NOAA/NESDIS

NESDIS FISMA Inventory Management Policy and Procedures

September 28, 2012

Prepared by:

U.S. Department of Commerce
National Oceanic and Atmospheric Administration (NOAA)
National Environmental Satellite, Data, and Information Service (NESDIS)

Table of Contents

UNITED STATES DEPARTMENT OF COMMERCE
National Oceanic and Atmospheric Administration
NATIONAL ENVIRONMENTAL SATELLITE. DATA AND IINFORMATION SERVICE
Siler Spring, Maryland 209 10

September 30, 2012

MEMORANDUM FOR: Distribution

FROM: Catrina D. Purvis
NESDIS Chief Information Officer (Acting)

SUBJECT: Issuance of Updated NESDIS Information Technology Security Policies and Procedures

This is to announce the issuance of ten updated NESDIS publications for implementing effective, compliant, and consistent information technology (IT)security practices within NESDIS. These documents highlight the specific steps necessary to ensure effective NESDIS implementation. Specifically issued under this memorandum are the

1. NESDIS *Federal Information Processing Standard 199 Security Categorization Policy and Procedures,* v3.0;
2. NESDIS *Plan of Action and Milestones Management Policy and Procedures,* v2.0;
3. NESDIS *Policy and Procedures for Determining Minimum Documentation Requirements for System /111erconnections,* v2.1;
4. NESDIS *Contingency Planning Policy and Procedures,* v2. 1;
5. NESDIS *Policy and Procedures for Ensuring Security i11 NESDIS IT Systems and Services Acquisitions,* v2. 1;
6. NESDIS *Security Assessment Report Policy and Procedures,* v2.0;
7. NESDIS *Federal Information Security Management Act (FISMA) Inventory Management Policy and Procedures,* v2 .0;
8. NESDIS *IT Security Training Policy and Procedures,* v2.l ;
9. NESDIS *Continuous Monitoring Planning Policy and Procedures,* v2. 1; and the
10. *Practices for Securing Open-source Project for a Network Data Access Protocol Server Software 011 NESDIS Information Systems,* v3.l.

These publications are part of the NESDIS-wide effort to maintain and enhance its foundation of NESDIS IT security policies and implementation practices that align with the latest

Department of Commerce and NOAA policies, requirements, and standards. I wish to thank all who contributed reviewing and commenting on the drafts prior to publication to ensure that they are complete, current, and meaningful. These documents will be posted to the Chief Information Division's Web site at https://intranet.nesdis.noaa.gov/ocio/it security/handbook/itsecurityhandbook.php. If you have any questions, please contact the NESDIS IT Security Officer, Nancy Defrancesco, at Nancv.DeFrancesco@noaa.2ov or phone (30I) 713-1312.

FISMA Inventory Management Policy and Procedures

Record of Changes/Revisions

Version	Date	Section	Author	Change Description
0.1	8/14/2009	All	Noblis	Initial Draft
0.2	9/15/2009	All	ITSO	Update for ITSO comments
0.3d	1/30/2010	7.1, 7.2, Appendix B	ITSO	Update for IRMT Security Team comments
0.4d	7/14/2010	Header/footer	ITSO	Remove FOUO markings
1.0	8/20/2010	All	ITSO	Finalize and prepare for issuance
1.1	4/19/2012	All	ITSO Support Staff	Biennial Update
2.0	9/28/2012	All	ITSO	Finalize and prepare for CIO issuance

1.0 Background and Purpose

The Federal Information Security Management Act (FISMA) requires that agencies establish an inventory of major information systems to support FISMA activities. The FISMA Inventory is used to track security information for all systems. Appendix F of the Department of Commerce (DOC) *IT Security Program Policy* (ITSPP) provides the DOC policy for management of the FISMA Inventory. DOC uses the Cyber Security Assessment and Management (CSAM) tool to manage the FISMA inventory across the Department. CSAM provides a DOC enterprise-wide view of security for all systems.

This policy and procedures document prescribes the implementation requirements to comply with the DOC ITSPP for the National Environmental Satellite, Data, and Information Service (NESDIS) and establishes NESDIS-specific FISMA Inventory Management Policies. It additionally provides detailed procedures for managing the FISMA Inventory within CSAM.

2.0 Scope

The scope of this document is limited to providing NESDIS-specific policies for managing the FISMA Inventory. It establishes responsibilities and provides associated step-by-step procedures for how each NESDIS System Owner (SO), Information System Security Officer (ISSO), and Information Technology Security Officer (ITSO) must use CSAM to manage the FISMA Inventory.

3.1 Roles, Responsibilities, and Coordination

3.2 NESDIS Assistant Administrator (AA)

The NESDIS AA serves as the Chief Executive Officer with overall responsibility to provide information security protections commensurate with the risk and magnitude of harm (i.e., impact) to organizational operations and assets, individuals, other organizations, and the Nation resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of: (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

3.3 Chief Information Officer (CIO)

The NOAA Assistant CIO for Satellite and Information Services establishes and oversees the NESDIS-specific continuous monitoring program and advises executive leadership regarding the security risk associated with continuous monitoring results reported.

3.4 Information Technology Security Officer (ITSO)

The ITSO performs oversight of and ensures compliance with the NESDIS FISMA Inventory management policies and CSAM procedures established by this document. The ITSO may delegate oversight responsibilities to other NESDIS CID personnel.

3.5 System Owner (SO)

The SO is responsible for maintaining FISMA Inventory data for systems under their purview. Some NESDIS, National Oceanic and Atmospheric Administration (NOAA), and DOC personnel have direct access to the information and will review it without notice. The SO is responsible for ensuring the information is accurate and current.

3.6 Information System Security Officer (ISSO)

The ISSO is responsible for assisting the SO with the maintenance of FISMA inventory data. If directed by the SO, the ISSO must ensure the information is accurate and current.

4.0 Management Commitment

The NESDIS Chief Information Division (CID) supports the NESDIS Assistant Administrator’s (AA) strong emphasis on securing NESDIS information and information systems. Through the issuance of this guidance, the NESDIS CID demonstrates its commitment to identifying policies and procedures for managing the FISMA Inventory in a consistent and cost-effective manner.

5.1 Compliance

The NESDIS ITSO monitors – through periodic quality reviews and monthly performance metrics – management of the CSAM FISMA Inventory within NESDIS to ensure compliance with applicable laws, directives, policies, and guidance. The ITSO reports monthly to the AA, and to the Chief Information Officer (CIO) and Office Directors as necessary, but at least monthly, regarding compliance. The AA, CIO, and/or Office Directors may initiate actions as necessary to correct reported deficiencies, including reallocation of resources to improve implementation of security practices, or removal of an individual from their role as AO, SO, ITSO, or ISSO.

5.2 References

- DOC ITSPP section 4.12.1 (January 2009)

6.1 Policy

As required by DOC ITSPP section 4.12.1 and ITSPP Appendix F, NESDIS SOs shall establish and update semi-annually, system identification information and status of the performance of security requirements in the CSAM tool. The NESDIS ITSO shall monitor the completeness and accuracy of FISMA inventory data maintained by SOs.

6.2 Policy Maintenance

The NESDIS ITSO shall review this policy and procedures bi-annually and update as necessary to reflect implementation challenges and new requirements. All updates to this policy shall be subject to a NESDIS-wide vetting process providing an opportunity for stakeholders to comment on the programmatic implications of updates.

6.3 Policy Feedback Process

NESDIS personnel are encouraged to notify the ITSO via e-mail at nesdis.it.security@noaa.gov regarding any errors found in the document or other clarifications or updates that are required.

6.4 Policy Effective Date

This policy is effective within 30 days of issuance.

7.0 FISMA Inventory Procedures

According to DOC policy FISMA Inventory data will be maintained in CSAM. System FISMA Inventory data is contained in the General, Info Types (Information Types), Locations, Interfaces, POCs (Points of Contact), and Status screens of CSAM (see section 7.2).

The SO must ensure that information for systems in development is added to the FISMA Inventory in CSAM according to the procedures outlined in section 7.1. The minimum information required for development systems is identified in Table 3 CSAM FISMA Inventory Data Requirements of Appendix A. FISMA Inventory information for the system must be maintained throughout its lifecycle, as described in the remainder of this section.

The SO must review and update FISMA Inventory data in the Status screen according to the frequency and schedule prescribed in Table 4 CSAM Security Status Update Guide of Appendix B. In general, these updates must be performed in CSAM on or before a security activity is due for completion. This is because some NESDIS, NOAA and DOC personnel have direct access to the information and will review it without notice. In addition, timely reporting will prevent those security activities that are tracked for the CID monthly and support the OMB Exhibit 300 process (see Table 5 Reference for OMB Exhibit 300s - Security and Privacy Tables of Appendix C) from being flagged as non-compliant as a result of reporting delays. The SO must allot time in associated schedules (e.g., A&A project schedule) to ensure that security status reporting occurs as required.

The SO, must review and update, as needed, FISMA Inventory data contained in CSAM screens for describing the system, identifying responsibility and specifying interconnections.

These include the General, Info Types, Locations, Interfaces, and POCs screens (see section 7.2). Reviews and updates will occur quarterly and according to the schedule outlined in Table 1 below. Update procedures and field requirements are in section 7.3 and Table 3 CSAM FISMA Inventory Data Requirements of Appendix A.

The NESDIS CID will perform a quality review of all FISMA Inventory data on a quarterly basis. Review procedures are outlined in section 7.4. The review schedule is contained in Table 2 NESDIS CID FISMA Inventory Review Schedule of that section.

Table 1 FISMA Inventory Update Schedule (System Description, Responsibility and Interconnections Only)

FY Quarter	SO review and updates completed by close of business on the 15th (or next business day)
1	November
2	February
3	May
4	August

Appendix B identifies what artifacts are required for each security related activity listed in the CSAM Status screen. Artifacts must be uploaded within 10 business days from the time a security activity is completed. Procedures for uploading artifacts are described in section 7.3.7.1. The SO must include time in project schedules (e.g., A&A project plan) to ensure artifacts are uploaded to CSAM as required.

7.1 Adding a System to the FISMA Inventory

Follow the steps below to request the addition of a system to the FISMA Inventory:

Step 1. The SO, or authorized delegate, will discuss with the NESDIS ITSO the need to add a system to the FISMA Inventory. If agreed that a new system is warranted, the NESDIS ITSO will provide the SO a form to complete and within five business days of receiving the completed form, will issue a memo to NOAA OCIO requesting that the system be added to CSAM.

Step 2. The SO, or authorized delegate, will then send the completed request form to the NESDIS IT Security Team at nesdis.it.security@noaa.gov.

Step 3. The NESDIS ITSO will send the form with request memo to the CIO (with courtesy copy to the NOAA OCIO IT Security Director).

Step 4. The NESDIS ITSO will notify the SO upon receipt of the confirmation from NOAA OCIO that the system has been added to the FISMA Inventory in CSAM.

The SO, or authorized delegate, will have 10 business days to complete Steps 5 and 6.

Step 5. Review and update as needed the system information added by the NOAA OCIO (see Table 3 CSAM FISMA Inventory Data Requirements of Appendix A for field requirements).

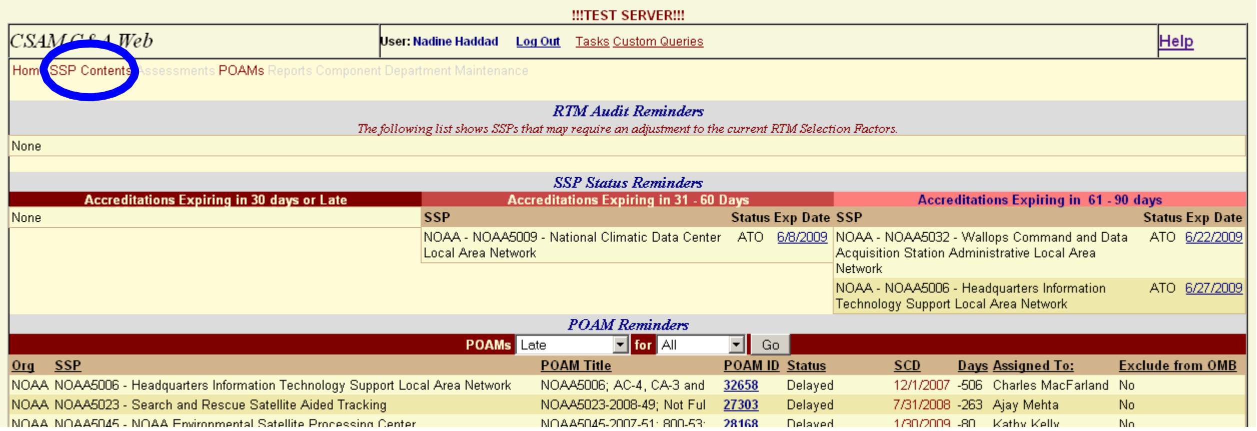
Step 6. Complete remaining updates associated with the new system record according to Table 3 CSAM FISMA Inventory Data Requirements of Appendix A.

7.2 Locating FISMA Inventory Data

FISMA Inventory data in CSAM is contained in multiple screens associated with each system.

Follow the steps below to locate FISMA Inventory data in CSAM:

Step 1. Select *SSP Contents* in the top menu.



RTM Audit Reminders

The following list shows SSPs that may require an adjustment to the current RTM Selection Factors.

None

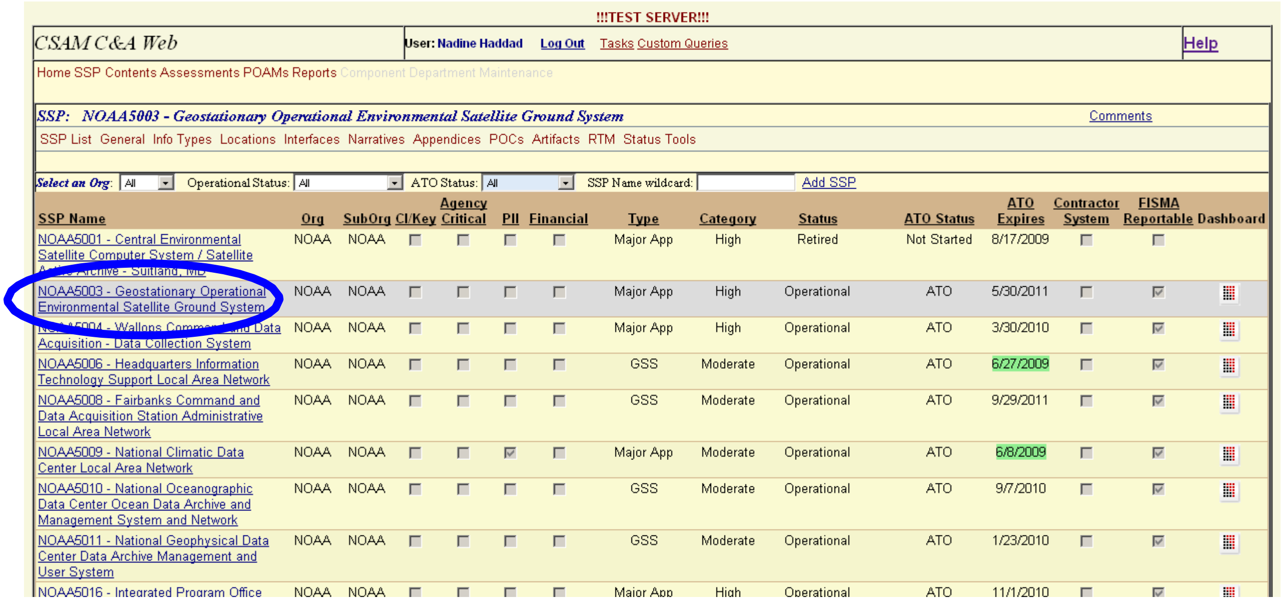
SSP Status Reminders

Accreditations Expiring in 30 days or Late	Accreditations Expiring in 31 - 60 Days			Accreditations Expiring in 61 - 90 days		
	SSP	Status	Exp Date	SSP	Status	Exp Date
None	NOAA - NOAA5009 - National Climatic Data Center Local Area Network	ATO	6/8/2009	NOAA - NOAA5032 - Wallops Command and Data Acquisition Station Administrative Local Area Network	ATO	6/22/2009
				NOAA - NOAA5006 - Headquarters Information Technology Support Local Area Network	ATO	6/27/2009

POAM Reminders

Org	SSP	POAM Title	POAM ID	Status	SCD	Days	Assigned To:	Exclude from OMB
NOAA	NOAA5006 - Headquarters Information Technology Support Local Area Network	NOAA5006; AC-4, CA-3 and	32658	Delayed	12/1/2007	-506	Charles MacFarland	No
NOAA	NOAA5023 - Search and Rescue Satellite Aided Tracking	NOAA5023-2008-49; Not Ful	27303	Delayed	7/31/2008	-263	Ajay Mehta	No
NOAA	NOAA5045 - NOAA Environmental Satellite Processing Center	NOAA5045-2007-51; 800-53;	28168	Delayed	1/30/2009	-80	Kathy Kelly	No

a. If you have more than one system in your SSP list, select the system SSP for which you would like to review FISMA information.



