the results and other pertinent information. All automated equipment tests (if applicable) can be answered by clicking the "Auto Test" button near the top of the screen.

Security Assessment

Save Reset Auto Test Import Export Completed: Prev Next

Displayed is the test plan developed for your system based on the information provided in earlier steps. The test procedures shown here are associated to the applicable requirements and ready to be executed. Enter the results of the testing/analysis by clicking the test title and entering the results and other pertinent information. All automated equipment tests (if applicable) can be answered by clicking the "Auto Test" button near the top of the screen.

View* All -All- Tester* Barlow, Eric Test Date(mm/dd/yyyy)* 04/12/2013

Test #	Title ^	Auto Test	Subject	View	N/E	N/A	D	F	P	Notes
519	AC-1.1 - Access Control Policy and Procedures		Main Location							The system clearly defines policy and procedures for Access Control. The policy is provided online via the portal. The procedures are provided in a handbook in pdf form (also on the portal) which may be distributed either electronically or physically.
467	AC-1.1 - Access Control Policy and Procedures		Main Location							

Tests can be conducted in two ways. The first is a manual entry of the data using IACS. Click on the title and fill out the pop-up screen.

Edit Test Result '519'

Save Reset Close

Procedure Name: AC-1.1(1)

View/Attachment:

Subject: Main Location

Tester* George Washington

Test Date(mm/dd/yyyy)* 04/12/1013

Result* Passed

Notes: The system clearly defines policy and procedures for Access Control. The policy is provided online via the portal. The procedures are provided in a handbook in pdf form (also on the portal) which may be distributed either electronically or physically.

Recommended Fix:

Procedure: Examine (Basic): Access control policy and procedures; other relevant documents or records.
 Interview (Basic): Organizational personnel with access control responsibilities.
 Expected Result: For specifications:
 - Determine if the specification exists.
 - Determine if the specification, as written, has no obvious inconsistencies with the functional requirements in the security control and no obvious internal errors.

The second method is to export the security assessment test plan in Excel format and answer the questions using Excel. Please note that if this method is used, the values for result must match the values that are in IACS. Refer to the table below for the values.

Element	Description
Tester	The name of the person conducting the security assessment for that particular control test case.
Test Date	The date of the test.
Result	The result of the test. The values are "Not Executed," "Deferred," "Failed," "Not Applicable," and "Passed."
Notes	A description of the result of the test.

Recommended Fix	Recommendations to fix the control if the test case fails.
-----------------	--

8.1.4 SECURITY ASSESSMENT PLAN

This step is where the companion to the RTM for the security assessment. The security assessment plan includes assumptions for the test, limitations to the test, assessment tools to be used, the composition of the assessment team, the testing schedule, hardware components, software, operating systems, network interfaces, and network interfaces to be tested, access methods, automated scans, and a signed letter authorizing the scans with approvals, caveats, and restrictions.

The security assessment plan is divided into sections. Each section is a separate text field. The capabilities of the text fields allow Microsoft Word compatible formatting. The remake button will return the section to the original text.

Security Assessment Plan

Completed:

Publishing Status: Never Published

Document Change History*

Version	Date	Author	Description

Assumptions* {Assumptions}

8.1.5 SECURITY ASSESSMENT PLAN EXTENSIBLE

This step is used to publish the security assessment plan for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. Please refer to the markings section for more information.

Security Assessment Plan Extensible

View Template Properties Document Settings Publish

Completed:

Publishing Status: Never Published

This process step uses extensible publishing.



8.2 SECURITY ASSESSMENT

Security Assessment is conducted by the Security Control Assessor (SCA); who refers to the Self-Assessment plan and procedures guidance; and results and performs more extensive testing with respect to roles and accesses, as well as the application or system itself.

In this task, the SCA:

- Reviews the test matrix and requirement information to ensure the right controls are present and understands what needs to be tested.
- Performs extensive tests and analysis and enters the results.
- Creates the Security Assessment Report (SAR), which documents the findings of the SCA, to identify each security weakness or deficiency found in the security controls and provides recommended corrective actions.
- Creates the Vulnerability Report, which details the results of the vulnerability scans that have been performed on the system, and makes up Appendix R of the main assessment documentation.

8.2.1 PROJECT TEST MATRIX

The project test matrix provides a detailed overview of the requirements and associated test procedures included in the test plan for the information system. This saves time and effort required to manually search through the test plan for this information. It provides a detailed summary of applicable test procedures and an explanation of those tests that are not applicable due to equipment type, equipment scope, etc.

Project Test Matrix



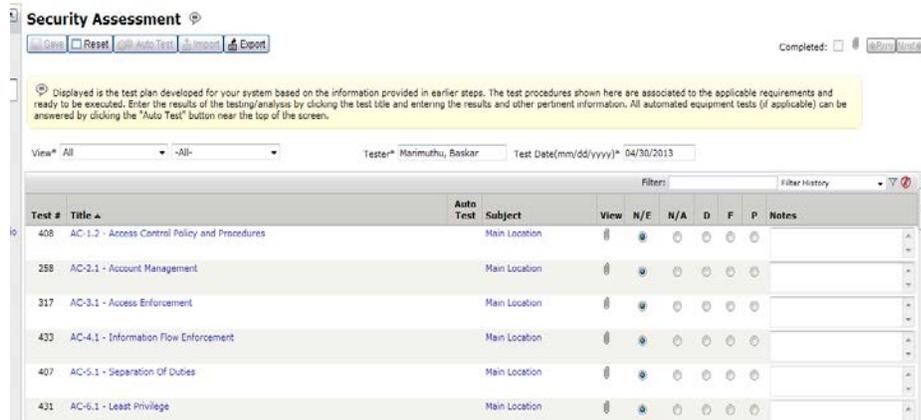
Completed:

This test matrix provides a detailed overview of the requirements and associated test procedures included in the test plan for your system. This saves you the time and effort required to manually search through the Test Plan for this information. Take some time to review the information displayed here, which provides a detailed summary of applicable test procedures and an explanation of those tests that are not applicable due to equipment type, equipment scope, etc.

REQUIREMENT		TEST GRPS	TEST PROC		SUBJECTS			TOTAL
Regulation	Paragraph/ReqID	Requirement	Assoc/Appl	Assoc/Appl	System	Location	TP/Equip	Tests
NIST 800-53 w/ DHS 4300A	AC-1	Access Control Policy and Procedures	2 / 2	6 / 3	3			3
NIST 800-53 w/ DHS 4300A	AC-2	Account Management	1 / 1	3 / 1	1			1
NIST 800-53 w/ DHS 4300A	AC-2[1]	Account Management	1 / 1	3 / 1	1			1

8.2.2 SECURITY ASSESSMENT

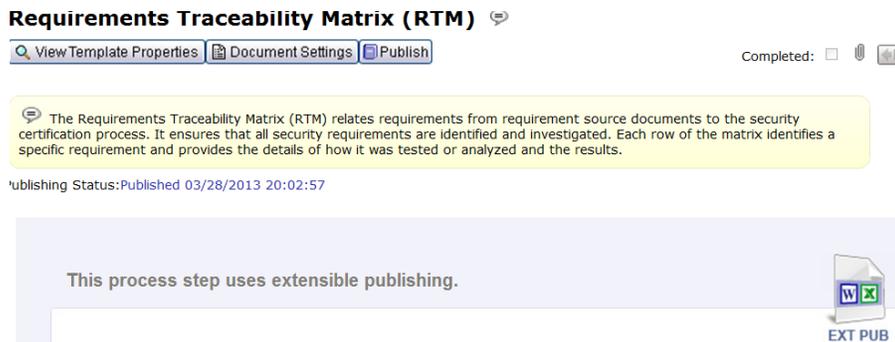
Displayed is the test plan development for your system based on the information provided in earlier steps. The test procedures shown here are associated to the applicable requirements and ready to be executed. Enter the test results of the testing/analysis by clicking the test title and entering the results and other pertinent information. All automated equipment test can be answered by clicking the “Auto Test” button near the top of the screen. To make this task easier, there is a function to export and import from Microsoft Excel.



8.2.3 REQUIREMENTS TRACEABILITY MATRIX (RTM)

The Requirements Traceability Matrix (RTM) relates requirements from requirement source documents to the security authorization process. It ensures that all security requirements are identified and investigated. Each row of the matrix identifies a specific requirement and provides the details of how it was tested or analyzed and the results.

This is a published document for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen.



8.2.4 SECURITY ASSESSMENT REPORT

The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the security assessment report. The security assessment report a key document in the security authorization package developed for authorizing officials. The report includes information from the assessor necessary to determine the effectiveness of the security controls employed within or inherited by the information system based upon the findings. The security assessment report is an important factor in an authorizing official’s determination of risk to organizational operations and assets, individuals, other organizations, and the Nation. Security control assessment results are documented at a level of detail appropriate for the assessment in accordance with the reporting format prescribed by policies.

The security assessment plan is divided into the following sections: Component’s address, scope, team composition, assumptions and constraints, security assessment results (high level summary), conclusion, level of acceptable risk, and SCA recommendation to AO. Each section is a separate text field. The capabilities of the text fields allow Microsoft Word compatible formatting. The remake button will return the section to the original text.

Security Assessment Report 

Completed: 

 The Security Assessment Report (SAR) contains all the results of the tests performed on the system under evaluation.

Publishing Status: Never Published

Document Change History*

Version	Date	Author	Description

8.2.5 SECURITY ASSESSMENT REPORT EXTENSIBLE

This step is used to publish the security assessment report for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. (This is usually For Official Use Only (FOUO)).

Security Assessment Report Extensible 

Completed: 

Publishing Status: Never Published

This process step uses extensible publishing.


EXT PUB

8.2.6 VULNERABILITY/PENETRATION TEST REPORT

This step contains the results of vulnerability scans and penetration tests that have been performed on the system. Section 2.0 details the results in a vulnerability table for each equipment record within each equipment group. It is important to list all the equipment in the categorize task as they will be used to help fill in this section. Use Section 3.0 to upload additional external vulnerability scan results. Each section is a separate text field. The capabilities of the text fields allow Microsoft Word compatible formatting. The remake button will return the section to the original text.

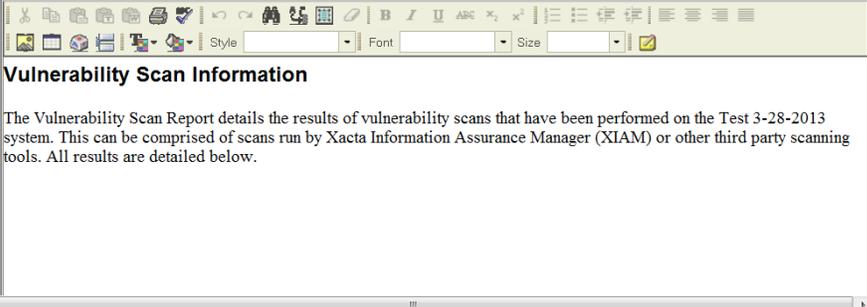
Vulnerability Report 

Completed: 

 This step contains the results of vulnerability scans that have been performed on the system. Section 2.0 details the results in a vulnerability table for each equipment record within each equipment group. Use Section 3.0 to upload additional external vulnerability scan results.

Publishing Status: Never Published

1.0*



8.3 RISK ANALYSIS

Risk Analysis is the last task in the Assess phase, where the controls put in place in the Implementation phase are assessed 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. At this point, the self-assessment and security assessment have been completed. The final certification analysis will be conducted and documentation will be updated in preparation for the next task -- Authorize.

In this task, the ISSO will:

- Analyze the system's risk elements.
- Review the RTM to assess controls based on test results.
- Create the Risk Assessment (RA) document, which consists of an analysis of the threats, vulnerabilities, countermeasures, and residual risks found to be applicable to the system.
- Review and/or update the Security Assessment Report (SAR) document, which is vital to the authorizing official's determination of risk.

In the Risk Analysis task the SCA has read/write access, and the Component CISO has approval authority.

To approve the task, the Component CISO should first ensure all data in the task is accurate and

complete. When the task is ready to be approved, click the approval icon, provide any necessary notes and click Save.

8.3.1 ANALYZE RISK ELEMENTS

The Analyze Risk Elements step presents a list of information system’s risk elements and provides the tools and information required to review and analyze them. A risk element is an item from a failed test or a user-defined item that could potentially impact the security of the system based upon threats and vulnerabilities to the information system.

Analyze Risk Elements 

    Completed:    

 The Analyze Risk Elements step presents you with a list of your system’s risk elements and provides you with the tools and information required to review and analyze them.

Show: Only Test Generated Risks 

Saved	Title	Location/Subject	Calc Risk	Adj Risk	Prop	Copy	Delete
No	Access Agreements [NIST 800-53 w/ DHS 4300A PS-6]	Main Location	High	High			
No	Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19[1]]	Main Location	High	High			
No	Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19[2]]	Main Location	High	High			
No	Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19[3]]	Main Location	High	High			
No	Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19]	Main Location	High	High			
No	Access Control for Output Devices [NIST 800-53 w/ DHS 4300A PE-5]	Main Location	High	High			

The Show drop-down is a filter where the ISSO may filter on the test generated risk elements, the user-defined risk elements, or both. Clicking on properties icon for the risk element will bring up a more detailed screen.

Edit Risk Element 'Access Agreements [NIST 800-53 w/ DHS 4300A PS-6]'

Name:

Location: Main Location

Calculated Risk Level: High

Associated Requirements* 

[NIST 800-53 w/ DHS 4300A PS-6] The organization:

(a) Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and,

(b) Requires foundation Ensures that the access agreements [Assignment: organization-defined] Associated Requirements



Statement of Issue* 

[Test: PS-6.1 - Access Agreements]

Not Entered



Recommended Fix* 

[Test: PS-6.1 - Access Agreements]

Not Entered



Impact Statement* 

Failure to meet access agreements requirements listed below could lead to disclosure

Element	Description
Name	The name of the control associated with the risk element. This is not editable.
Location	The physical location of the risk element. This is not editable.
Associated Requirements	Contains the description of the control requirement.
Statement of Issue	Contains the associated test and result of the test.
Recommended Fix	The recommendations for fixing the test if it is not compliant.
Impact Statement	The impact to the system security if the risk element is not mitigated.
Safeguard	Any compensating controls for reducing the impact of the risk element.
Risk Level	The impact of the risk element. This uses the FIPS 199 definitions of low, moderate, and high. This requires a note if it is changed from the baseline.
Risk Assessment	Any notes from the risk assessment.

8.3.2 REQUIREMENTS TRACEABILITY MATRIX (RTM)

The Requirements Traceability Matrix (RTM) relates requirements from requirement source documents to the security authorization process. It ensures that all security requirements are identified and investigated. Each row of the matrix identifies a specific requirement and provides the details of how it was tested or analyzed and the results.

This is a published document for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. Please refer to the markings section for more information.

Requirements Traceability Matrix (RTM)

[View Template Properties](#) [Document Settings](#) [Publish](#)

Completed:  

 The Requirements Traceability Matrix (RTM) relates requirements from requirement source documents to the security certification process. It ensures that all security requirements are identified and investigated. Each row of the matrix identifies a specific requirement and provides the details of how it was tested or analyzed and the results.

Publishing Status: Published 03/28/2013 20:02:57

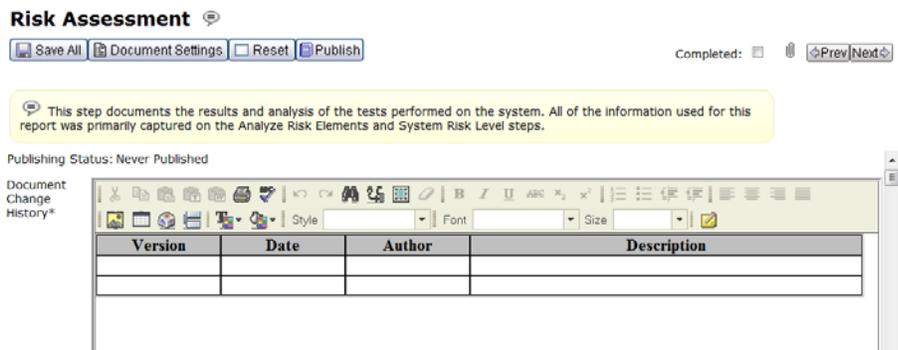
This process step uses extensible publishing.



8.3.3 RISK ASSESSMENT (RA)

This step documents the results and analysis of the tests performed on the system. All of the information used for this report is primarily captured on the Analyze Risk Elements and System

Risk Level steps. Each section is a separate text field. The capabilities of the text fields allow Microsoft Word compatible formatting. The remake button will return the section to the original text.



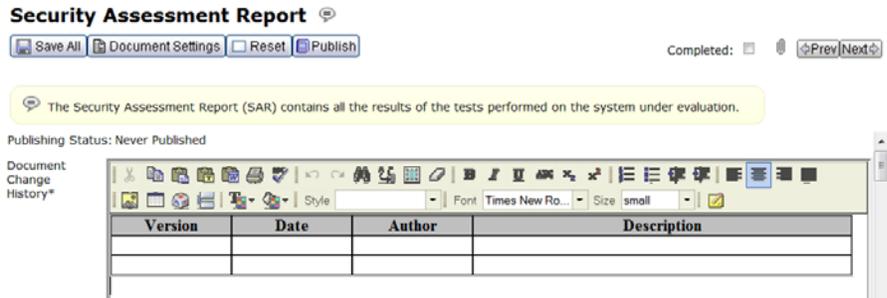
8.3.4 RISK ASSESSMENT EXTENSIBLE

This step is used to publish the risk assessment for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. Please refer to the markings section for more information.



8.3.5 SECURITY ASSESSMENT REPORT

The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the security assessment report. The security assessment report is one of the key documents in the security authorization package developed for authorizing officials. The security assessment report includes information from the assessor necessary to determine the effectiveness of the security controls employed within or inherited by the information system based upon the SCA findings. The security assessment report is an important factor in an authorizing official’s determination of risk to organizational operations and assets, individuals, other organizations, and the Nation. Security control assessment results are documented at a level of detail appropriate for the assessment in accordance with the reporting format prescribed by DHS, Component, and/or federal policies. Each section is a separate text field. The capabilities of the text fields allow Microsoft Word compatible formatting. The remake button will return the section to the original text.