!!!TEST SERVER!!!

CSAM C&A Web | User: Nadine Haddad Log Out Tasks Custom Queries | Help

Home SSP Contents Assessments POAMs Reports Component Department Maintenance

SSP: NOAA5003 - Geostationary Operational Environmental Satellite Ground System Comments

SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools

Select an Org: All Operational Status: All ATO Status: All SSP Name wildcard: Add SSP

				Agency							ATO	Contractor	FISMA	
SSP Name	Org	SubOrg	CI/Key	Critical	PII	Financial	Type	Category	Status	ATO Status	Expires	System	Reportable	Dashboard
NOAA5001 - Central Environmental Satellite Computer System / Satellite Active Archive - Suitland, MD	NOAA	NOAA	☐	☐	☐	☐	Major App	High	Retired	Not Started	8/17/2009	☐	☐	
NOAA5003 - Geostationary Operational Environmental Satellite Ground System	NOAA	NOAA	☐	☐	☐	☐	Major App	High	Operational	ATO	5/30/2011	☐	☑	▦
NOAA5004 - Wallops Command and Data Acquisition - Data Collection System	NOAA	NOAA	☐	☐	☐	☐	Major App	High	Operational	ATO	3/30/2010	☐	☑	▦
NOAA5006 - Headquarters Information Technology Support Local Area Network	NOAA	NOAA	☐	☐	☐	☐	GSS	Moderate	Operational	ATO	6/27/2009	☐	☑	▦
NOAA5008 - Fairbanks Command and Data Acquisition Station Administrative Local Area Network	NOAA	NOAA	☐	☐	☐	☐	GSS	Moderate	Operational	ATO	9/29/2011	☐	☑	▦
NOAA5009 - National Climatic Data Center Local Area Network	NOAA	NOAA	☐	☐	☑	☐	Major App	Moderate	Operational	ATO	6/8/2009	☐	☑	▦
NOAA5010 - National Oceanographic Data Center Ocean Data Archive and Management System and Network	NOAA	NOAA	☐	☐	☐	☐	GSS	Moderate	Operational	ATO	9/7/2010	☐	☑	▦
NOAA5011 - National Geophysical Data Center Data Archive Management and User System	NOAA	NOAA	☐	☐	☐	☐	GSS	Moderate	Operational	ATO	1/23/2010	☐	☑	▦
NOAA5016 - Integrated Program Office	NOAA	NOAA	☐	☐	☐	☐	Major App	High	Operational	ATO	11/1/2010	☐	☑	▦

Step 2. Select the FISMA Inventory data you want to view:

a. **General:** Displays a summary of information entered for a system, including some information contained in other screens (e.g., Data Types screen).

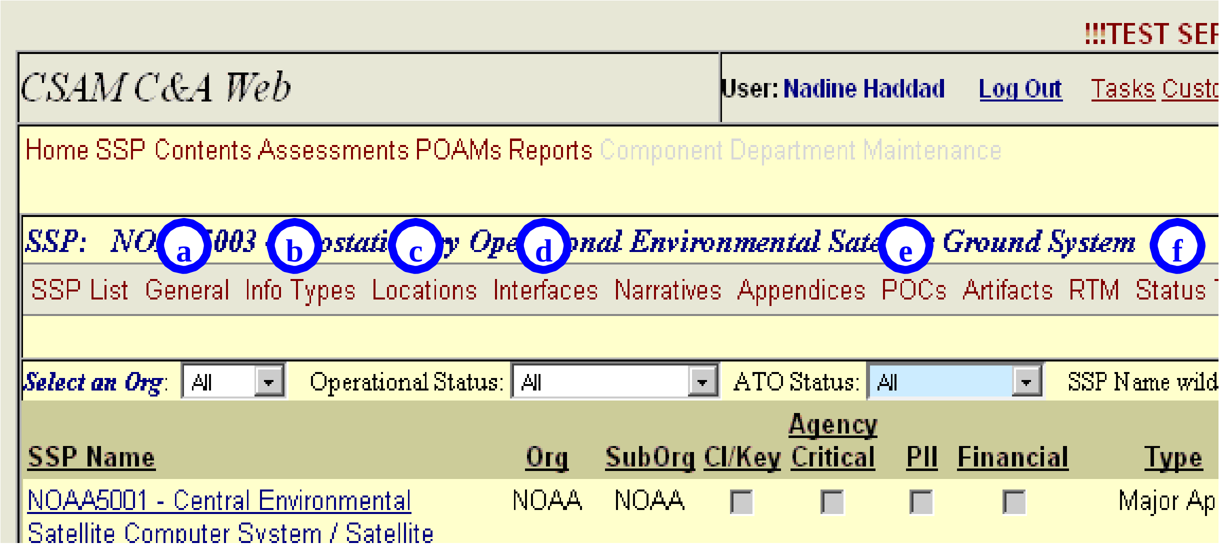
b. **Info Types:** This screen will display a complete list of data types and associated security impact levels for Confidentiality, Integrity, and Availability. The Data Types must match the formal FIPS 199 categorization of the system. It is possible to add multiple data types to the list as well as edit or delete data types.

c. **Locations:** This screen lists the physical locations where a system is operated or accessed. It is possible to add multiple locations to the list as well as edit or delete location records.

d. **Interfaces:** This screen lists all interconnections a system has with other systems. It is possible to add multiple interconnections, remove listed interconnections and attach any interconnection agreements and/or memorandums of understanding (MOUs).

e. **POCs:** This screen displays a list of key points of contact for a system, minimally the AO, SO, and ISSO.

f. **Status:** This screen displays key information about the security status of a system.



!!!TEST SEF

CSAM C&A Web

User: Nadine Haddad Log Out Tasks Custo

Home SSP Contents Assessments POAMs Reports Component Department Maintenance

SSP: NO 003 ostati y Ope onal Environmental Sate Ground System

SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status

Select an Org: All Operational Status: All ATO Status: All SSP Name wild

SSP Name	Org	SubOrg	CI/Key	Agency Critical	PII	Financial	Type
NOAA5001 - Central Environmental Satellite Computer System / Satellite	NOAA	NOAA	□	□	□	□	Major Ap

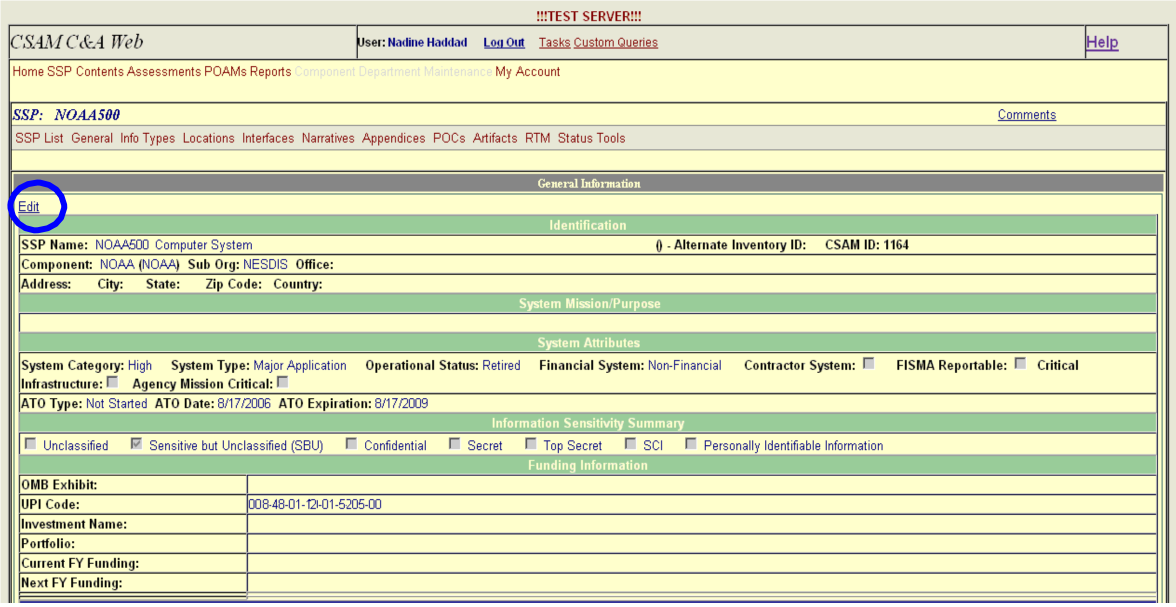
7.3 Updating FISMA Inventory Data

To locate each screen in the FISMA Inventory, see section 7.2. Requirements for updating the General, Info Types, Locations, Interfaces, POCs and Status screens are outlined in Table 3 CSAM FISMA Inventory Data Requirements of Appendix A. Please note that one must have the Primary Author role in order to make updates to each screen. Consult the supplementary document *Getting Started with the Cyber Security Assessment and Management (CSAM) Tool* for a discussion of CSAM roles.

7.3.1 General

Follow the steps below to begin making changes to the General screen:

Step 1. Select the *Edit* link in the top left corner of the screen.



SSP: NOAA500

General Information

Identification

SSP Name: NOAA500 Computer System () - Alternate Inventory ID: CSAM ID: 1164

Component: NOAA (NOAA) Sub Org: NESDIS Office:

Address: City: State: Zip Code: Country:

System Mission/Purpose

System Attributes

System Category: High System Type: Major Application Operational Status: Retired Financial System: Non-Financial Contractor System: □ FISMA Reportable: □ Critical Infrastructure: □ Agency Mission Critical: □

ATO Type: Not Started ATO Date: 8/17/2006 ATO Expiration: 8/17/2009

Information Sensitivity Summary

□ Unclassified ☑ Sensitive but Unclassified (SBU) □ Confidential □ Secret □ Top Secret □ SCI □ Personally Identifiable Information

Funding Information

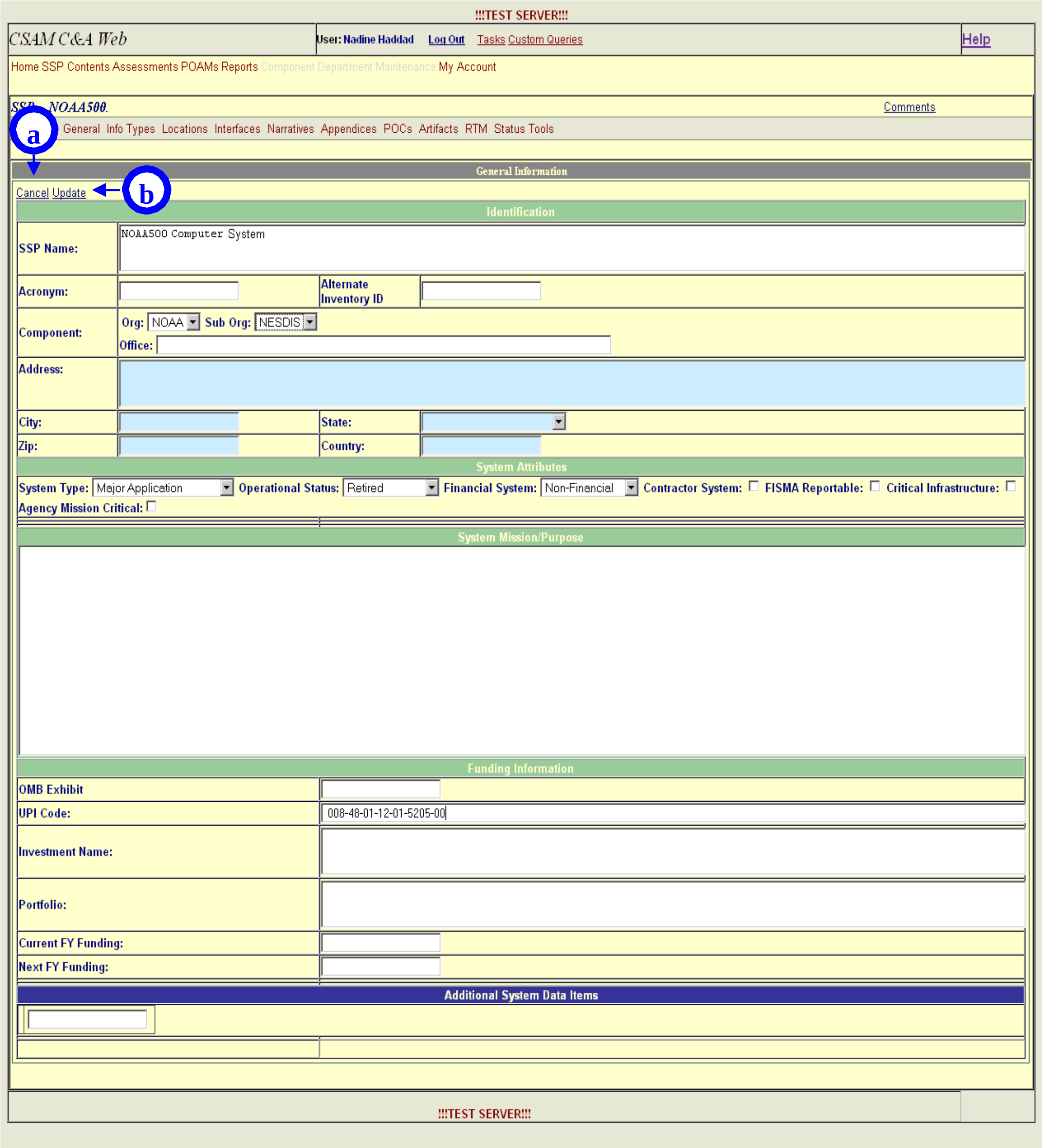
OMB Exhibit:	
UPI Code:	008-48-01-12-01-5205-00
Investment Name:	
Portfolio:	
Current FY Funding:	
Next FY Funding:	

Step 2. Enter required information into the form (see Table 3 CSAM FISMA Inventory Data Requirements of Appendix A).

Step 3. Exit with or without saving changes.

a. Select *Cancel* to exit without saving changes.

b. Select *Update* to exit and save changes.


!!!TEST SERVER!!!
CSAM C&A Web
Log Out
Tasks Custom Queries
Help
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
Comments
General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
a
b
Cancel Update
!!!TEST SERVER!!!