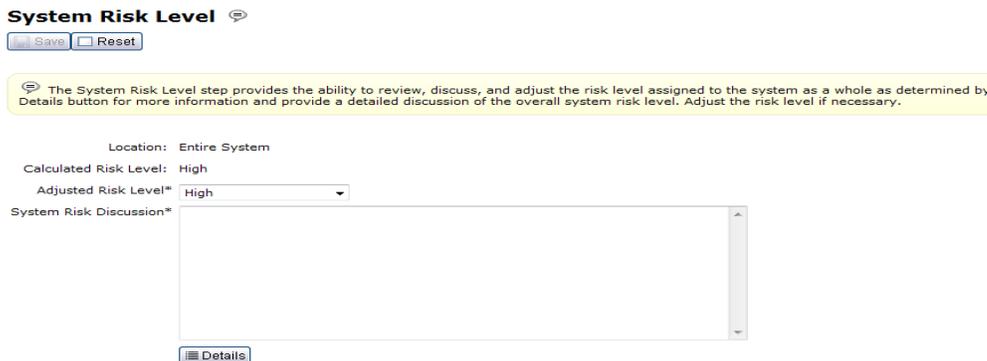
8.3.6 SECURITY ASSESSMENT REPORT EXTENSIBLE

This step is used to publish the SAR for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. Please refer to the markings section for more information.



8.3.7 SYSTEM RISK LEVEL

This step provides the ability to review, discuss and adjust the risk level assigned to the system as a whole as determined by the Analyze Risk Element step. Click on the Details button for more information and provide a detailed discussion of the overall system risk level. Adjust the risk level if necessary.



9.0 AUTHORIZE

The authorize phase of the risk management framework (RMF) is where the AO makes a decision whether or not to authorize the system for operation based on the security plan, security assessment report, and the plan of actions and milestones (POA&M). This provides the AO, at a minimum, the necessary information about risk impact.

The security assessment report contains the findings from the testing. It identifies which findings may be deemed as acceptable risk and which findings are not acceptable as it would adversely impact the system's security posture and inadequately protect the data should the system be compromised.

Unacceptable risks (also called residual risks) are findings that are detrimental for the operation of the system. These must have a plan for implementing solutions and mitigating the risks. This plan is called a POA&M.

9.1 POA&M

The plan of action and milestones, prepared for the authorizing official by the information system owner or the common control provider, is one of three key documents in the security authorization package and describes the specific tasks that are planned:

1. to correct any weaknesses or deficiencies in the security controls noted during the assessment; and
2. to address the residual vulnerabilities in the information system. The plan of action and milestones identifies:
 - a. the tasks to be accomplished with a recommendation for completion either before or after information system implementation;
 - b. the resources required to accomplish the tasks;
 - c. any milestones in meeting the tasks; and
 - d. the scheduled completion dates for the milestones.

The plan of action and milestones is used by the authorizing official to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment. All security weaknesses and deficiencies identified during the security control assessment are documented in the security assessment report to maintain an effective audit trail.

A final review of the Plan of Actions and Milestones (POA&M) will be performed prior to submission to the approving authority. The initial POA&M elements and POA&M report have been created in the previous Risk Analysis task. Now they will undergo a final review to ensure they are accurate and acceptable before the final package is submitted to the authorizing official.

In the task, the ISSO will:

- Review and/or update the individual POA&M elements to ensure everything has been included, analyzed, planned and prioritized.

- Perform the final review of the POA&M Report itself. *Note: If any changes were made to the POA&M Elements Review step, the POA&M Report Extensible should be re-published before reviewing, so the latest POA&M element information is included.*

9.1.1 POA&M ELEMENTS

A plan is needed to address each of the risk elements identified during the risk analysis of your system. This step allows the ISSO to import the risk elements and document the schedule of actions that will be taken to remove (or lower) the risk to your system, such as implement a security patch, complete vulnerability testing, etc. This information can be updated throughout the assessment process and will appear in the Plan of Action and Milestones documentation.

POA&M Elements

Completed:

A plan is needed to address each of the risk elements identified during the risk analysis of your system. This step allows you to import the risk elements and then document the schedule of actions that will be taken to remove (or lower) the risk to your system, such as implement a security patch, complete vulnerability testing, etc. This information can be updated throughout the assessment process and will appear in the Plan of Action and Milestones documentation.

Filter: Filter History

Rank	POA&M Nbr ▲	Title	Weakness	POC	CAT	Scheduled Completion Date	Status	Assoc. Risk Analyzed	View	Prop.	Copy	Delete	Select All

POA&Ms are created either from a risk element or manually with the New button.

Add Plan of Action Item

POA&M Nbr:

Title*

Creation Date (mm/dd/yyyy)*

Weakness:

Severity Code:

Point of Contact:

Resources Required:

Scheduled Completion Date (mm/dd/yyyy): Not Applicable:

Milestones:

Date	Description	Delete	Properties

Element	Description
Title	The title of the POA&M. This is usually the name of the NIST control or the

	OIG/GAO report.
Creation Date	The date the POA&M was created. This field is not editable.
Weakness	The weakness identified in the POA&M. This can include the weakness description, findings, remedial actions, and additional comments.
Severity Code	The severity of the POA&M if it is not implemented in a timely manner. IV is the lowest severity and I is the highest.
Point of Contact	The point of contact for the POA&M. This is the person who is most likely to be in the best position for directing and coordinating the activities. This is usually the ISSO.
Resources Required	The amount of resources (time and effort) required to implement the solution identified in the POA&M.
Scheduled Completion Date	The date the POA&M is scheduled for full implementation. This date should be realistic and achievable.
Milestones	A list of milestones. Milestones are critical points of achievement for the implementation of the POA&M.
Item Identified During	This defines where the POA&M was identified in. POA&Ms are found during security assessments, vulnerability scans, etc.
(other)	If the Item Identified During is defined as other (the only option available), the reason is specified here.
Report ID	The report id if the POA&M's source is an OIG or GAO report.
Overall Status	The overall status of the POA&M.
Comments	Comments for the POA&M.

9.1.2 POA&M REPORT EXTENSIBLE

This step is used to publish the POA&M for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. (This is usually For Official Use Only (FOUO)).

POA&M Report Extensible

 View Template Properties  Document Settings  Publish

Completed:     Prev

Publishing Status: Never Published

This process step uses extensible publishing.



9.2 COMPONENT DOCUMENT REVIEW

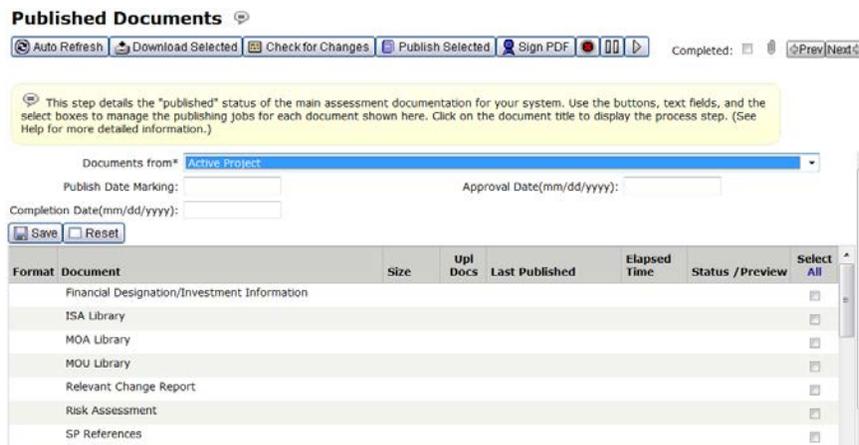
The goal of document review (DR) is to implement a rigorous set of quality standards across all DHS Security Authorization (SA) packages to ensure that applicable DHS and NIST controls have been properly documented. Where applicable, the DR team will enforce the creation of mitigation plans for control requirements that have not been met. DR ensures that Sensitive but

Unclassified (SBU) and National Security System (NSS) SA artifacts are in compliance with DHS policy and guidance. The objectives are to:

- Assess the completeness of the information provided in SA documentation against DHS quality standards;
- Improve the informational and educational feedback process to assist Components in developing a more consistent and repeatable SA process;
- Complete a review of a SA package for a particular information system or major application before it has been signed by the Authorizing Official (AO);
- Provide feedback to help refine the AO process, and to identify trends across Component packages to help determine the root causes of deficiencies.

9.2.1 PUBLISHED DOCUMENTS

This step details the publishing status of the main assessment documentation for your system. It allows you to publish, track, view, and download multiple documents. The list of documents to be published is shown here along with the document size, uploaded documents, last publish date, and the preview icon to view a previously published document. Use the buttons, text fields, and the select boxes to manage the publishing jobs for each document. This step is commonly used in more than one task. This allows you to create draft versions of your documents (or sections of your documents) as the project progresses, and to create final versions once the project is complete. The completed document status will be indicated on this step, as well as, the actual document page.



9.2.2 SECURITY AUTHORIZATION PACKAGE TRANSMITTAL LETTER

This step is for creating the security authorization package transmittal letter. It identifies the location of the testing, and the personnel who conducted the testing. It is the final step in creating a security authorization package for submittal to the AO. This section is a text field. The capabilities of the text fields allow Microsoft Word compatible formatting. The remake button will return the section to the original text.

Security Authorization Package Transmittal Letter

The screenshot shows a web-based publishing interface for a document titled "Security Authorization Package Transmittal Letter". At the top, there are buttons for "Save All", "Document Settings", "Reset", and "Publish". To the right, there is a "Completed:" status indicator and a "Prev/Next" navigation button. Below the buttons, the "Publishing Status" is shown as "Never Published". The main content area displays a rich text editor with the following text:

A security assessment of the Test 3-28-2013 and its constituent subsystem-level components *(if applicable)* located at [LOCATION] has been conducted in accordance with Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, and the Department of Homeland Security Headquarters (DHS HQ) policy on security authorization. The attached security authorization package contains: (i) current Security Plan, (ii) Security Assessment Report, and (iii) Plan of Action and Milestones.

The security controls listed in the Security Plan have been assessed by [SECURITY CONTROL ASSESSOR OR COMPANY] using the assessment methods and procedures described in the Security Assessment Report to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome of meeting the security requirements for the system. The Plan of Action and Milestones describes the corrective measures that have been implemented or are planned to address any deficiencies in the security controls for the information system and to reduce or eliminate known vulnerabilities.

9.2.3 SECURITY AUTHORIZATION PACKAGE TRANSMITTAL LETTER EXTENSIBLE

This step is used to publish the security authorization package transmittal letter for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. (This is usually For Official Use Only (FOUO)).

Security Authorization Package Transmittal Letter Extensible

The screenshot shows a web-based publishing interface for a document titled "Security Authorization Package Transmittal Letter Extensible". At the top, there are buttons for "View Template Properties", "Document Settings", and "Publish". To the right, there is a "Completed:" status indicator and a "Prev" navigation button. Below the buttons, the "Publishing Status" is shown as "Never Published". The main content area displays a light blue box with the text "This process step uses extensible publishing." and a small icon of a document with a "W" and "X" logo, labeled "EXT PUB".

9.3 ATO DECISION

In the **ATO Decision** task, the Authorizing Official (AO) will review the accreditation package and make the decision to grant or deny authorization to operate (ATO). In this task, they will:

- Use the Published Documents step to review the accreditation package.
- Use the ATO Letter step to review the ATO Letter.
- Update the Project Accreditation (with History) step, if included in the ATO Decision task.
- If ATO is granted, they will sign the ATO Letter and approve the task.

9.3.1 PUBLISHED DOCUMENTS

This step details the publishing status of the main assessment documentation for your system. It allows you to publish, track, view, and download multiple documents. The list of documents to be published is shown here along with the document size, uploaded documents, last publish date, and the preview icon to view a previously published document. Use the buttons, text fields, and the select boxes to manage the publishing jobs for each document. This step is commonly used in

more than one task. This allows you to create draft versions of your documents (or sections of your documents) as the project progresses, and to create final versions once the project is complete. The completed document status will be indicated on this step, as well as, the actual document page.

Published Documents

Auto Refresh Download Selected Check for Changes Publish Selected Sign PDF Completed: [Prev](#) [Next](#)

This step details the "published" status of the main assessment documentation for your system. Use the buttons, text fields, and the select boxes to manage the publishing jobs for each document shown here. Click on the document title to display the process step. (See Help for more detailed information.)

Documents from* **Active Project**

Publish Date Marking: Approval Date(mm/dd/yyyy):

Completion Date(mm/dd/yyyy):

Format	Document	Size	Upl Docs	Last Published	Elapsed Time	Status / Preview	Select All
	Financial Designation/Investment Information						<input type="checkbox"/>
	ISA Library						<input type="checkbox"/>
	MOA Library						<input type="checkbox"/>
	MOU Library						<input type="checkbox"/>
	Relevant Change Report						<input type="checkbox"/>
	Risk Assessment						<input type="checkbox"/>
	SP References						<input type="checkbox"/>

9.3.2 PROJECT ACCREDITATION

The Project Accreditation (with history) is used to indicate the authorization type granted to projects based on the results of the assessment effort, as well as to maintain a project's authorization history.

Project Accreditation (With History)

Completed: [Prev](#) [Next](#)

Assessment Event added

The Project Accreditation (with history) is used to indicate the accreditation type granted to non-commercial projects based on the results of the assessment effort, as well as to maintain a project's accreditation history.

Initial Expiration Warning(days):

Expiration Warning Interval(days):

Assessment Status	Approval Date	Approval Expiration Date	Properties	Delete	Select All
Authorization to Operate (ATO)	04/01/2012	04/01/2015		<input type="checkbox"/>	<input type="checkbox"/>

Click on new to add a new authorization.

Edit Assessment Event Annual Review Determination 2 (precautionary improvements)

Assessment Status:

Approval Date (mm/dd/yyyy)*:

Authorization Termination Date (mm/dd/yyyy):

Review Date (mm/dd/yyyy):

Comment:

Element	Description
Assessment Status	The authorization status of the information system.
Approval Date	The date the system is authorized to operate.
Authorization Termination Date	The date the system's authorization to operate expires.
Review Date	The date the system's authorization is reviewed.
Comments	Any comments from the AO regarding the authorization.

9.3.3 ATO LETTER

The ATO Letter provides authorization to operate information systems or to use security controls inherited by those systems. Use the white boxes below to complete the ATO Letter. Feel free to update or add additional content. Publish the Extensible ATO Letter instead of this step. This page feeds the Extensible ATO Letter process step. This section is a text field. The capabilities of the text fields allow Microsoft Word compatible formatting. The remake button will return the section to the original text.

ATO Letter

Completed:

The ATO Letter provides authorization to operate information systems or to use security controls inherited by those systems. Use the white boxes below to complete the ATO Letter. Feel free to update or add additional content. Publish the Extensible ATO Letter instead of this step. This page feeds the Extensible ATO Letter process step.

Publishing Status: Published 03/28/2013 20:06:17

Results of Security Assessment

I have reviewed the results of the security assessment of the Test 3-28-2013, its constituent system elements (if applicable) located at Not Specified and the supporting evidence provided in the associated security authorization package. The authorization package includes the current Security Plan (SP), the Security Assessment Report (SAR), and the Plan of Action and Milestones (POA&Ms). After evaluating the results of the security assessment, it is my opinion as the Authorizing Official (AO) that an acceptable level of risk to the Department of Homeland Security Headquarters (DHS HQ) exists and that the Test 3-28-2013 should be authorized to operate.

I authorize full deployment and production operations for the Test 3-28-2013, for processing Sensitive Information. An Authorization to Operate (ATO) is granted, valid from [ATO authorization date not specified] to [ATO authorization termination date not specified], or sooner if significant changes are made to the system engineering design and architecture. This security authorization is my formal declaration that adequate security controls have been implemented in the information system and that a satisfactory level of security is present in the system.

9.3.4 ATO LETTER EXTENSIBLE

This step is used to publish the security authorization package transmittal letter for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. (This is usually For Official Use Only (FOUO)).

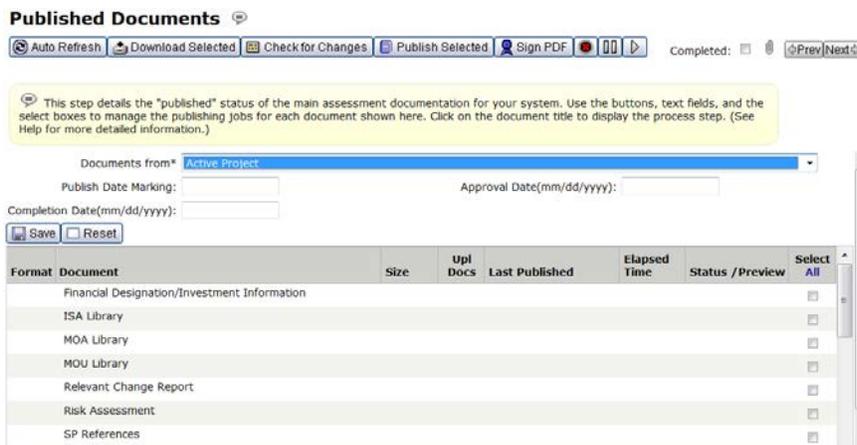


9.4 DHS DOCUMENT REVIEW

This step allows documents to be published and system authorization to be documented.

9.4.1 PUBLISHED DOCUMENTS

This step details the publishing status of the main assessment documentation for your system. It allows you to publish, track, view, and download multiple documents. The list of documents to be published is shown here along with the document size, uploaded documents, last publish date, and the preview icon to view a previously published document. Use the buttons, text fields, and the select boxes to manage the publishing jobs for each document. This step is commonly used in more than one task. This allows you to create draft versions of your documents (or sections of your documents) as the project progresses, and to create final versions once the project is complete. The completed document status will be indicated on this step, as well as, the actual document page.



10.0 MONITOR

10.1 SYSTEM DOCUMENTATION

Continuous monitoring provides the ability to address the security impacts on an information system resulting from changes to the hardware, software, firmware, or operational environment.

10.1.1 PROJECT DEFINITION

This task defines all the steps involved in the initial setup of the project in IACS.

Project Definition 

Completed: 

 The project definition step prompts you to enter fundamental high-level information about the system being assessed. The information entered here will automatically appear in Section 1 of the SSP documentation.

Project Name: DHS Test System 03212013

IT System Category*

System Type*

Acronym:

Version:

Definition:

This section contains the project name, IT system category, system type, acronym, version, and a high level description of the system or program. This section is maintained by the DHS Inventory team and any changes go through the [DHS Inventory Process].

Element	Description
Project Name*	This is the Federal Information Security Management Act (FISMA) name of the system or program.
System Type*	The type of the system. Currently IACS only contains general support systems (GSS) and major applications (MA) which are reportable to the Office of Management and Budget (OMB) through the FISMA process.
Acronym	The common used acronym of the system or program (e.g. IACS).
Version	This is an optional field for setting the version number of the system (e.g. IACS 2.0).
Definition	This field contains a high level description of the purpose, mission, and/or scope of the system or program.

10.1.2 PROJECT INFORMATION DETAIL

The Project Information Detail page allows the application to collect detailed project information that will be used in reporting.

Project Information Detail

Completed: 

 The Project Information Detail page allows the application to collect detailed project information that will be used in the IC IT Registry report. The information entered on this page will directly impact the IC IT Registry report.