User: Nadine Haddad

SSP - NOAA500

General Information

Identification

SSP Name:	NOAA500 Computer System		
Acronym:		Alternate Inventory ID	
Component:	Org: NOAA Sub Org: NESDIS Office:		
Address:			
City:		State:	
Zip:		Country:	

System Attributes

System Type: Major Application Operational Status: Retired Financial System: Non-Financial Contractor System: □ FISMA Reportable: □ Critical Infrastructure: □
Agency Mission Critical: □

System Mission/Purpose

Funding Information

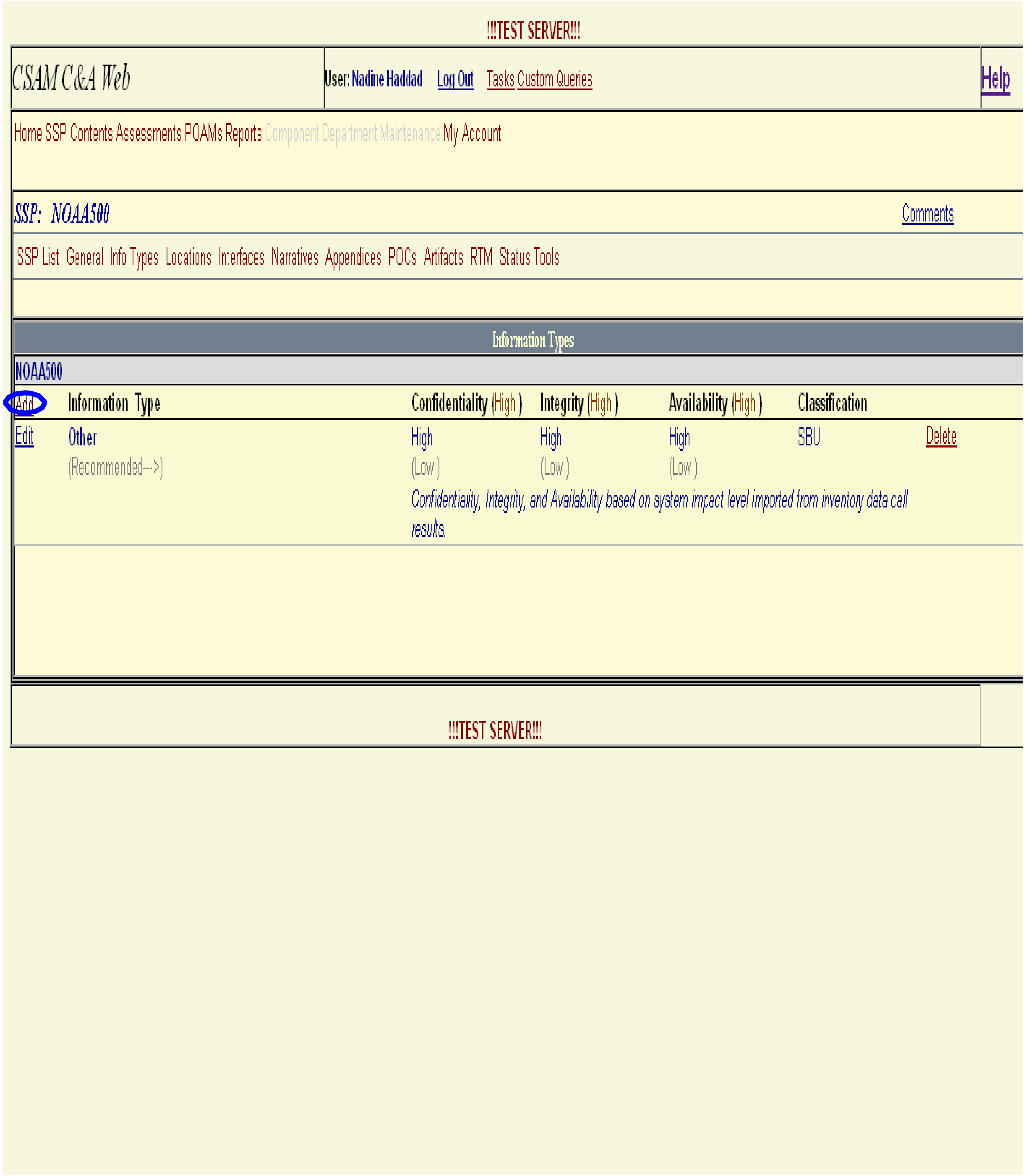
OMB Exhibit	
UPI Code:	008-48-01-12-01-5205-00
Investment Name:	
Portfolio:	
Current FY Funding:	
Next FY Funding:	

Additional System Data Items

7.3.2 Info Types

Follow the steps below to add an information type:

Step 1. Select the *Add* link in the top left corner of the screen.


!!!TEST SERVER!!!
CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks
Custom Queries
Help
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
SSP: NOAA500
Comments
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
Information Types
NOAA500

Add	Information Type	Confidentiality (High)	Integrity (High)	Availability (High)	Classification	
Edit	Other (Recommended-->)	High (Low)	High (Low)	High (Low)	SBU	Delete

Confidentiality, Integrity, and Availability based on system impact level imported from inventory data call results.

Step 2. Perform the following actions to add the information type:

a. Select a business area.

b. Select an information type.

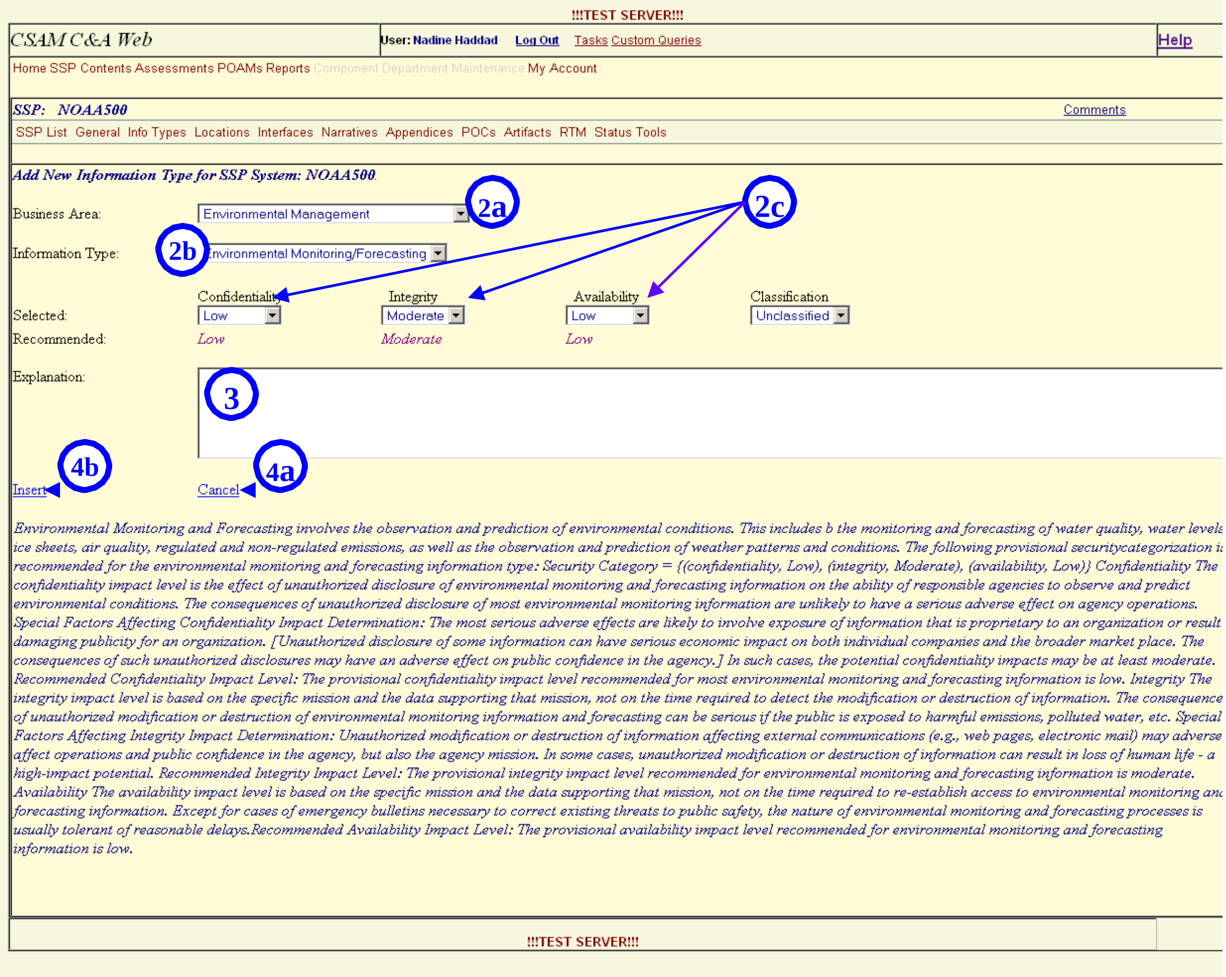
Note : Confidentiality, Integrity, and Availability impact levels will be automatically defined based on the selected business area and the information type selected (see “2c” in the figure below).

Step 3. Explain any modifications to the default Confidentially, Integrity and Availability values in the “Explanation” field.

Step 4. Exit with or without savings changes.

a. Select *Cancel* to exit without saving.

b. Select *Insert* to save all changes and exit.


!!!TEST SERVER!!!
CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks
Custom Queries
Help
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
SSP: NOAA500
Comments
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
2a
2b
2c
3
4a
4b
Insert
Cancel
!!!TEST SERVER!!!

Add New Information Type for SSP System: NOAA500.

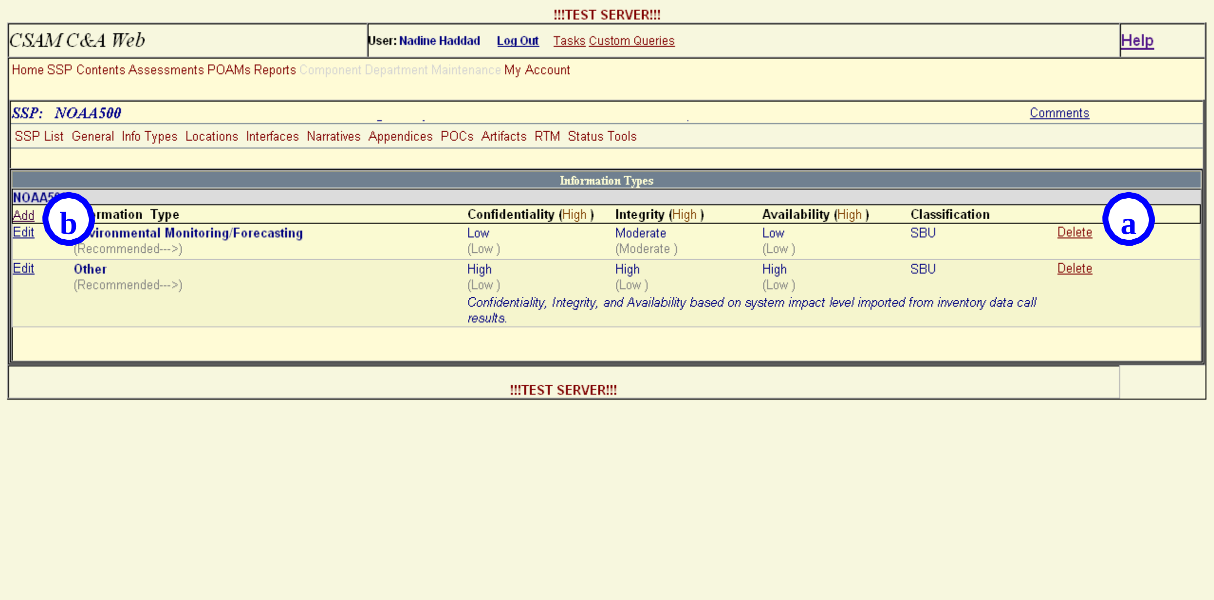
Business Area:	Environmental Management			
Information Type:	Environmental Monitoring/Forecasting			
	Confidentiality	Integrity	Availability	Classification
Selected:	Low	Moderate	Low	Unclassified
Recommended:	*Low*	*Moderate*	*Low*	
Explanation:				

Environmental Monitoring and Forecasting involves the observation and prediction of environmental conditions. This includes b the monitoring and forecasting of water levels ice sheets, air quality, regulated and non-regulated emissions, as well as the observation and prediction of weather patterns and conditions. The following provisional securitycategorization i recommended for the environmental monitoring and forecasting information type: Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)} Confidentiality The confidentiality impact level is the effect of unauthorized disclosure of environmental monitoring and forecasting information on the ability of responsible agencies to observe and predict environmental conditions. The consequences of unauthorized disclosure of most environmental monitoring information are unlikely to have a serious adverse effect on agency operations. Special Factors Affecting Confidentiality Impact Determination: The most serious adverse effects are likely to involve exposure of information that is proprietary to an organization or result damaging publicity for an organization. [Unauthorized disclosure of some information can have serious economic impact on both individual companies and the broader market place. The consequences of such unauthorized disclosures may have an adverse effect on public confidence in the agency.] In such cases, the potential confidentiality impacts may be at least moderate. Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most environmental monitoring and forecasting information is low. Integrity The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequence of unauthorized modification or destruction of environmental monitoring information and forecasting can be serious if the public is exposed to harmful emissions, polluted water, etc. Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adverse affect operations and public confidence in the agency, but also the agency mission. In some cases, unauthorized modification or destruction of information can result in loss of human life - a high-impact potential. Recommended Integrity Impact Level: The provisional integrity impact level recommended for environmental monitoring and forecasting information is moderate. Availability The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to environmental monitoring and forecasting information. Except for cases of emergency bulletins necessary to correct existing threats to public safety, the nature of environmental monitoring and forecasting processes is usually tolerant of reasonable delays.Recommended Availability Impact Level: The provisional availability impact level recommended for environmental monitoring and forecasting information is low.

Step 5. If a new information type is added, it will appear in the *Information Types* list as shown in the figure below.

a. To remove the record, select *Delete.*

b. To modify an existing record, select the *Edit* link that corresponds with that record.


!!!TEST SERVER!!!
CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks Custom Queries
Help
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
SSP: NOAA500
Comments
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
Information Types
NOAA5
b
a
!!!TEST SERVER!!!

Add	rmation Type	Confidentiality (High)	Integrity (High)	Availability (High)	Classification	
Edit	vironmental Monitoring/Forecasting (Recommended--->)	Low (Low)	Moderate (Moderate)	Low (Low)	SBU	Delete
Edit	Other (Recommended--->)	High (Low)	High (Low)	High (Low)	SBU	Delete

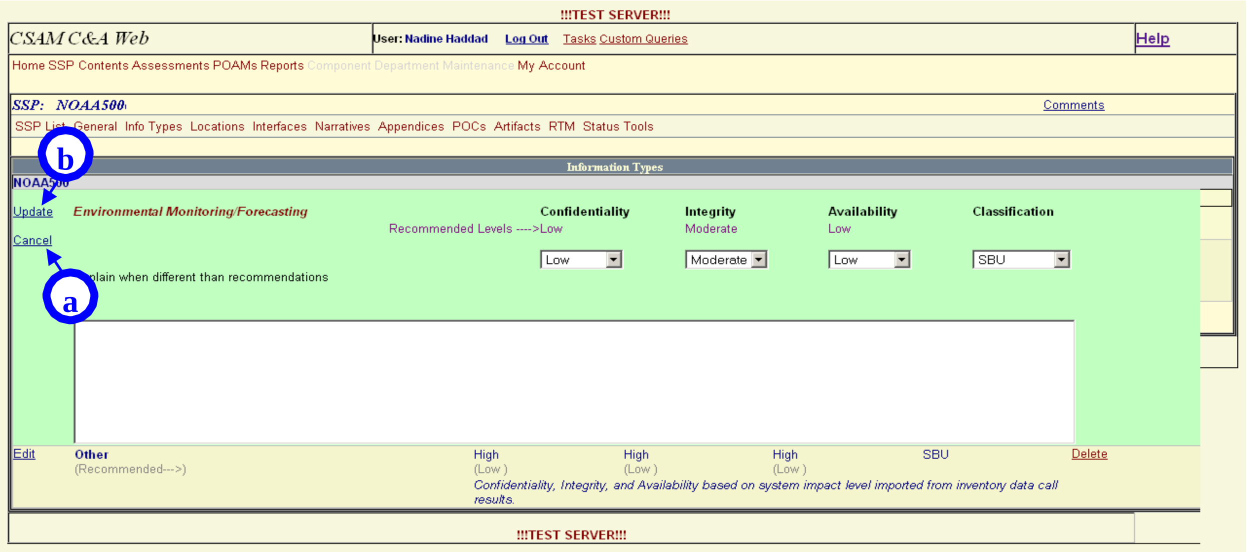
Confidentiality, Integrity, and Availability based on system impact level imported from inventory data call results.

Step 6. Make any necessary changes to information in the form.

Step 7. Exit with or without saving changes.

a. Select *Cancel* to exit without saving changes.

b. Select *Update* to exit and save changes.



!!!TEST SERVER!!!