SSP Name: Test 3-28-2013

IT Project Name:

Project ID:

Agency/Organization* Department of Homeland Security Headq

Reporting Authority* Department of Homeland Security Headq

Point of Contact:

IT System Type* Not Specified

System Location* Not Specified

System Operational:

Highest Information Category: No Marking

Lowest User Clearance: No Marking

Element	Description
SSP Name	The FISMA Name of the information system (e.g. IACS)
IT Project Name	Contains Investment Name
Project ID	Contains the UII Code & OMB Exhibit
Agency/Organization	The component responsible for the information system.
Reporting Authority	The component responsible for the information system.
Point of Contact	The person responsible for coordinating the security activities for the information system (usually the ISSO).
IT System Type	Determines whether the system is CFO designated, financial, mixed financial, or a non-financial system
System Location	[Unknown]
System Operational	Determines whether the system is operational (granted an authority to operate).
Highest Information Category	The highest category of information contained in the system.
Lowest User Clearance	The lowest classification required for users to the system.

10.1.3 PROJECT MILESTONES

The Project Milestones task is used to create a plan or project schedule for the security assessment of the system. It should identify all major milestones that should be reached with either approximate or exact dates. This task is updated throughout the process. To make this task easier, there is a function to export and import from Microsoft Excel.

The suggested method for this task is to click on the export button, fill out the excel spreadsheet, and import it into IACS.

Project Milestones

 New  Copy/Replace  Delete Selected  Import  Export Reset

Completed:  Prev/Next

 Project Milestones are used to outline a plan or project schedule for assessing a system. Identify all major milestones that should be reached for your assessment and an approximation or exact date that the milestone will be reached. The information entered here can be updated throughout the assessment process.

Title	Start Date	Completion Date	Properties	Copy	Delete	Select
Kick-off	03/01/2013	03/01/2013				
Risk Categorization	03/02/2013	03/10/2013				
Control Selection	03/10/2013	03/10/2013				
Implement Controls	03/11/2013	03/30/2013				

10.1.4 SYSTEM BOUNDARY

This task defines all computers and related equipment within a location(s), defined under the System Environment step, along with the internal and external connections (e.g., a router and all systems connected to its local-area ports). Graphical representations of the system boundary may also be uploaded here.

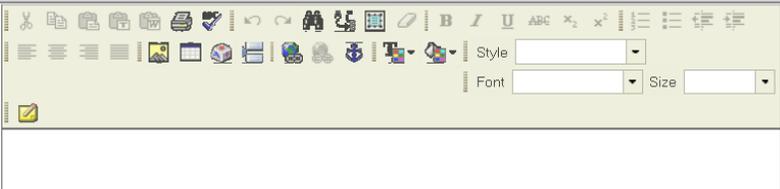
System Boundary

 Save Reset

Completed:

 Define all computers and related equipment within the location(s), defined under the System Environment step, along with internal and external connections (e.g., a router and all systems connected to its local-area ports).

System Boundary:



10.1.5 SYSTEM ENVIRONMENT

The System Environment task defines the environments or locations in which the system operates and to adjust the threat levels associated with each location/environment. A default location is provided as the "main location" of the system being assessed. This information is published in the Risk Assessment documentation.

To modify the default, click on the "Properties" icon.

Name ▲	Description	Category	SCIF Certified	TEMPEST Certified	Weight	View	Test	Default	Properties	Copy	Delete
Main Location	Main Location		No	No	Medium		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			

To create a new environment, click on the "New" icon.

Edit System Location 'Main Location'

General

Threats

Geography

Name* Main Location

Description: Main Location

Weight* Medium

Include Location in Test Plan:

General

Threats

Geography

Name	Group ▲	Weight
Humidity	Environment Failure	Medium
Power	Environment Failure	Medium
Sand/Dust	Environment Failure	Medium
Temperature	Environment Failure	Medium
Vibration/Shock	Environment Failure	Medium

General

Threats

Geography

Site:

Building:

Room:

City:

State:

Country:

Category: - Select One -

SCIF Certified:

TEMPEST Certified:

Tab	Element	Description
General	Name	The name of the location or environment.
	Description	A detailed description of the environment.
	Weight	The risk impact of the environment.
	Include Location in	Determines whether or not to include this site in the

	Test Plan	security assessment (test) plan.
Threats	Multiple	Weight of threats by the impact level and likelihood of threats occurring.
Geography	Site	The name of the site where the information system is housed.
	Building	The name of the building where the information system is housed.
	Room	The room name and/or number of where the information system is housed. The purpose is to easily identify the location of the system.
	City	The city where the information system is located.
	State	The state where the information system is located.
	Country	The country where the information system is located.
	Category	This is a drop-down to select the category of the site or location.
	SCIF Certified	This determines if the location is a certified SCIF.
	TEMPEST Certified	This determines if the location is TEMPEST certified.

10.1.6 SYSTEM INTERFACES/INTERCONNECTIONS

This task defines the physical and logical external connections, or system interfaces, used by your system. Explain how the system interacts with other systems or networks. The System Interfaces entered will appear in the SP documentation.

Add System Interface

Specify Interface* System Interface

Name*

Description:

Port:

Protocol:

Organization:

Interface Type: - Select One -

Connection Agreement Type: Not Specified

Connection Agreement Date (mm/dd/yyyy):

FIPS 199 Category: - Select One -

System C&A Status: - Select One -

Element	Description
Specify Interface	This is a drop-down menu to identify whether the interface is Cross Domain Solution or not.
Name	The name of the interface
Description	A detailed description of the interface.
Port	The port or port range of the interface.
Protocol	The protocol(s) used for the interface.
Organization	The organization of the interface. This is not the organization of the system but the interface the system connects with.
Interface Type	The type of the interface.
Connection Agreement Type	The type of agreement used between both parties (e.g. MOU).
Connection Agreement Date	The date the agreement was signed and went into effect.
FIPS 199 Category	The security impact level of the interface based on FIPS 199.
System C&A Status	The security authorization status of the other system in the agreement.

10.1.7 SYSTEM DATA FLOW

This task defines the routes by which the data flows through the system (e.g., flow of information between database servers and application servers; local network connections for backup or system mirroring; flow of routine e-mail traffic, etc.). Select New to name and define the different types of data flows used by your system.

Element	Description
Name*	The name of the service or daemon.
Port	The port the service communicates with
Protocol	The protocol the service uses (e.g. TCP/UDP).
Description	The description of the service. This should be as descriptive as possible.

Add System Data Flow

Name*

Port:

Protocol:

Description:

10.1.8 MANAGE SOFTWARE

The Manage Software step is initially blank. When equipment is imported into the project, all the installed software (detected from the scan) will be displayed here along with the associated equipment count. A manual entry of software is also available in this step. Review the list of software applications and make any necessary modifications. Since software applications are directly linked to equipment inventory and test procedures, this ensures the appropriate test procedures are pulled on the Test Plan & Results step, under the Vulnerability Assessment and Testing task. This step is one instance of the same page – changes will appear in each instance under different tasks.

Manage Software

Completed:  

 The Manage Software step is initially blank. As equipment is imported into the project, all installed software, detected from the scan, will be displayed here along with the associated equipment count. Review the list of software applications and make any necessary modifications. Since software applications are directly linked to equipment inventory and test procedures, this ensures that the appropriate test procedures are pulled on the Test Plan & Results step, under the Vulnerability Assessment and Testing task. (See Help for more detailed information.) The Manage Software process step is one instance of the same page – changes will appear in each instance under different tasks.

-All-

		Filter:		Filter History					
Application ▲	Type	Category	Alias Count	Equip. Count	Approved	Publish All	Properties	Copy	De

To manually add software, click on new.

Add Software Application

General
Aliases

Name*
 Vendor:
 Version:
 Type* Unknown
 DADMS #:
 FAM Status:
 CC Eval Status:
 Description:
 IA Enabled?:
 Admin Tool?:
 Category:

Element	Description
Name	The name of the software
Vendor	The name of the software vendor
Version	The version number of the software.
Type	The type of software.
DADMS #	[UNKNOWN]
CC Eval Status	[UNKNOWN]
Description	A brief description of the software.
IA Enabled?	Determines if the software is IA enabled.
Admin Tool?	Determines if the software is used as an admin tool.
Category	The category of the software.

Once saved, clicking on the alias tab will let the ISSO enter alias information about the software.

10.1.9 CONTROLS IMPLEMENTATION

This step is used to define the implementation details for the NIST 800-53 and DHS 4300A controls. Only the *applicable* controls are displayed. As changes and updates are made here, the information will automatically be populated in the appropriate SP sections.

NIST 800-53 w/ DHS 4300A											
Applicability Filter: Applicable Only										Filter: <input type="text"/>	
Paragraph/ReqID ▲	Title	Class	Type	Inheritance	Status	Priority	Responsible Entities	Implementation	Estimated Completion	View	Propertie
AC-1	Access Control Policy and Procedures	Technical			Implemented	P1	DHS CISO	This control may...			
AC-2	Account Management	Technical				P1					

Make updates by selecting the Properties icon for each requirement.

Edit Requirement 'AC-2 Account Management'

Type:

Status:

Priority:

Responsible Entities:

Implementation:

Estimated Completion Date (mm/dd/yyyy):

Notes:

Element	Description
Type	The type of the control (system specific, hybrid, common, system specific.).
Status	The implementation status of the control.
Priority	The priority or sequencing of the control. Higher priority controls are to be implemented first.
Responsible Entities	The entities and personnel responsible for the implementation of the control. It can also contain the description of the control implementation of the system it is inheriting from.
Implementation	The detailed description of the implementation of the control.
Estimation Completion Date	The estimated date when the control will be implemented.
Notes	Any extra notes or comments about the control implementation.

10.1.10EQUIPMENT GROUPS

Equipment groups should be defined for each location within the project. It is important to define the equipment groups, before importing the equipment, to both provide a process for grouping the equipment inventory during the import and for easily categorizing the components of the information system. The ISSO can use the default set of groups provided here or simply add/modify the equipment groups to best fit the individual system environment.

Equipment Groups

[New](#) [Copy/Replace](#) [Delete Selected](#)

Completed:  [Pre](#)

 A default set of the basic equipment groups is defined here. Equipment groups should be defined for each location within the project. It is important to define the equipment groups, before importing the equipment, to provide a process for grouping the equipment inventory during the import. You can use the default set of groups provided here or simply add/modify the equipment groups to best fit your system environment.

Group Name ▲	Location	Description	Equipment To Test	Properties	Copy	Delete
Mainframes	Main Location		0/0			
Networking Equipment	Main Location		0/0			
Unix Servers	Main Location		0/0			
Unix Workstations	Main Location		0/0			
Windows Laptops	Main Location		0/0			
Windows Servers	Main Location		0/0			

To add a new equipment group, click on new. To modify an existing equipment group, click on properties.

Add Equipment Group

[Save](#) [Reset](#) [Close](#)

Group Name* OS X Servers
 Description: OS X Servers.
 Manufacturer: Apple
 Model:
 OS: 10.8.3
 Location* Offsite
 Host Name Display Pattern* {\$name}
 Weight* Medium

Equipment To Test

Name ▲	Sele:
	All

Name	Description
Group Name	The name of the group. This should be as general as possible.
Description	A description of the equipment group.
Manufacturer	The manufacturer of the equipment group.
Model	The model (usually model number) of the group.
OS	The operating of the equipment group if applicable.
Location	The physical location of the equipment group. The locations are created in the categorize phase.
Weight	The risk weight of the equipment group.

10.1.11EQUIPMENT INVENTORY

Define specific details of all computers, servers, printers that exist within the boundary of the information system. This step allows either manual entry of equipment or import an inventory list directly into the project, such as a Nessus scan file. Each individual piece of equipment can be characterized in detail, including hardware description, network address, operating system, information on installed software applications, and indication if the equipment will be tested.

This information is used to build the appropriate equipment tests defined in the test plan for the system.

Equipment Inventory

Completed:

Define specific details of all computers, servers, printers that exist within the boundary of your system. This step allows you to manually enter equipment or import an inventory list directly into the project, such as the Xacta Detect scan file. Each individual piece of equipment can be characterized in detail, including hardware description, network address, operating system, information on installed software applications, and indication if the equipment will be tested. This information is used to build the appropriate equipment tests defined in the test plan for the system.

Host Name (IP)	Group Name	Last Updated	Test	Properties	Vulnerable	Copy	Delete
1-DHS-Server	Windows Servers	04/11/2013 10:30:54	✓				

To add equipment inventory, click on new.

Edit Equipment '1-DHS-Server'

General	Detail	Installed Software	Vulnerabilities	Point of Contact 1	Point of Contact 2
<p>Group*: Windows Servers</p> <p>Host Name*: 1-DHS-Server</p> <p>Manufacturer: HP</p> <p>Model: HP1XA001</p> <p>IP Address: 1.2.3.4</p> <p>MAC Address: a1b2c3</p> <p>Serial No: 0000000-1</p> <p>Visual ID: 100000001</p> <p>Agent Id:</p> <p>Test This Equipment: <input checked="" type="checkbox"/></p> <p>Description: The main server.</p> <p>IA Enabled: <input checked="" type="checkbox"/></p> <p>CC Eval Status: N/A</p> <p>Function: The main server</p>					
<p>Equipment Class*</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Any <input type="checkbox"/> Computer <input type="checkbox"/> Other <input type="checkbox"/> Printer <input checked="" type="checkbox"/> Servers 					

Tab	Element	Description
General	Group	The equipment group of the item.
	Host Name	The host name of the equipment.
	Manufacturer	The name of the company that manufactured the equipment.
	Model	The model (typically model number) of the equipment.
	IP Address	The IP address of the equipment.
	MAC Address	The MAC address of the equipment.
	Serial No.	The serial number of the equipment.
	Visual ID	An ID that can be used for equipment tracking (e.g. an asset ID tag).
	Agent Id	Asset Id
	Test This Equipment	Determines whether a test plan should be created in IACS for the equipment.

	Description	A description of the equipment and mission.
	IA enabled	[UNKNOWN]
	CC Eval Status	[UNKNOWN]
	Function	A description of the equipment's function.
	Peripherals	A list of the peripheral equipment attached.
Detail	Select Property	A dropdown of the properties associated with the equipment.
Installed Software	Operating system	The operating system of the equipment. This is a drop-down list. The application list is populated from the managed software step.
Vulnerabilities	N/A	This page is populated from a scan.
Point of Contact 1	Title	The title of the contact.
	Name	The name of the contact
	Organization	The organization of the contact (e.g. Data Center)
	Location	The physical location of the contact.
	Phone	The phone number of the contact.
	Email	The email of the contact.
Point of Contact 2	Title	The title of the contact.
	Name	The name of the contact
	Organization	The organization of the contact (e.g. Data Center)
	Location	The physical location of the contact.
	Phone	The phone number of the contact.
	Email	The email of the contact.

10.1.12 SYSTEM USERS

This task is for identifying and adding users with responsibilities of the system or program in regards to operation, administration, maintenance and security. These are not individual users but rather categories of users (i.e. system administrators, patch managers, etc.). This allows minimum qualifications to users in any of these categories to be documented. To create a new system user, click on "New"

Add System User

Category*

Min. Clearance / Investigation*

Foreign Nationals*

Position Designation*

Description*

Element	Description
Category	This is the category or type of user. For example a system administrator.
Min. Clearance/Investigation	This is the minimum clearance or investigation level required for the user.
Foreign Nationals	This setting determines whether foreign nationals are allowed.
Position Designation	This setting determines whether the position is critical/non-critical and sensitive/non-sensitive.
Description	A brief description of the position.

10.1.13 PROJECT PERSONNEL

This task is for defining and documenting all the personnel who have responsibilities to assess the system or program. To enter personnel, please press the “New” button. Import from LDAP is not available at this time.

Project Personnel

Completed: 

 This step is used to list all personnel who participate in the assessment of the system, based on their assigned role. To create a new personnel record, click the "New" button under the page title.

Auto-copy from assigned project users:

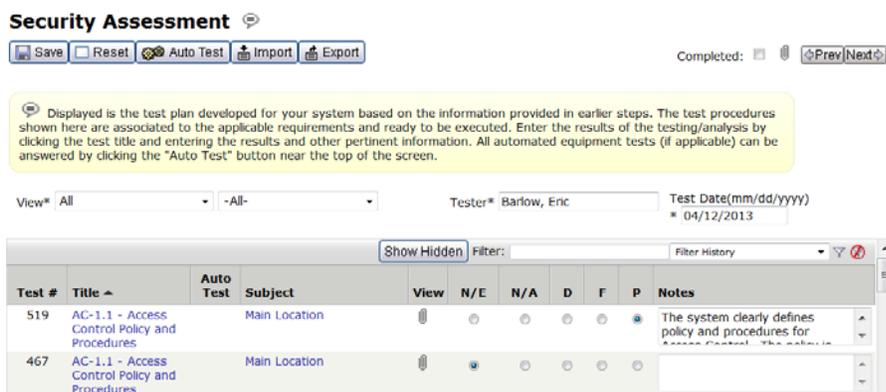
Name ▲	Role	Organization	Office	Properties	Copy	Delete
--------	------	--------------	--------	------------	------	--------

Element	Definition
Role Name*	This field is a drop-down list of the roles available in IACS.
Title	The field is for the title of the person. This may be the official title of the person or a title

	related to the activities of the system.
First Name*	The first name of the person.
Middle Initial	The middle initial of the person.
Last Name*	The last name of the person.
Personnel Type	This field is a drop-down list to determine if the person is a contractor, military, or federal civil employee.
Office	The office of the person.
Office Designation	The office designation of the person.
Organization	The organization of the person.
Street Address	The address of the person's workplace.
Address Continued	
City	
State/Province	
ZIP/Postal Code	
Citizenship*	The person's citizenship status.
Phone	The phone of the person.
Secure Phone	The secure phone (if applicable) of the person.
Fax	The fax of the person.
Email*	The email of the person.

10.1.14 SECURITY ASSESSMENT

This step displays the test plan developed for the information system based on the information provided in earlier steps. The test procedures shown are associated to the applicable requirements and ready to be executed. The ISSO enters the results of the testing/analysis by clicking the test title and entering the results and other pertinent information. All automated equipment tests (if applicable) can be answered by clicking the "Auto Test" button near the top of the screen.



Tests can be conducted in two ways. The first is a manual entry of the data using IACS. Click on the title and fill out the pop-up screen.

Edit Test Result '519'

Procedure Name: AC-1.1(1)

View/Attachment: 

Subject: [Main Location](#)

Tester*

Test Date(mm/dd/yyyy)*

Result*

Notes:

Recommended Fix:

Procedure: Examine (Basic): Access control policy and procedures; other relevant documents or records.