CSAM C&A Web | User: Nadine Haddad | Log Out | Tasks Custom Queries | Help

Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account

SSP: NOAA500 | Comments

SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools

Information Types

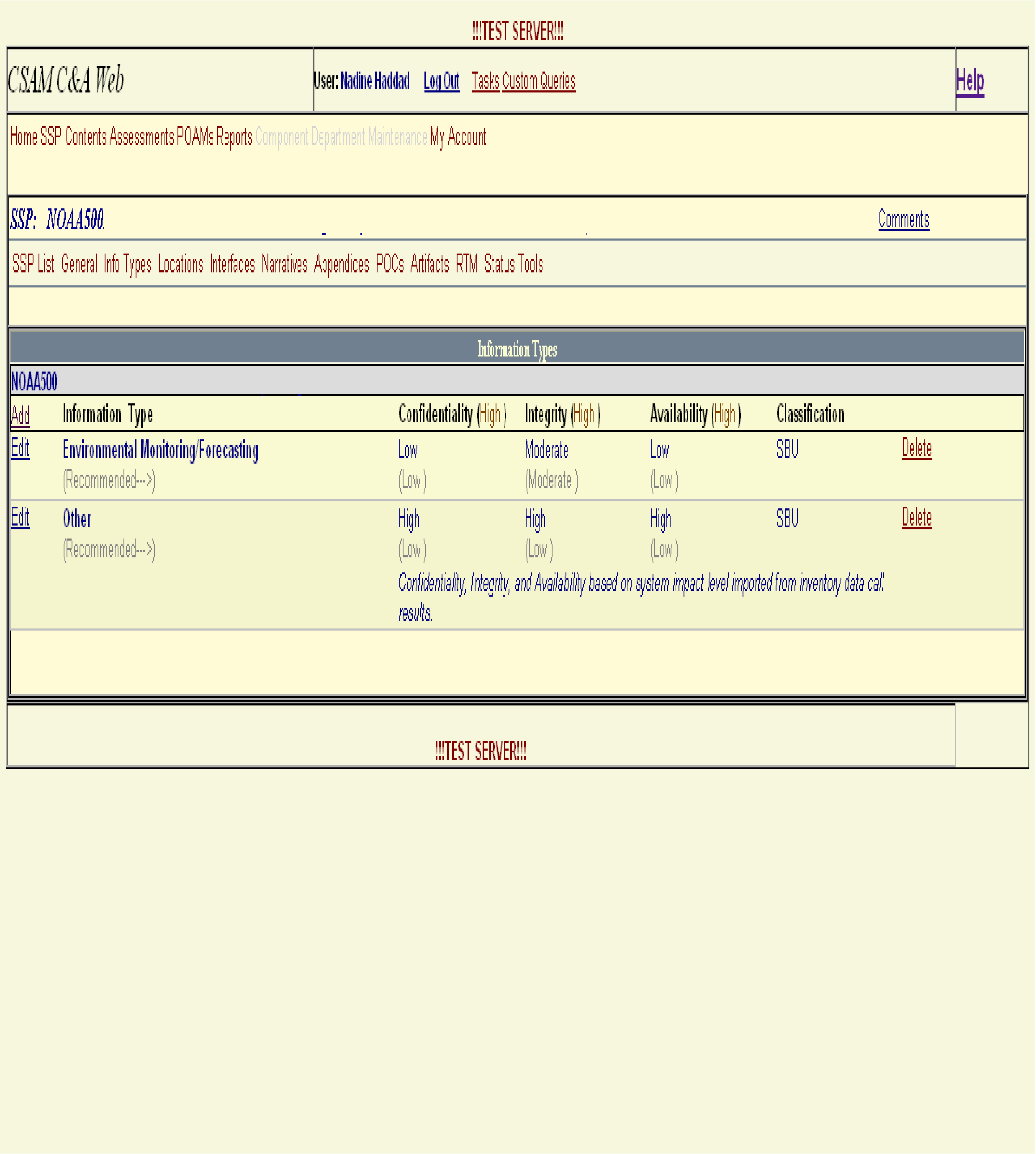
NOAA500

		Confidentiality	Integrity	Availability	Classification	
Update Cancel	*Environmental Monitoring/Forecasting* Recommended Levels ---->	Low Low	Moderate Moderate	Low Low	SBU	
	plain when different than recommendations					
Edit	**Other** (Recommended--->)	High (Low)	High (Low)	High (Low)	SBU	Delete

Confidentiality, Integrity, and Availability based on system impact level imported from inventory data call results.

!!!TEST SERVER!!!

Saved changes will appear in the “Information Types” list as shown in the figure below.


!!!TEST SERVER!!!
CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks
Custom Queries
Help
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
SSP: NOAA500
Comments
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
Information Types
NOAA500
!!!TEST SERVER!!!

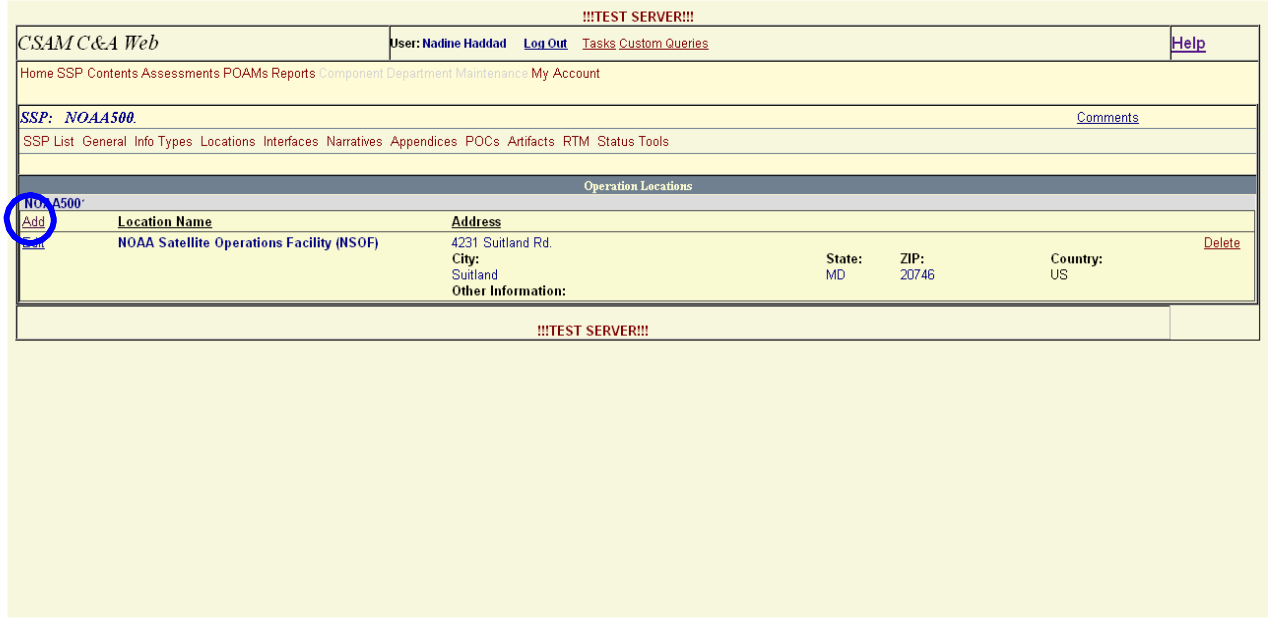
Add	Information Type	Confidentiality (High)	Integrity (High)	Availability (High)	Classification	
Edit	Environmental Monitoring/Forecasting (Recommended-->)	Low (Low)	Moderate (Moderate)	Low (Low)	SBU	Delete
Edit	Other (Recommended-->)	High (Low)	High (Low)	High (Low)	SBU	Delete

Confidentiality, Integrity, and Availability based on system impact level imported from inventory data call results.

7.3.3 Locations

Follow the steps below to add a location:

Step 1. Select the *Add* link in the top left corner of the screen.


!!!TEST SERVER!!!
CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks Custom Queries
Help
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
SSP: NOAA500.
Comments
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
Operation Locations
NOAA500'
!!!TEST SERVER!!!

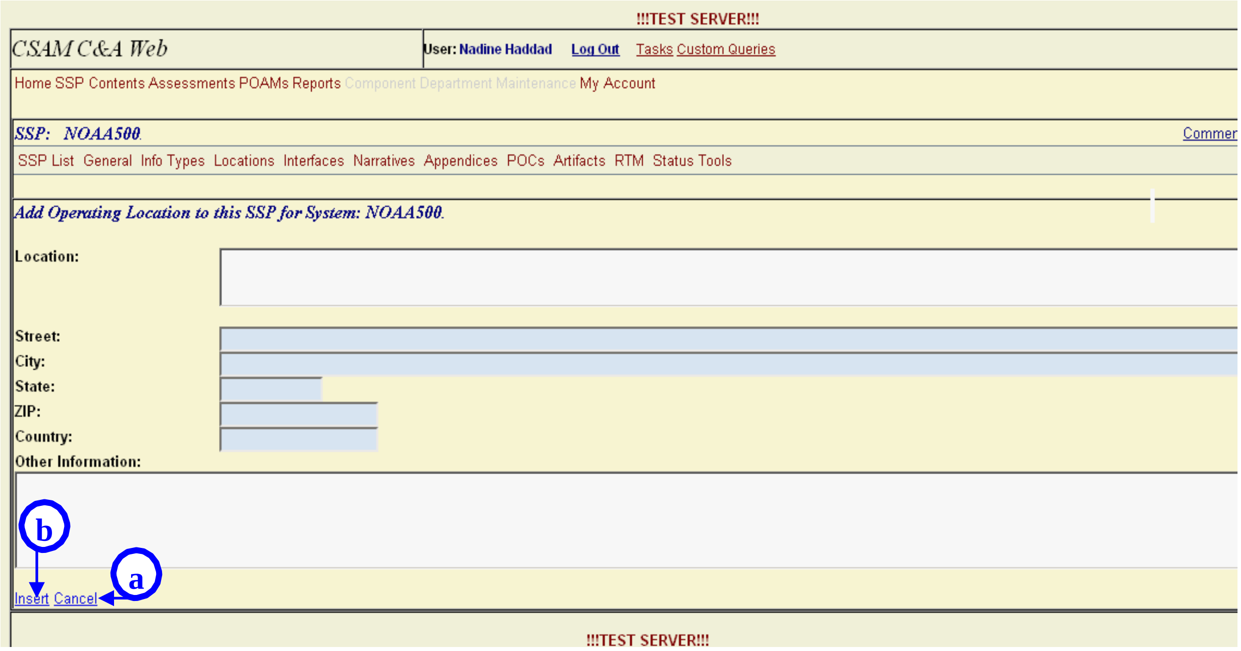
Add	Location Name	Address				
Edit	NOAA Satellite Operations Facility (NSOF)	4231 Suitland Rd.				Delete
		City: Suitland	State: MD	ZIP: 20746	Country: US	
		Other Information:				

Step 2. Enter the Location name, Street Address, City, State and Country into the form.

Step 3. Exit with or without saving changes.

a. Select *Cancel* to exit without saving changes.

b. Select *Insert* to save changes and exit.


!!!TEST SERVER!!!
CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks
Custom Queries
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
Commer
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
b
a
Insert
Cancel
!!!TEST SERVER!!!

SSP: NOAA500.

Add Operating Location to this SSP for System: NOAA500.

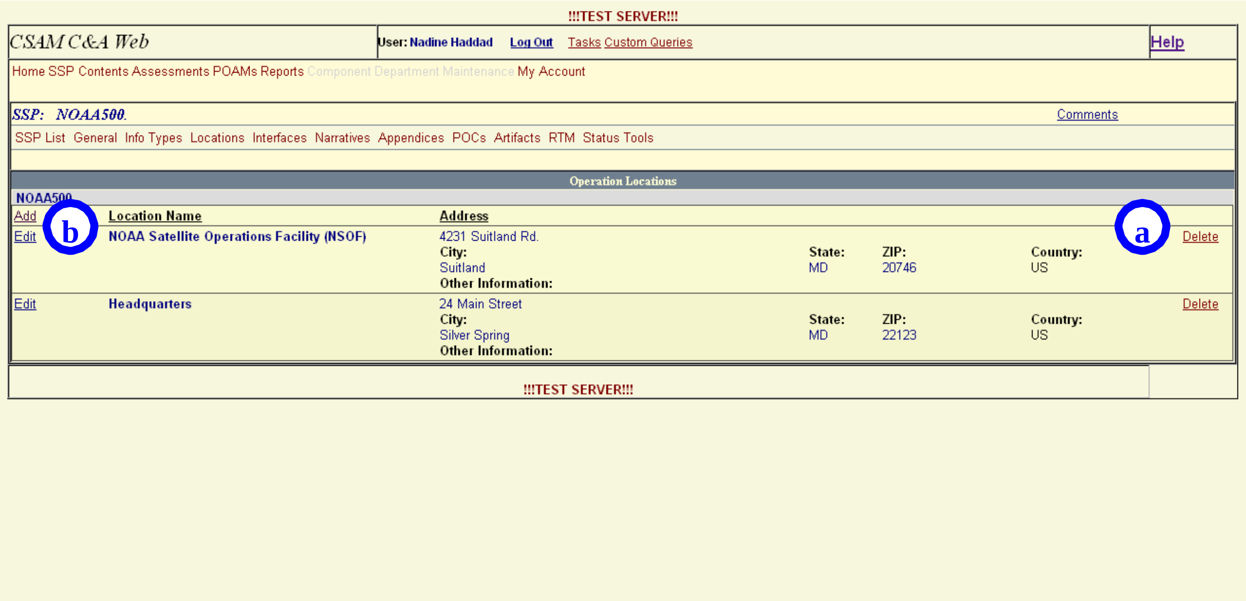
Location:

Street:
City:
State:
ZIP:
Country:
Other Information:

Step 4. If a new record was added, it will appear in the Operation Locations list as shown in the figure below.

a. To remove the record, select *Delete*.

b. To modify an existing record, select the *Edit* link that corresponds with that record.


!!!TEST SERVER!!!
CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks
Custom Queries
Help
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
Comments
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
b
a
!!!TEST SERVER!!!

SSP: NOAA500.

Operation Locations

NOAA500

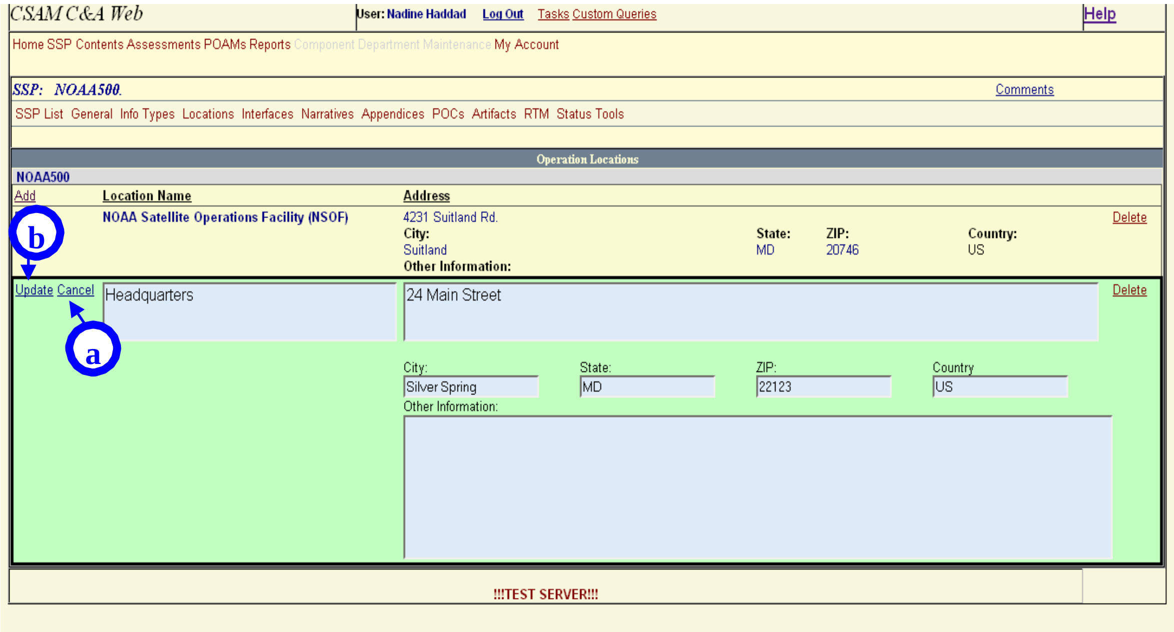
Add	Location Name	Address				
Edit	NOAA Satellite Operations Facility (NSOF)	4231 Suitland Rd. City: Suitland Other Information:	State: MD	ZIP: 20746	Country: US	Delete
Edit	Headquarters	24 Main Street City: Silver Spring Other Information:	State: MD	ZIP: 22123	Country: US	Delete

Step 5. Make any necessary changes to information in the form.

Step 6. Exit with or without savings changes.

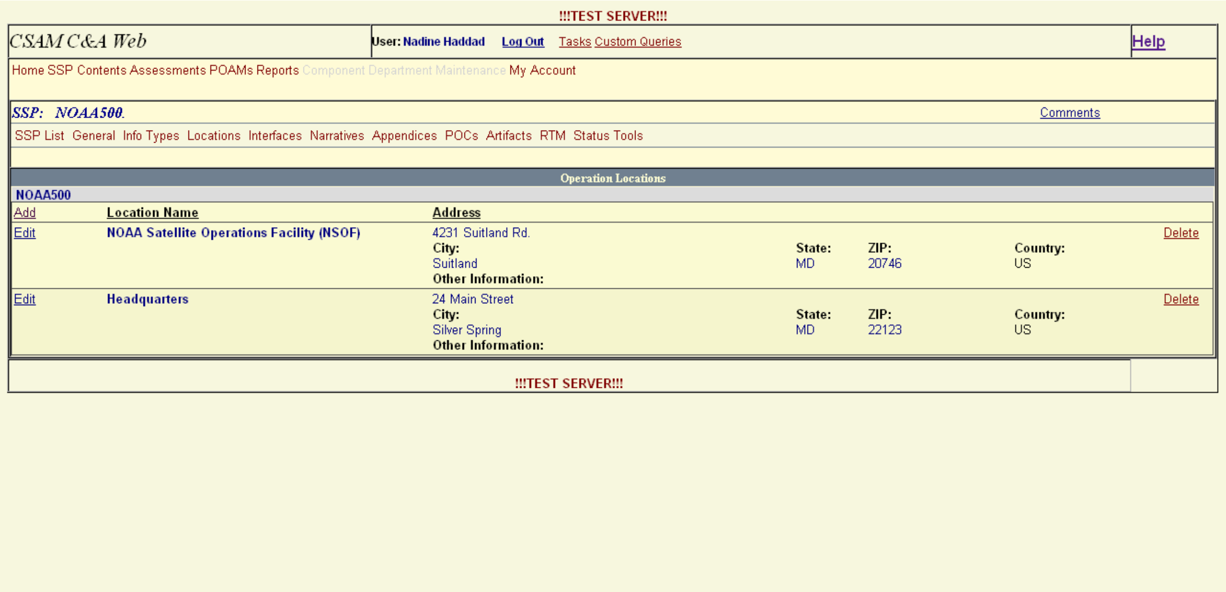
a. Select *Cancel* to exit without saving changes.

b. Select *Update* to exit and save changes.


CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks Custom Queries
Help
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
SSP: NOAA500.
Comments
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
Operation Locations
NOAA500
b
Update Cancel
a
Delete
!!!TEST SERVER!!!

Add	Location Name	Address				
	NOAA Satellite Operations Facility (NSOF)	4231 Suitland Rd. City: Suitland Other Information:	State: MD	ZIP: 20746	Country: US	Delete
Update Cancel	Headquarters	24 Main Street City: Silver Spring Other Information:	State: MD	ZIP: 22123	Country US	Delete

If the record has been edited, saved changes will appear in the Operation Locations list.

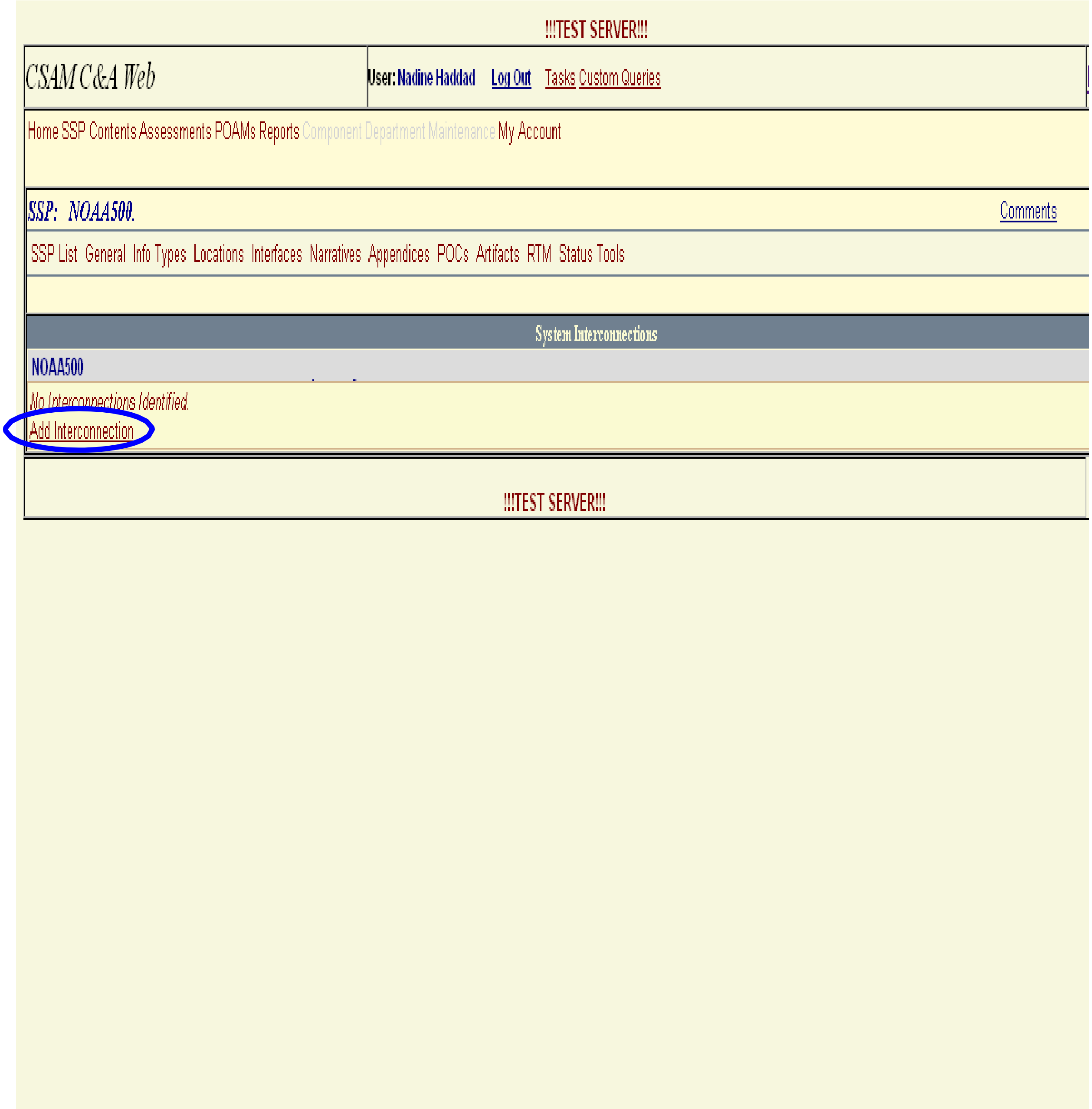

!!!TEST SERVER!!!
CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks Custom Queries
Help
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
SSP: NOAA500.
Comments
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
Operation Locations
NOAA500
!!!TEST SERVER!!!

Add	Location Name	Address				
Edit	NOAA Satellite Operations Facility (NSOF)	4231 Suitland Rd. City: Suitland Other Information:	State: MD	ZIP: 20746	Country: US	Delete
Edit	Headquarters	24 Main Street City: Silver Spring Other Information:	State: MD	ZIP: 22123	Country: US	Delete

7.3.4 Interfaces

Follow the steps below to add an interface:

Step 1. Select the *Add Interconnection* link in the top left corner of the screen.


!!!TEST SERVER!!!
CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks Custom Queries
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
SSP: NOAA500.
Comments
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
System Interconnections
NOAA500
Add Interconnection
!!!TEST SERVER!!!

No Interconnections Identified.

Step 2. Enter required information into the form.

Step 3. Enter or select the System Name for which an interconnection exists (selecting the system name will automatically populate the remainder of the form).

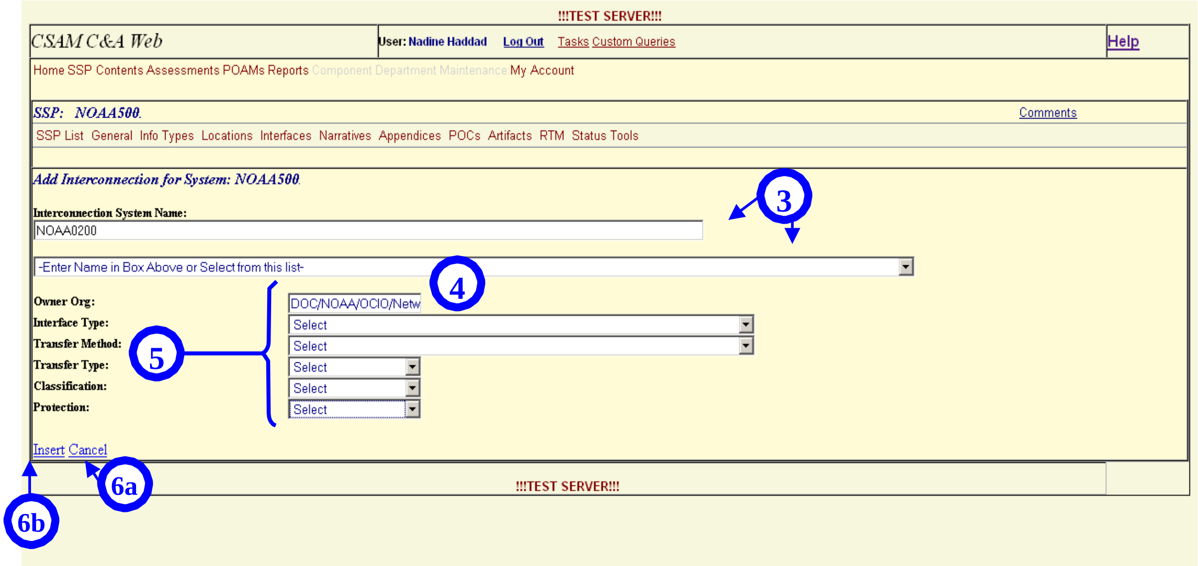
Step 4. Verify or enter the Owner Org field.

Step 5. Verify or enter the Interface Type, Transfer Method, Transfer Type, Classification, and Protection fields (if not known, choose the option "Select" for these values).

Step 6. Exit with or without saving changes.

a. Select *Cancel* to exit without saving changes.

b. Select *Insert* to save changes and exit.


!!!TEST SERVER!!!
CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks Custom Queries
Help
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
SSP: NOAA500.
Comments
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
3
4
5
Insert Cancel
6a
6b
!!!TEST SERVER!!!

Add Interconnection for System: NOAA500.

Interconnection System Name: NOAA0200

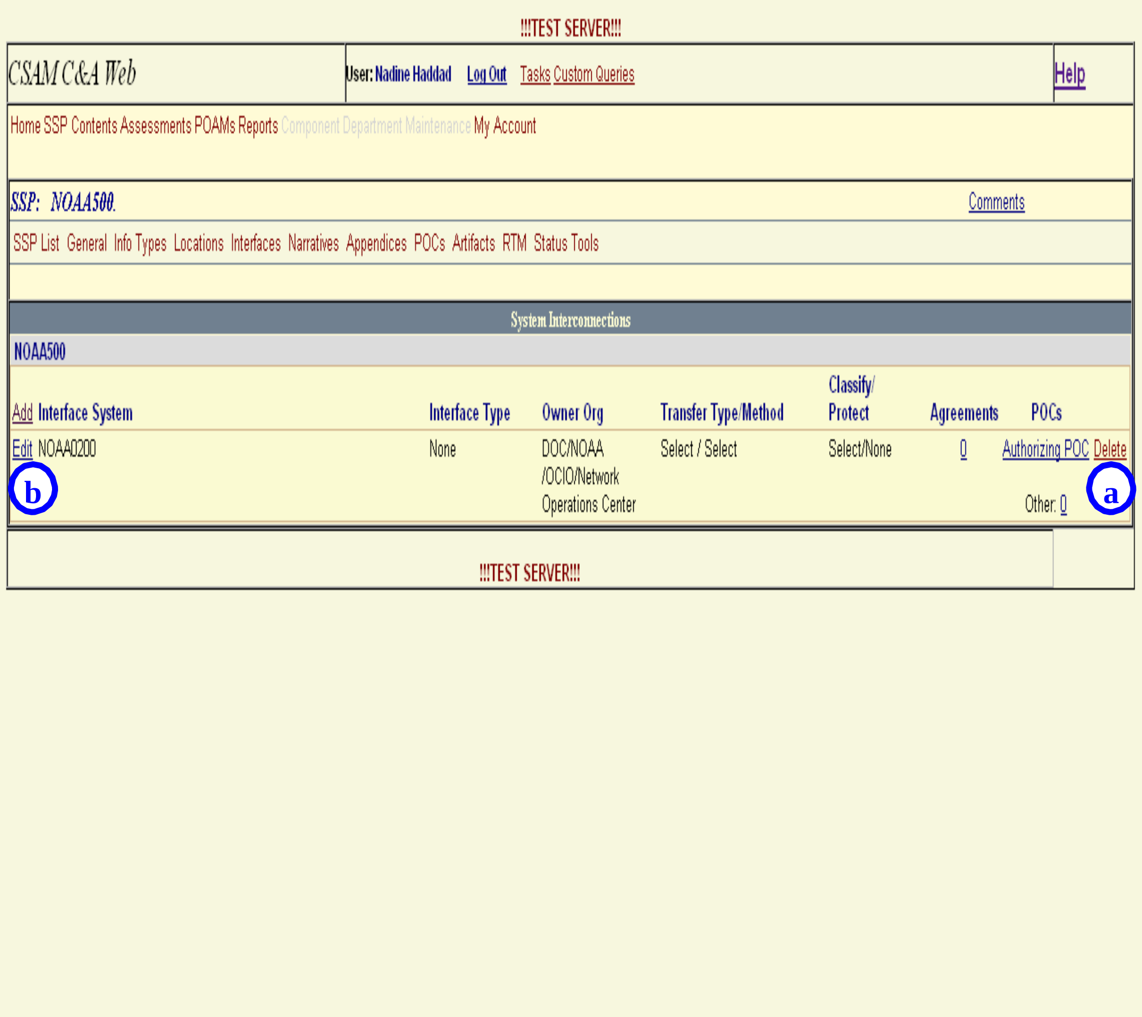
-Enter Name in Box Above or Select from this list-

Owner Org: DOC/NOAA/OCIO/Netw
Interface Type: Select
Transfer Method: Select
Transfer Type: Select
Classification: Select
Protection: Select

Step 7. If a new record is added, it will appear in the System Interconnections list as shown in the figure below.

a. To remove the record, select *Delete*.

b. To modify an existing record, select the *Edit* link that corresponds with that record.


!!!TEST SERVER!!!
CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks Custom Queries
Help
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
SSP: NOAA500.
Comments
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
System Interconnections
NOAA500
b
a
!!!TEST SERVER!!!

Add Interface System	Interface Type	Owner Org	Transfer Type/Method	Classify/ Protect	Agreements	POCs
Edit NOAA0200	None	DOC/NOAA /OCIO/Network Operations Center	Select / Select	Select/None	0	Authorizing POC Delete Other: 0

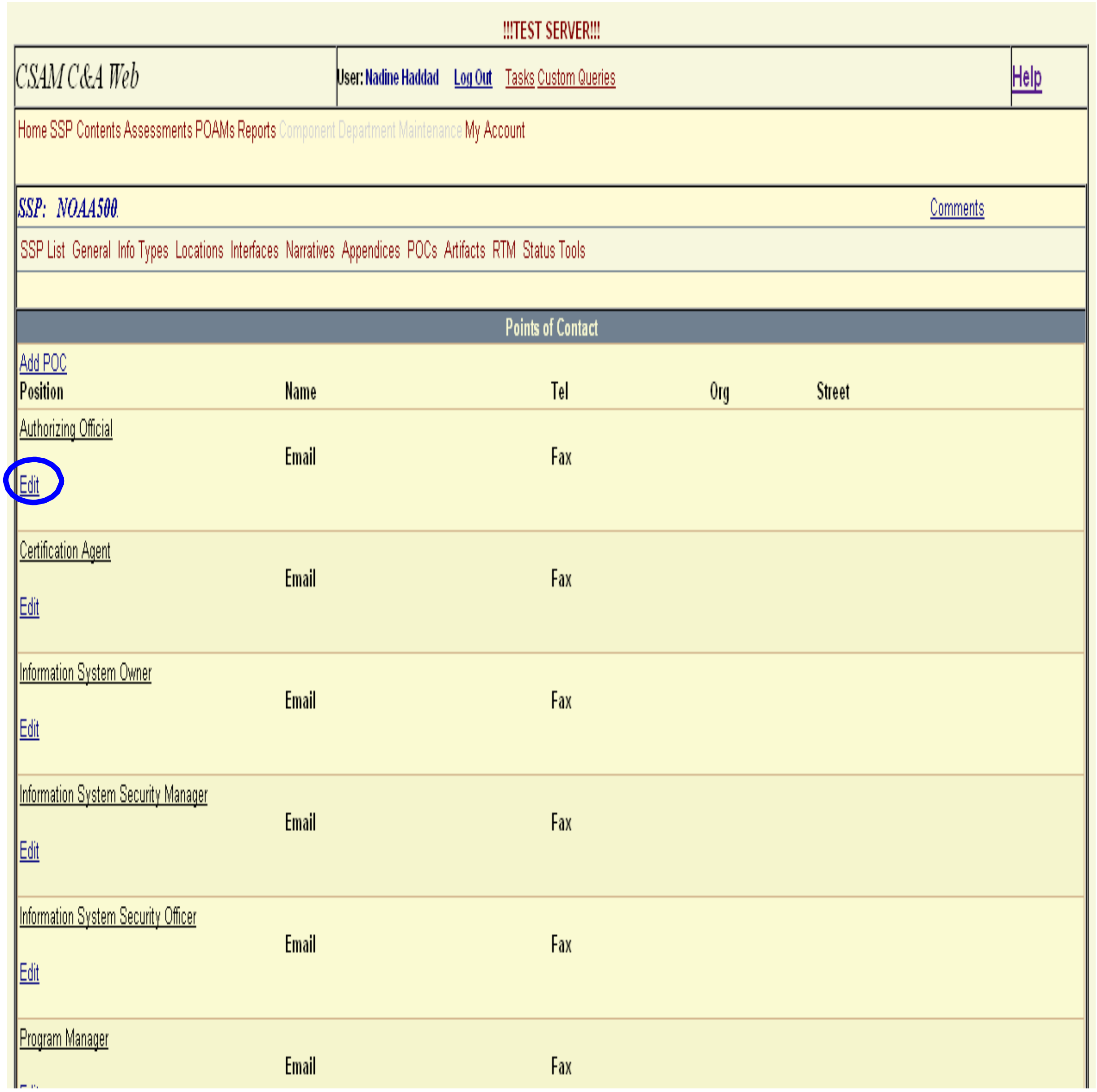
7.3.5 POCs

There are two options to add a POC. One option is to update a predefined role-placeholder. Another is to add a new record.