Interview (Basic): Organizational personnel with access control responsibilities.

Expected Result: For specifications:

- Determine if the specification exists.
- Determine if the specification, as written, has no obvious inconsistencies with the functional requirements in the security control and no obvious internal errors.

The second method is to export the security assessment test plan in Excel format and answer the questions using Excel. Please note that if this method is used, the values for result must match the values that are in IACS. Refer to the table below for the values.

Element	Description
Tester	The name of the person conducting the security assessment for that particular control test case.
Test Date	The date of the test.
Result	The result of the test. The values are "Not Executed," "Deferred," "Failed," "Not Applicable," and "Passed."
Notes	A description of the result of the test.
Recommended Fix	Recommendations to fix the control if the test case fails.

10.1.15ANALYZE RISK ELEMENTS

The Analyze Risk Elements step presents a list of information system's risk elements and provides the tools and information required to review and analyze them. A risk element is an item from a failed test or a user-defined item that could potentially impact the security of the system based upon threats and vulnerabilities to the information system.

Analyze Risk Elements

Completed:    

 The Analyze Risk Elements step presents you with a list of your system's risk elements and provides you with the tools and information required to review and analyze them.

Show: Only Test Generated Risks 

Filter: Filter History 

Saved	Title	Location/Subject	Calc Risk	Adj Risk	Prop	Copy	Delete
No	Access Agreements [NIST 800-53 w/ DHS 4300A PS-6]	Main Location	High	High			
No	Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19[1]]	Main Location	High	High			
No	Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19[2]]	Main Location	High	High			
No	Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19[3]]	Main Location	High	High			
No	Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19]	Main Location	High	High			
No	Access Control for Output Devices [NIST 800-53 w/ DHS 4300A PE-5]	Main Location	High	High			

The Show drop-down is a filter where the ISSO may filter on the test generated risk elements, the user-defined risk elements, or both. Clicking on properties icon for the risk element will bring up a more detailed screen.

Edit Risk Element 'Access Agreements [NIST 800-53 w/ DHS 4300A PS-6]'

Name:

Location:

Calculated Risk Level: High

Associated Requirements*



Statement of Issue*

Not Entered



Recommended Fix*

Not Entered



Impact Statement*

Element	Description
Name	The name of the control associated with the risk element. This is not editable.
Location	The physical location of the risk element. This is not editable.
Associated Requirements	Contains the description of the control requirement.
Statement of Issue	Contains the associated test and result of the test.
Recommended Fix	The recommendations for fixing the test if it is not compliant.

Impact Statement	The impact to the system security if the risk element is not mitigated.
Safeguard	Any compensating controls for reducing the impact of the risk element.
Risk Level	The impact of the risk element. This uses the FIPS 199 definitions of low, moderate, and high. This requires a note if it is changed from the baseline.
Risk Assessment	Any notes from the risk assessment.

10.1.16 POA&M ELEMENTS

A plan is needed to address each of the risk elements identified during the risk analysis of your system. This step allows the ISSO to import the risk elements and document the schedule of actions that will be taken to remove (or lower) the risk to your system, such as implement a security patch, complete vulnerability testing, etc. This information can be updated throughout the assessment process and will appear in the Plan of Action and Milestones documentation.

POA&M Elements 

Completed: 

 A plan is needed to address each of the risk elements identified during the risk analysis of your system. This step allows you to import the risk elements and then document the schedule of actions that will be taken to remove (or lower) the risk to your system, such as implement a security patch, complete vulnerability testing, etc. This information can be updated throughout the assessment process and will appear in the Plan of Action and Milestones documentation.

Filter: <input type="text"/>													
Filter History ▼ 													
Rank	POA&M Nbr ▲	Title	Weakness	POC	CAT	Scheduled Completion Date	Status	Assoc. Risk Analyzed	View	Prop.	Copy	Delete	Select All

POA&Ms are created either from a risk element or manually with the New button.

Add Plan of Action Item

POA&M Nbr:

Title*

Creation Date
(mm/dd/yyyy)*

04/15/2013

Weakness:

Severity Code:

- Not Assigned -

Point of
Contact:

Resources
Required:

Scheduled
Completion
Date

Not Applicable:

(mm/dd/yyyy):

Milestones:

Milestones			
Date	Description	Delete	Properties
<input type="button" value="New"/>			

Element	Description
Title	The title of the POA&M. This is usually the name of the NIST control or the OIG/GAO report.
Creation Date	The date the POA&M was created. This field is not editable.
Severity Code	The severity of the POA&M if it is not implemented in a timely manner. IV is the lowest severity and I is the highest.
Point of Contact	The point of contact for the POA&M. This is the person who is most likely to be in the best position for directing and coordinating the activities. This is usually the ISSO.
Resources Required	The amount of resources (time and effort) required to implement the solution identified in the POA&M.
Scheduled Completion Date	The date the POA&M is scheduled for full implementation. This date should be realistic and achievable.
Milestones	A list of milestones. Milestones are critical points of achievement for the implementation of the POA&M.
Item Identified During (other)	This defines where the POA&M was identified in. POA&Ms are found during security assessments, vulnerability scans, etc. If the Item Identified During is defined as other (the only option available), the reason is specified here.
Report ID	The report id if the POA&M's source is an OIG or GAO report.
Overall Status	The overall status of the POA&M.
Comments	Comments for the POA&M.

10.1.17 REQUIREMENTS TRACEABILITY MATRIX (RTM)

The Requirements Traceability Matrix (RTM) relates requirements from requirement source documents to the security authorization process. It ensures that all security requirements are identified and investigated. Each row of the matrix identifies a specific requirement and provides the details of how it was tested or analyzed and the results.

This is a published document for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen.

Requirements Traceability Matrix (RTM)

 View Template Properties  Document Settings  Publish

Completed:  

 The Requirements Traceability Matrix (RTM) relates requirements from requirement source documents to the security certification process. It ensures that all security requirements are identified and investigated. Each row of the matrix identifies a specific requirement and provides the details of how it was tested or analyzed and the results.

ublishing Status: **Published** 03/28/2013 20:02:57

This process step uses extensible publishing.



10.1.18 SECURITY ASSESSMENT REPORT

The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the security assessment report. The security assessment report a key document in the security authorization package developed for authorizing officials. The report includes information from the assessor necessary to determine the effectiveness of the security controls employed within or inherited by the information system based upon the findings. The security assessment report is an important factor in an authorizing official's determination of risk to organizational operations and assets, individuals, other organizations, and the Nation. Security control assessment results are documented at a level of detail appropriate for the assessment in accordance with the reporting format prescribed by policies.

The security assessment plan is divided into the following sections: Component's address, scope, team composition, assumptions and constraints, security assessment results (high level summary), conclusion, level of acceptable risk, and SCA recommendation to AO. Each section is a separate text field. The capabilities of the text fields allow Microsoft Word compatible formatting. The remake button will return the section to the original text.

Security Assessment Report

Completed: 

 The Security Assessment Report (SAR) contains all the results of the tests performed on the system under evaluation.

Publishing Status: Never Published

Document
Change
History*



Version	Date	Author	Description

10.1.19 SECURITY PLAN

This step is for entering the sections of the SP not associated with the controls. Each section is a separate text field. The capabilities of the text fields allow Microsoft Word compatible formatting.

Security Plan

Completed: 

Publishing Status: Never Published

Document
Change
History*



Version	Date	Author	Description

Component's
Address*

[DO NOT TYPE in the gray column. Provide response in the second column.]

Component's Address

10.1.20 SECURITY PLAN EXTENSIBLE

This step is used to publish the SP for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. (This is usually For Official Use Only (FOU)).

Security Plan Extensible

 View Template Properties  Document Settings  Publish

Completed:   

Publishing Status: Never Published

This process step uses extensible publishing.



10.1.21 CONTINGENCY PLAN

This task is used to develop and publish the Contingency Plan (CP). The CP task stays open until the Authorize task is completed and ready for approval in order to ensure the system is updated and current just prior to receiving an ATO decision, allowing users to provide information security updates during the accreditation package development. Once the Authorize task is completed the Information Security Monitoring task will need to be approved first in order for the AO to make a decision. In the CP task, there is only one process step to complete before notifications are sent out. The ISSM and/or the ISSO are responsible for the task as each of their roles have read and write access to it.

Recall, The CP task stays open until the Authorize task is ready for approval in order to ensure the system is updated and current just prior to receiving an ATO decision. Once the Authorize task is completed the CP task will need to be approved first in order for the AO to make a decision.

The CP task is approved by either the ISSM or the ISSO and the Gov. only ISSM. This means two approvals are needed for this task. The ISSM, ISSO, and Gov. only ISSM will receive notifications in their inboxes when the task is approved or ready for approval as well as when the task is activated or not approved.

To approve the Information Security Monitoring task, the ISSM, ISSO, and Gov. only ISSM should first ensure the Information Security Monitoring is up to date, accurate, and complete. The CP process step should be marked as completed. When the task is ready to be approved, click the approval icon, provide any necessary notes and click Save.

At this point, notifications will be sent out and the AO can proceed with approving the Authorize task.

The CP task is divided into several steps which correspond to sections in the CP. Each section is a separate text field. The capabilities of the text fields allow Microsoft Word compatible formatting. The remake button will return the section to the original text.

10.1.21.1 CONTINGENCY PLAN (SECTIONS 1-2)

10.1.21.2 CONTINGENCY PLAN (SECTION 3-5)

Contingency Plan (Sections 3-5)

Completed:

The Contingency Plan establishes procedures to recover the system following a disruption.