7.3.5.1 Update a Role-Placeholder

Follow the steps below to update a predefined role-placeholder:

Step 1. Select the corresponding *Edit* link.


!!!TEST SERVER!!!
CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks Custom Queries
Help
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
SSP: NOAA500
Comments
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
Points of Contact
Add POC

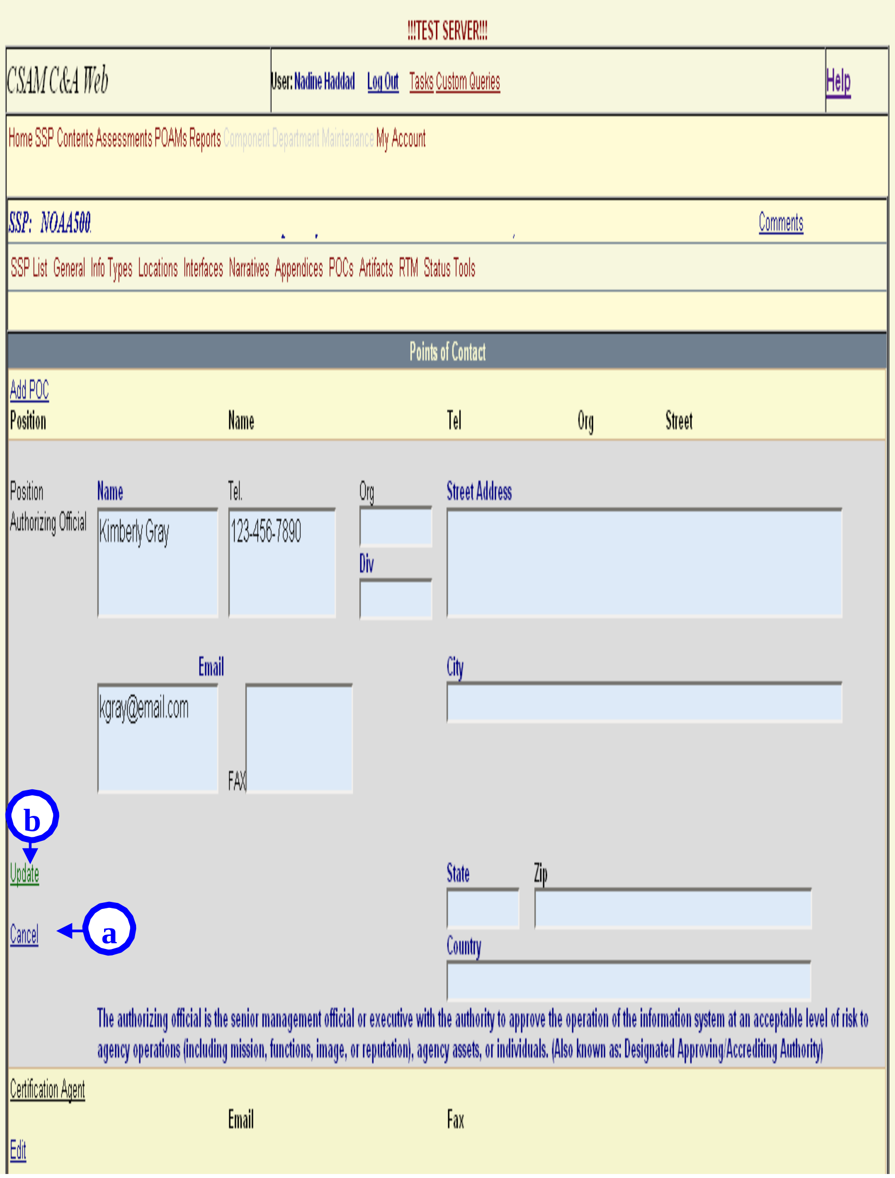
Position	Name	Tel	Org	Street
Authorizing Official Edit	Email	Fax		
Certification Agent Edit	Email	Fax		
Information System Owner Edit	Email	Fax		
Information System Security Manager Edit	Email	Fax		
Information System Security Officer Edit	Email	Fax		
Program Manager	Email	Fax		

Step 2. Enter the contact’s Name, Phone Number, and Email address into the form.

Step 3. Exit with or without saving changes.

a. Select *Cancel* to exit without saving changes.

b. Select *Update* to exit and save changes.



Position: Authorizing Official

Name: Kimberly Gray

Tel.: 123-456-7890

Org:

Div:

Street Address:

Email: kgray@email.com

FAX:

City:

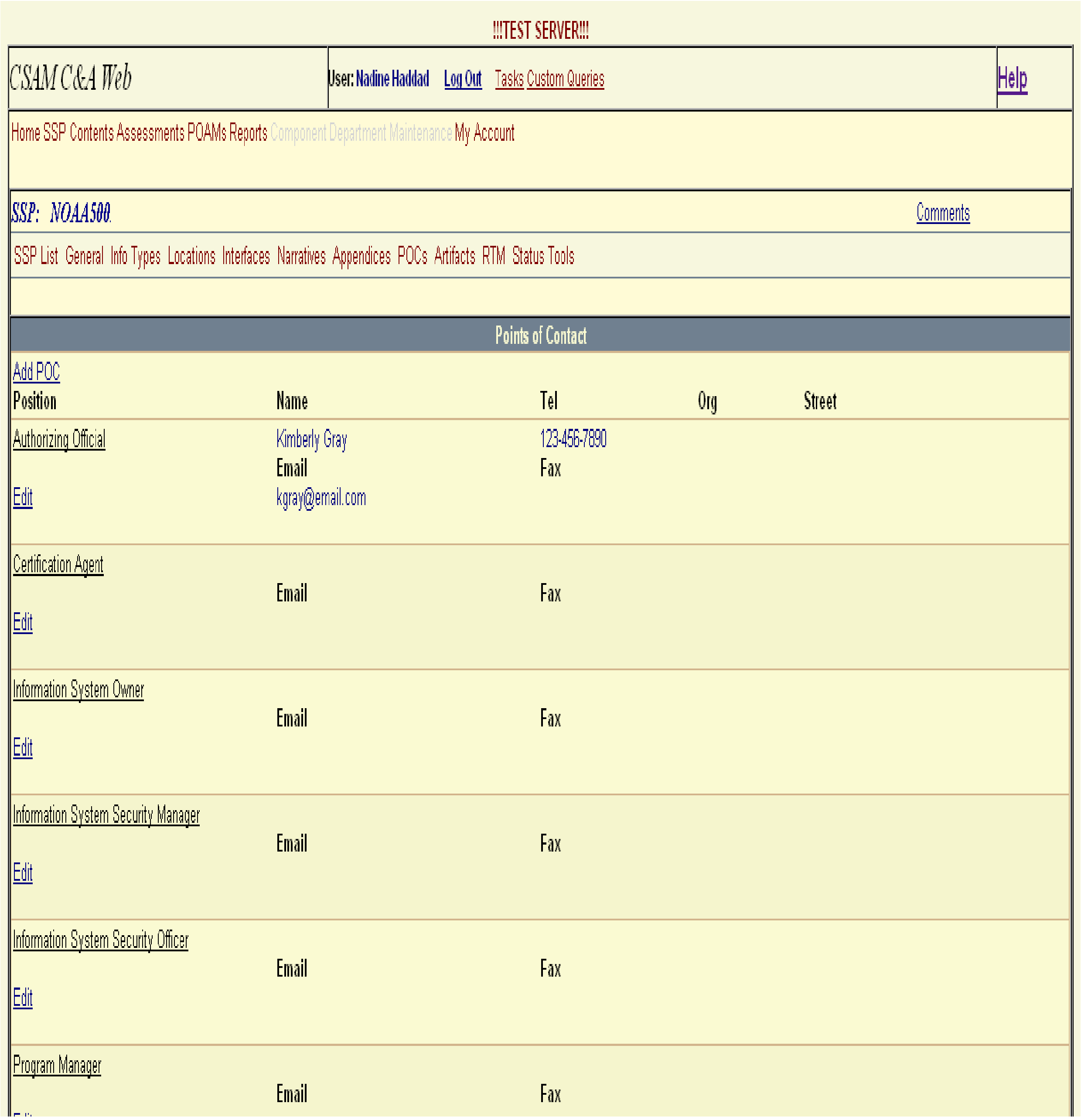
State:

Zip:

Country:

The authorizing official is the senior management official or executive with the authority to approve the operation of the information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. (Also known as: Designated Approving/Accrediting Authority)

Saved changes will appear in the POC list as shown in the figure below.

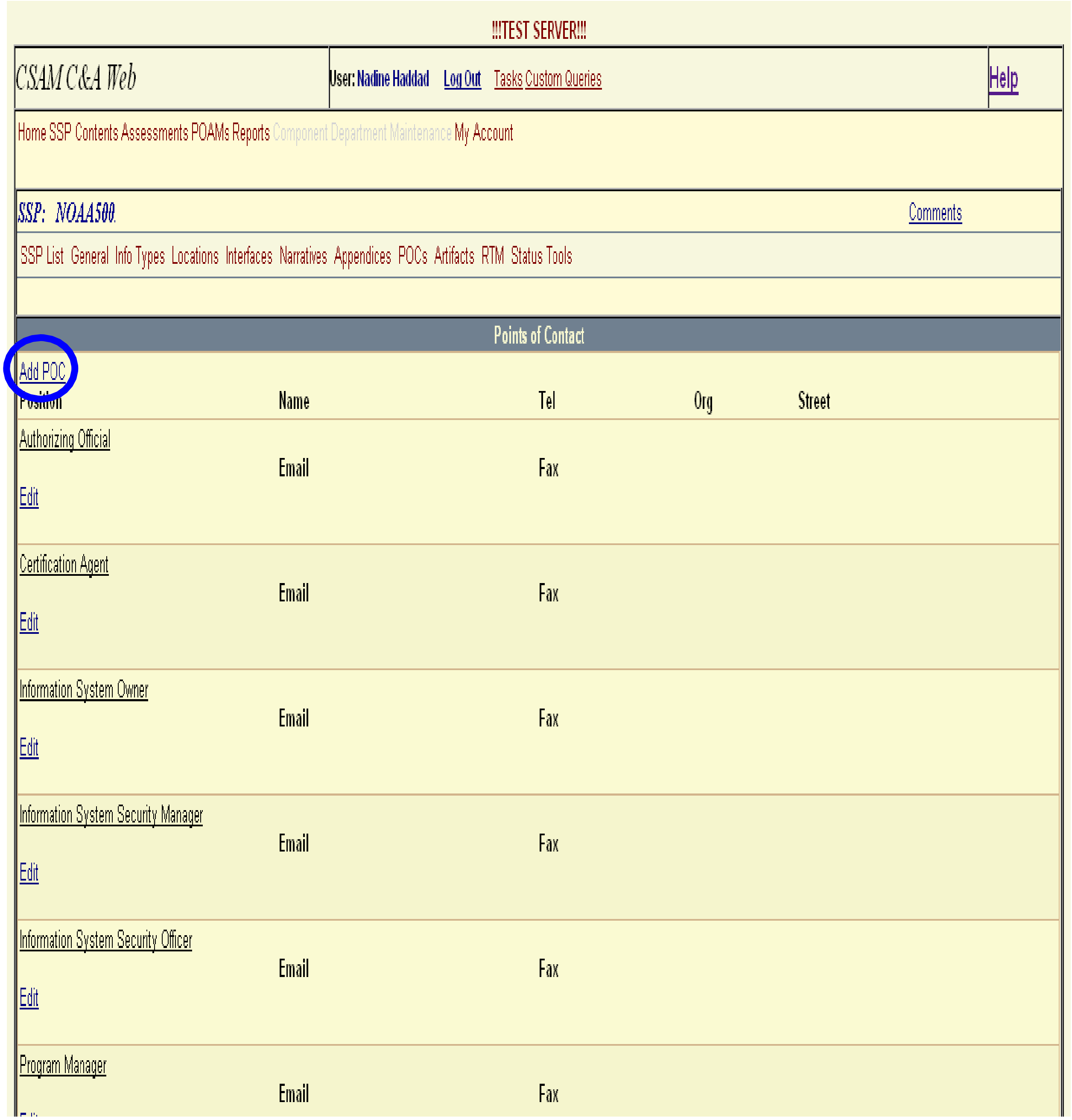

!!!TEST SERVER!!!
CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks Custom Queries
Help
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
SSP: NOAA500
Comments
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
Points of Contact
Add POC

Position	Name	Tel	Org	Street
Authorizing Official	Kimberly Gray	123-456-7890		
	Email	Fax		
Edit	kgray@email.com			
Certification Agent				
	Email	Fax		
Edit				
Information System Owner				
	Email	Fax		
Edit				
Information System Security Manager				
	Email	Fax		
Edit				
Information System Security Officer				
	Email	Fax		
Edit				
Program Manager				
	Email	Fax		

7.3.6 Add a POC Record

Follow the steps below to add a POC record:

Step 1. Select the Add POC link in the top left corner of the screen.


!!!TEST SERVER!!!
CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks Custom Queries
Help
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
SSP: NOAA500
Comments
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
Points of Contact
Add POC

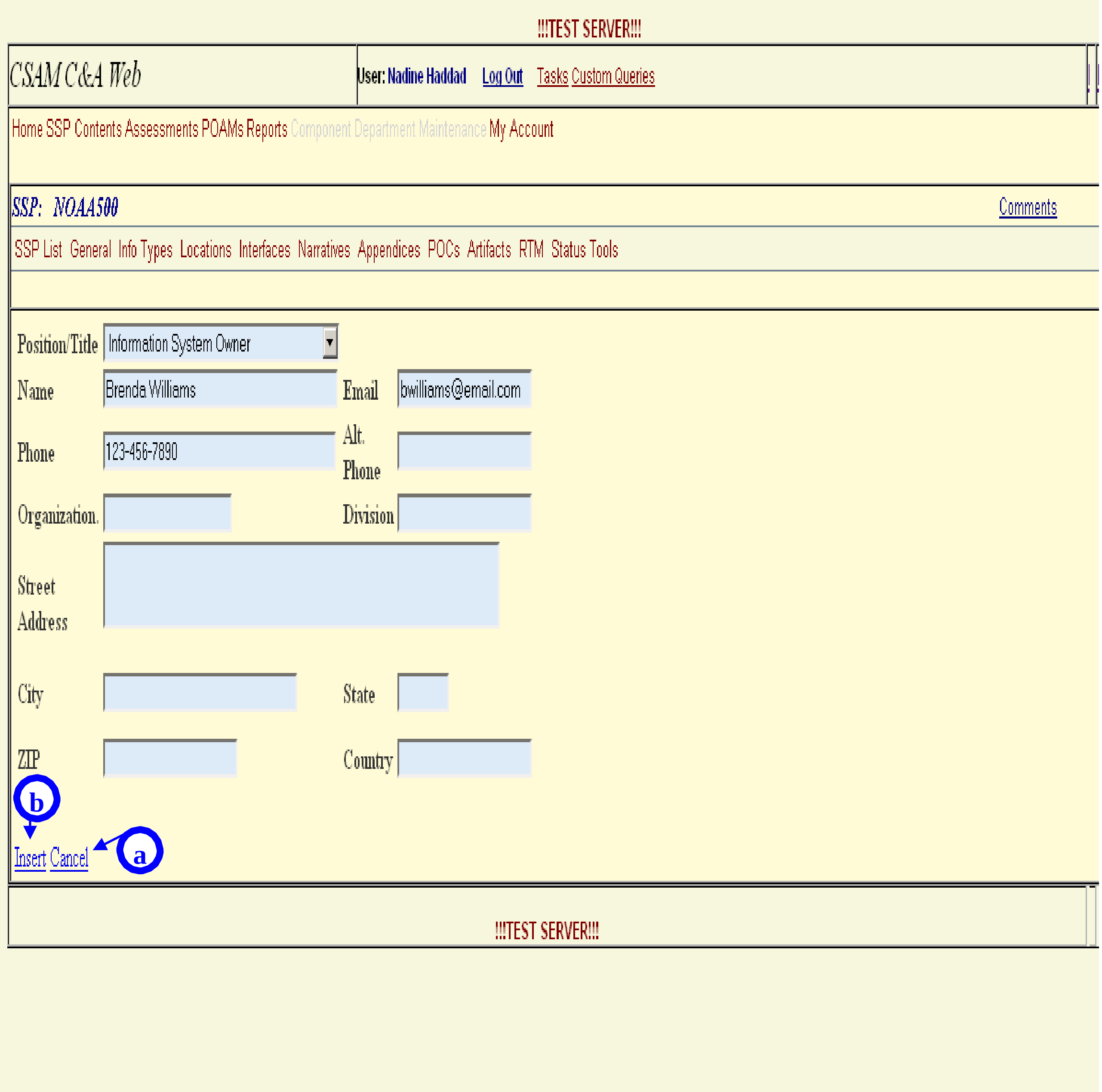
Position	Name	Tel	Org	Street
Authorizing Official Edit	Email	Fax		
Certification Agent Edit	Email	Fax		
Information System Owner Edit	Email	Fax		
Information System Security Manager Edit	Email	Fax		
Information System Security Officer Edit	Email	Fax		
Program Manager	Email	Fax		

Step 2. Enter the contact's Name, Phone Number, and Email address into the form.

Step 3. Exit with or without saving changes.

a. Select *Cancel* to exit without saving changes.

b. Select *Insert* to exit and save changes.



!!!TEST SERVER!!!
CSAM C&A Web
User: Nadine Haddad
Log Out
Tasks
Custom Queries
Home SSP Contents Assessments POAMs Reports Component Department Maintenance My Account
SSP: NOAA500
Comments
SSP List General Info Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools
b
Insert
Cancel
a
!!!TEST SERVER!!!

Position/Title: Information System Owner

Name: Brenda Williams

Email: bwilliams@email.com

Phone: 123-456-7890

Alt. Phone:

Organization:

Division:

Street Address:

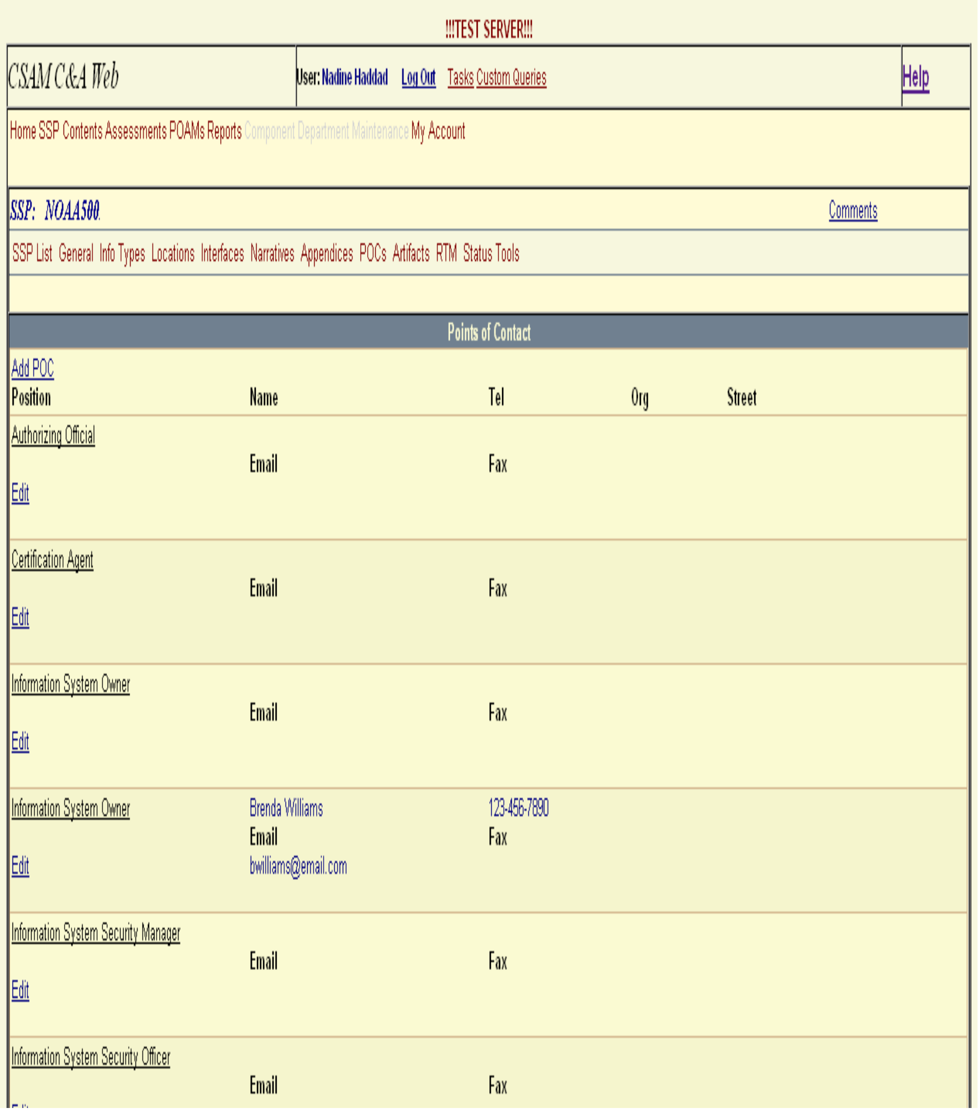
City:

State:

ZIP:

Country:

If a new record is added, it will appear in the POC list as shown in the figure below.



Position	Name	Tel	Org	Street
Authorizing Official Edit	Email	Fax		
Certification Agent Edit	Email	Fax		
Information System Owner Edit	Email	Fax		
Information System Owner Edit	Brenda Williams Email bwilliams@email.com	123-456-7890 Fax		
Information System Security Manager Edit	Email	Fax		
Information System Security Officer	Email	Fax		

To modify an existing record, follow the steps in section 7.3.5.1.

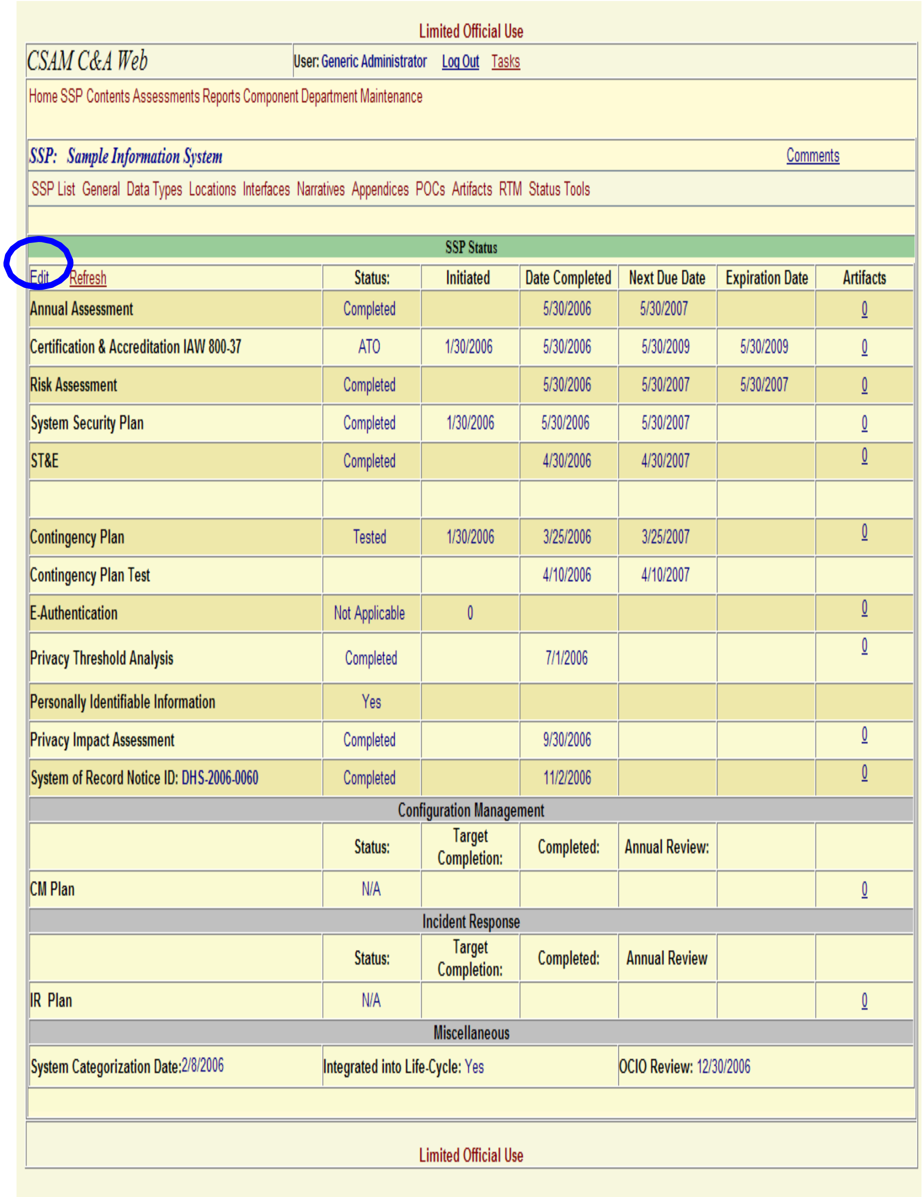
7.3.7 Status

Requirements for updating the Status screen are outlined in

Table 4 CSAM Security Status Update Guide of Appendix B.

Follow the steps below to update the Status screen:

Step 1. Select *Edit* in the top left corner of the Status screen to begin making changes.



Limited Official Use

CSAM C&A Web | User: Generic Administrator | Log Out | Tasks

Home SSP Contents Assessments Reports Component Department Maintenance

SSP: *Sample Information System*

Comments
SSP List General Data Types Locations Interfaces Narratives Appendices POCs Artifacts RTM Status Tools

SSP Status

Edit Refresh	Status:	Initiated	Date Completed	Next Due Date	Expiration Date	Artifacts
Annual Assessment	Completed		5/30/2006	5/30/2007		0
Certification & Accreditation IAW 800-37	ATO	1/30/2006	5/30/2006	5/30/2009	5/30/2009	0
Risk Assessment	Completed		5/30/2006	5/30/2007	5/30/2007	0
System Security Plan	Completed	1/30/2006	5/30/2006	5/30/2007		0
ST&E	Completed		4/30/2006	4/30/2007		0
Contingency Plan	Tested	1/30/2006	3/25/2006	3/25/2007		0
Contingency Plan Test			4/10/2006	4/10/2007		
E-Authentication	Not Applicable	0				0
Privacy Threshold Analysis	Completed		7/1/2006			0
Personally Identifiable Information	Yes					
Privacy Impact Assessment	Completed		9/30/2006			0
System of Record Notice ID: DHS-2006-0060	Completed		11/2/2006			0
Configuration Management						
	Status:	Target Completion:	Completed:	Annual Review:		
CM Plan	N/A					0
Incident Response						
	Status:	Target Completion:	Completed:	Annual Review		
IR Plan	N/A					0
Miscellaneous						
System Categorization Date:2/8/2006	Integrated into Life-Cycle: Yes			OCIO Review: 12/30/2006		

Limited Official Use

Step 2. Perform necessary updates (Requirements for updating the Status screen are outlined Table 4 CSAM Security Status Update Guide in Appendix B).

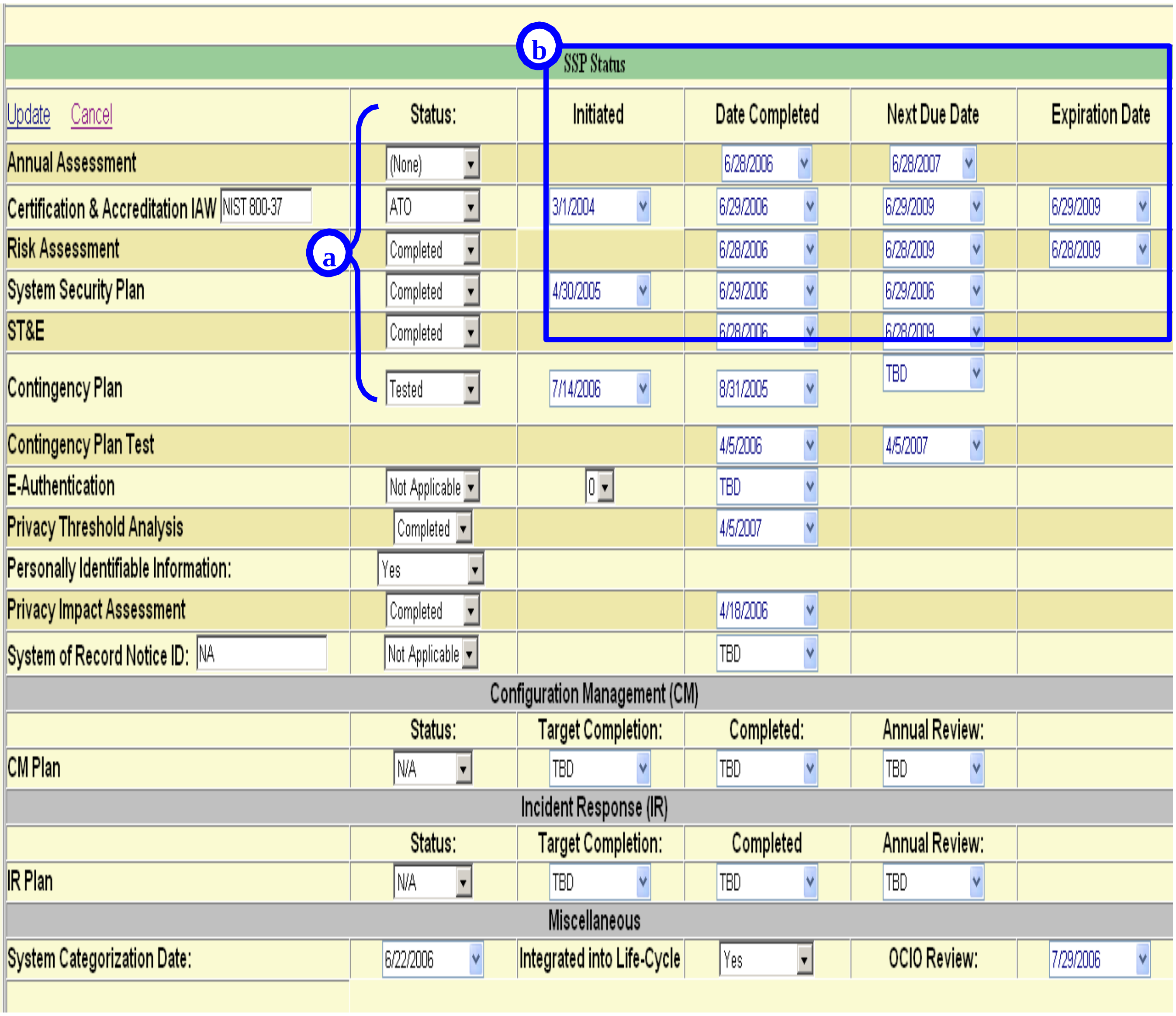
Step 3. Select an option from the drop-down list that corresponds with that security activity to update the Status value of a security activity.