Publishing Status: Never Published

Damage Assessment Procedures*

Damage Assessment Procedures:
(Detailed procedures should be outlined to include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical status of physical infrastructure; status of information system equipment functionality and inventory, including items that will need to be replaced; and estimated time services to normal operations).

- Upon notification from the [SYSTEM OWNER/CONTINGENCY PLAN COORDINATOR], the DAT is to ...
- The [DAT] is to ...

Alternate

10.1.21.3 CONTINGENCY PLAN (SECTION 6-7)

10.1.22 CONTINGENCY PLAN TEST

This step is for the ISSO to enter in the CPT results. The CPT step is divided into several sections which correspond to sections in the CPT. Each section is a separate text field. The capabilities of the text fields allow Microsoft Word compatible formatting. The remake button will return the section to the original text.

Contingency Plan Test

Completed:

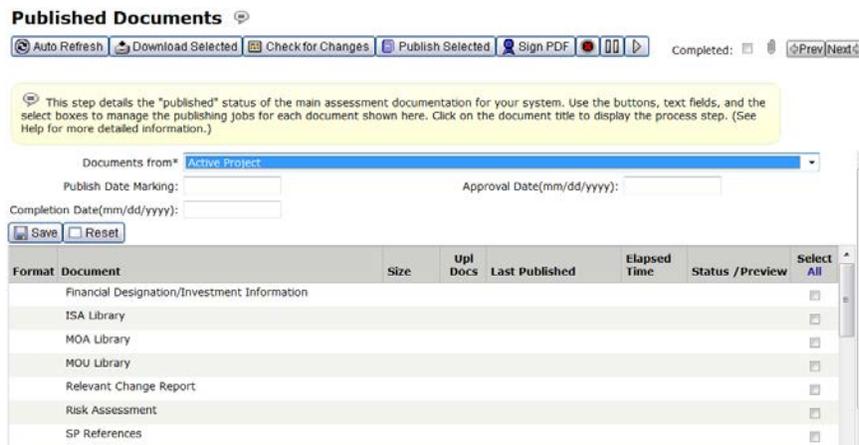
Publishing Status: Never Published

Document Change History*

Version	Date	Author	Description

10.1.23 PUBLISHED DOCUMENTS

This step details the publishing status of the main assessment documentation for your system. It allows you to publish, track, view, and download multiple documents. The list of documents to be published is shown here along with the document size, uploaded documents, last publish date, and the preview icon to view a previously published document. Use the buttons, text fields, and the select boxes to manage the publishing jobs for each document. This step is commonly used in more than one task. This allows you to create draft versions of your documents (or sections of your documents) as the project progresses, and to create final versions once the project is complete. The completed document status will be indicated on this step, as well as, the actual document page.



10.2 MONITOR POA&M

Monitor POA&M is the second task in the Monitor Phase, which is used to constantly monitor the information system on an ongoing basis through the use of various assessment, documentation and reporting methodologies for any change in the authorized risk level of the system. In the Monitor step, all the tasks are available at the same time because the processes in the step occur simultaneously. The Monitor POA&M task is primarily the responsibility of the ISSO and ISSM.

In this task, they will:

- Update process steps to reflect system changes
- Review published documents and supplemental documentation for reference, and republish documents to reflect changes

In the Monitor POA&M task, the ISSO and ISSM, unlike other tasks in the project, does not require approval.

10.2.1 ANALYZE RISK ELEMENTS

The Analyze Risk Elements step presents a list of information system's risk elements and provides the tools and information required to review and analyze them. A risk element is an item from a failed test or a user-defined item that could potentially impact the security of the system based upon threats and vulnerabilities to the information system.

Analyze Risk Elements

Completed:

The Analyze Risk Elements step presents you with a list of your system's risk elements and provides you with the tools and information required to review and analyze them.

Show: Only Test Generated Risks

Filter:

Saved	Title	Location/Subject	Calc Risk	Adj Risk	Prop	Copy	Delete
No	Access Agreements [NIST 800-53 w/ DHS 4300A PS-6]	Main Location	High	High			
No	Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19[1]]	Main Location	High	High			
No	Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19[2]]	Main Location	High	High			
No	Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19[3]]	Main Location	High	High			
No	Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19]	Main Location	High	High			
No	Access Control for Output Devices [NIST 800-53 w/ DHS 4300A PE-5]	Main Location	High	High			

The Show drop-down is a filter where the ISSO may filter on the test generated risk elements, the user-defined risk elements, or both. Clicking on properties icon for the risk element will bring up a more detailed screen.

Edit Risk Element 'Access Agreements [NIST 800-53 w/ DHS 4300A PS-6]'

Name:

Location:

Calculated Risk Level: High

Associated Requirements*

Statement of Issue*

Recommended Fix*

Impact Statement*

Element	Description
Name	The name of the control associated with the risk element. This is not editable.
Location	The physical location of the risk element. This is not editable.

Associated Requirements	Contains the description of the control requirement.
Statement of Issue	Contains the associated test and result of the test.
Recommended Fix	The recommendations for fixing the test if it is not compliant.
Impact Statement	The impact to the system security if the risk element is not mitigated.
Safeguard	Any compensating controls for reducing the impact of the risk element.
Risk Level	The impact of the risk element. This uses the FIPS 199 definitions of low, moderate, and high. This requires a note if it is changed from the baseline.
Risk Assessment	Any notes from the risk assessment.

10.2.2 POA&M ELEMENTS

A plan is needed to address each of the risk elements identified during the risk analysis of your system. This step allows the ISSO to import the risk elements and document the schedule of actions that will be taken to remove (or lower) the risk to your system, such as implement a security patch, complete vulnerability testing, etc. This information can be updated throughout the assessment process and will appear in the Plan of Action and Milestones documentation.

POA&M Elements 

Completed: 

 A plan is needed to address each of the risk elements identified during the risk analysis of your system. This step allows you to import the risk elements and then document the schedule of actions that will be taken to remove (or lower) the risk to your system, such as implement a security patch, complete vulnerability testing, etc. This information can be updated throughout the assessment process and will appear in the Plan of Action and Milestones documentation.

Filter: Filter History  

Rank	POA&M Nbr ▲	Title	Weakness	POC	CAT	Scheduled Completion Date	Status	Assoc. Risk Analyzed	View	Prop.	Copy	Delete	Select All

POA&Ms are created either from a risk element or manually with the New button.

Add Plan of Action Item

POA&M Nbr:

Title*

Creation Date
(mm/dd/yyyy)*

04/15/2013

Weakness:

Severity Code:

- Not Assigned -

Point of
Contact:

Resources
Required:

Scheduled
Completion
Date

Not Applicable:

(mm/dd/yyyy):

Milestones:

<input type="button" value="New"/>			
Date	Description	Delete	Properties

Element	Description
Title	The title of the POA&M. This is usually the name of the NIST control or the OIG/GAO report.
Creation Date	The date the POA&M was created. This field is not editable.
Severity Code	The severity of the POA&M if it is not implemented in a timely manner. IV is the lowest severity and I is the highest.
Point of Contact	The point of contact for the POA&M. This is the person who is most likely to be in the best position for directing and coordinating the activities. This is usually the ISSO.
Resources Required	The amount of resources (time and effort) required to implement the solution identified in the POA&M.
Scheduled Completion Date	The date the POA&M is scheduled for full implementation. This date should be realistic and achievable.
Milestones	A list of milestones. Milestones are critical points of achievement for the implementation of the POA&M.
Item Identified During (other)	This defines where the POA&M was identified in. POA&Ms are found during security assessments, vulnerability scans, etc. If the Item Identified During is defined as other (the only option available), the reason is specified here.
Report ID	The report id if the POA&M's source is an OIG or GAO report.
Overall Status	The overall status of the POA&M.
Comments	Comments for the POA&M.

10.2.3 POA&M REPORT EXTENSIBLE

This step is used to publish the POA&M for use outside of the IACS tool. Click on publish and select the appropriate markings on the pop-up screen. Please refer to the markings section for more information.



10.3 CHANGE LOG

Change Log is the third task in the Monitor phase, which is used to constantly monitor the information system on an ongoing basis through the use of various assessment, documentation and reporting methodologies for any change in the authorized risk level of the system.

In this task:

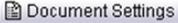
- The ISSO or ISSM completes the Relevant Change Report process step to reflect significant security changes
- The task is submitted for approval and notifications are sent to the ISSO, ISSM, and Component CISO
- When the Change Log task is approved, a snapshot of the project will automatically be taken to preserve historical information.
- The ISSO, ISSM, and Component CISO receives notifications when the task is approved, so they may review the Relevant Change Report and determine if reaccreditation is warranted
- If the system must be reaccredited, the AO reactivates the appropriate tasks, kicking off the reaccreditation process.

Once documentation, testing, certification, and analysis are complete, the associated Tasks will have to be reapproved.

10.3.1 RELEVANT CHANGE REPORT

The ISSO will use this report to document any relevant changes and if required, submit to the DAO for review. Each section is a separate text field. The capabilities of the text fields allow Microsoft Word compatible formatting.

Relevant Change Report

 Save All  Document Settings  Reset  Publish

Completed:    Prev  Next

 **Markings:** Please ensure all paragraphs in text boxes are portion marked with the appropriate security classification and releasability.

The ISSO will use this report to document any relevant changes and if required, submit to the DAO for review.

Publishing Status: Never Published

1.0*

Change Log

The ISSO will document any relevant system changes, the impact and justification of the change(s) below. When the remainder of this report is complete submit to the DAO for review.