Step 4. Type in or select the date from the calendar drop-down that appears to update the Initiated Date, Date Completed, Next Due Date, and Expiration Date.

Note: If a date-field is left blank or a date is removed, CSAM automatically assigns a value of "TBD."

See the next section (7.3.7.1) for uploading artifacts.

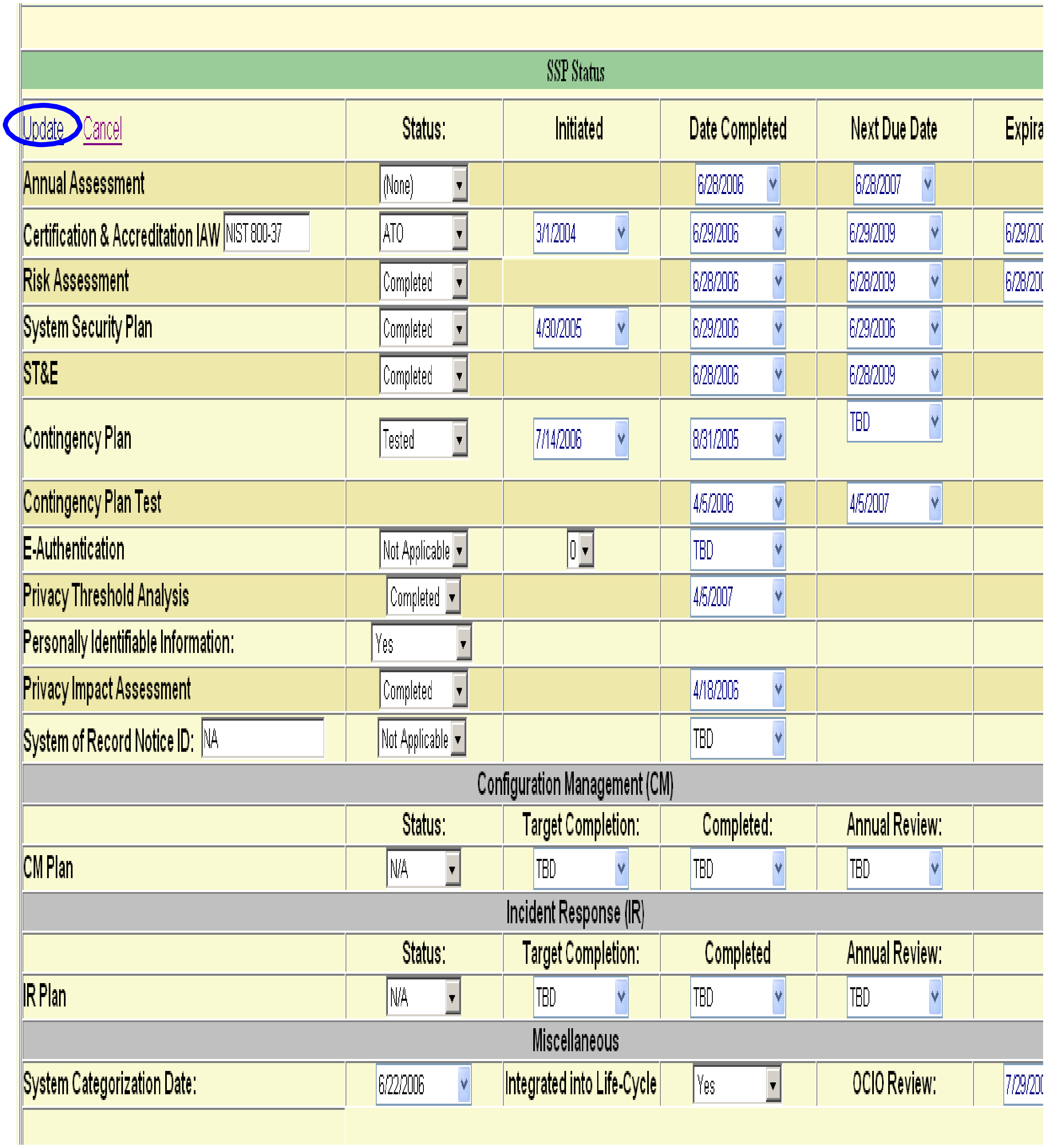
c



SSP Status

Update Cancel	Status:	Initiated	Date Completed	Next Due Date	Expiration Date
Annual Assessment	(None)		6/28/2006	6/28/2007	
Certification & Accreditation IAW NIST 800-37	ATO	3/1/2004	6/29/2006	6/29/2009	6/29/2009
Risk Assessment	Completed		6/28/2006	6/28/2009	6/28/2009
System Security Plan	Completed	4/30/2005	6/29/2006	6/29/2006	
ST&E	Completed		6/28/2006	6/28/2009	
Contingency Plan	Tested	7/14/2006	8/31/2005	TBD	
Contingency Plan Test			4/5/2006	4/5/2007	
E-Authentication	Not Applicable	0	TBD		
Privacy Threshold Analysis	Completed		4/5/2007		
Personally Identifiable Information:	Yes				
Privacy Impact Assessment	Completed		4/18/2006		
System of Record Notice ID: NA	Not Applicable		TBD		
Configuration Management (CM)					
	Status:	Target Completion:	Completed:	Annual Review:	
CM Plan	N/A	TBD	TBD	TBD	
Incident Response (IR)					
	Status:	Target Completion:	Completed	Annual Review:	
IR Plan	N/A	TBD	TBD	TBD	
Miscellaneous					
System Categorization Date:	6/22/2006	Integrated into Life-Cycle	Yes	OCIO Review:	7/29/2006

After making the necessary changes, select the *Update* link at the top left corner of the form.



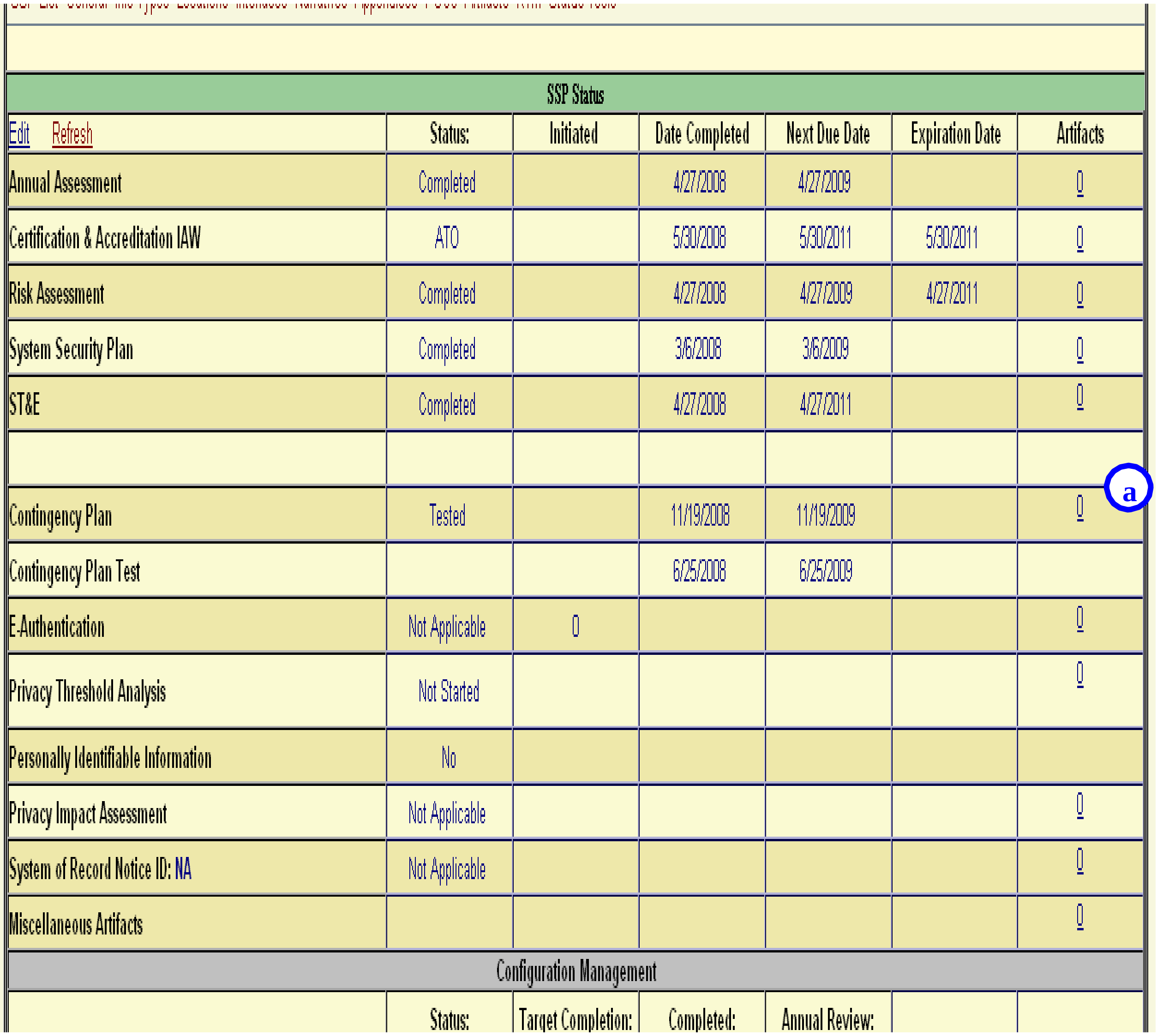
SSP Status

Update Cancel	Status:	Initiated	Date Completed	Next Due Date	Expira
Annual Assessment	(None)		6/28/2006	6/28/2007	
Certification & Accreditation IAW NIST 800-37	ATO	3/1/2004	6/29/2006	6/29/2009	6/29/20
Risk Assessment	Completed		6/28/2006	6/28/2009	6/28/20
System Security Plan	Completed	4/30/2005	6/29/2006	6/29/2006	
ST&E	Completed		6/28/2006	6/28/2009	
Contingency Plan	Tested	7/14/2006	8/31/2005	TBD	
Contingency Plan Test			4/5/2006	4/5/2007	
E-Authentication	Not Applicable	0	TBD		
Privacy Threshold Analysis	Completed		4/5/2007		
Personally Identifiable Information:	Yes				
Privacy Impact Assessment	Completed		4/18/2006		
System of Record Notice ID: NA	Not Applicable		TBD		
Configuration Management (CM)					
	Status:	Target Completion:	Completed:	Annual Review:	
CM Plan	N/A	TBD	TBD	TBD	
Incident Response (IR)					
	Status:	Target Completion:	Completed	Annual Review:	
IR Plan	N/A	TBD	TBD	TBD	
Miscellaneous					
System Categorization Date:	6/22/2006	Integrated into Life-Cycle	Yes	OCIO Review:	7/29/20

7.3.7.1 Upload Artifacts

Please note that one must have the Artifact Uploader role to upload FISMA Inventory artifacts. See the supplementary document *Getting Started with the Cyber Security Assessment and Management (CSAM) Tool* for a discussion of CSAM roles.

Step 1. Select the *Artifacts* link associated with security activity. For example, to upload the latest version of the Contingency Plan to this area, first select the associated Artifacts link ("a" in the figure below).



SSP Status

Edit Refresh	Status:	Initiated	Date Completed	Next Due Date	Expiration Date	Artifacts
Annual Assessment	Completed		4/27/2008	4/27/2009		0
Certification & Accreditation IAW	ATO		5/30/2008	5/30/2011	5/30/2011	0
Risk Assessment	Completed		4/27/2008	4/27/2009	4/27/2011	0
System Security Plan	Completed		3/6/2008	3/6/2009		0
ST&E	Completed		4/27/2008	4/27/2011		0
Contingency Plan	Tested		11/19/2008	11/19/2009		0
Contingency Plan Test			6/25/2008	6/25/2009		
E-Authentication	Not Applicable	0				0
Privacy Threshold Analysis	Not Started					0
Personally Identifiable Information	No					
Privacy Impact Assessment	Not Applicable					0
System of Record Notice ID: NA	Not Applicable					0
Miscellaneous Artifacts						0

Configuration Management

	Status:	Target Completion:	Completed:	Annual Review:		

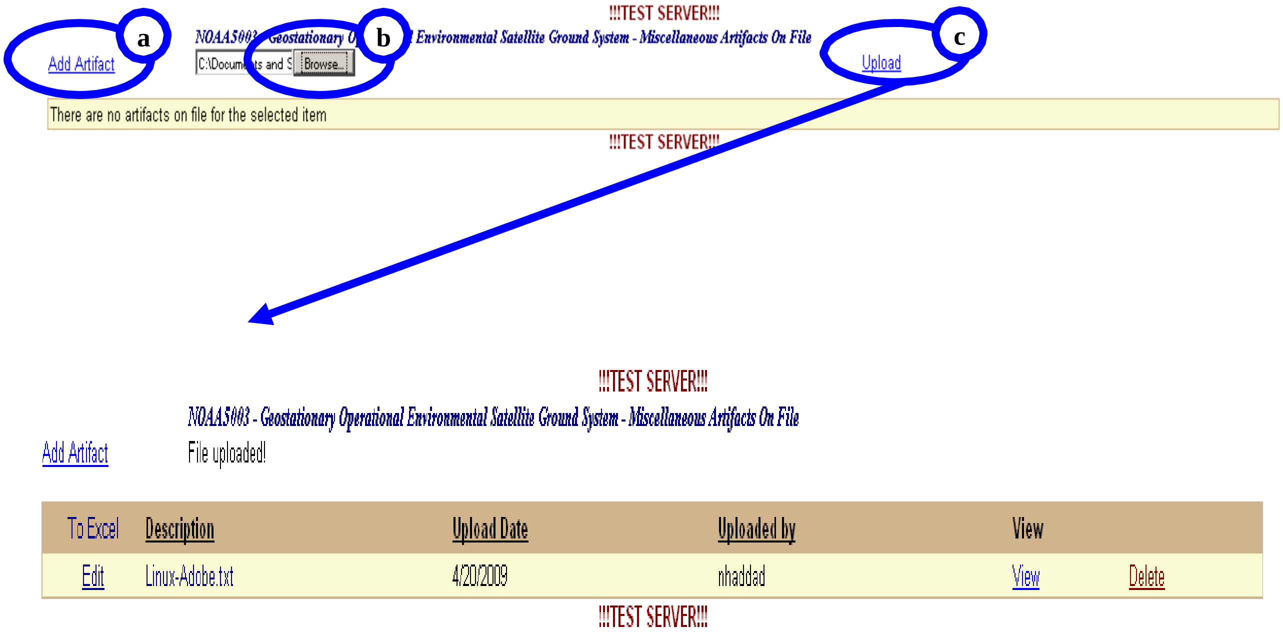
Step 2. Depending on the browser, either a new tab or window will appear. In the new tab/window, select the *Add Artifact* link.

Step 3. In the file field that appears, select the *Browse* button. A "File Upload" dialogue box will appear.

Step 4. Locate the artifact you would like to upload and select *Open*.

Step 5. Select the *Upload* link. The file will now be listed on the current page.

Step 6. Close the tab/window.



!!!TEST SERVER!!!

NOAA5003 - Geostationary O... Environmental Satellite Ground System - Miscellaneous Artifacts On File

There are no artifacts on file for the selected item

!!!TEST SERVER!!!

!!!TEST SERVER!!!

NOAA5003 - Geostationary Operational Environmental Satellite Ground System - Miscellaneous Artifacts On File

Add Artifact

File uploaded!

To Excel	Description	Upload Date	Uploaded by	View	
Edit	Linux-Adobe.txt	4/20/2009	nhaddad	View	Delete

!!!TEST SERVER!!!

7.4 NESDIS CID Review

NESDIS CID will perform a quality review of FISMA Inventory data contained in CSAM. The review will occur quarterly. A review schedule is contained in Table 2 below. The NESDIS CID will inform the SO via email of any FISMA inventory data modifications that occur as a result of the review. If the NESDIS CID requests changes, the SO, or authorized delegate, will have three business days to perform the necessary updates and notify the NESDIS CID via email at nesdis.hq.secteam@noaa.gov of completion. The NESDIS CID will perform a follow-up review and request changes if necessary.

Table 2 NESDIS CID FISMA Inventory Review Schedule

FY Quarter	NESDIS CID quality review begins on or after the 16th (or next business day)
1	November
2	February
3	May
4	August

Appendix A

Table 3 CSAM FISMA Inventory Data Requirements

Screen	Field	Requirements/Guidance	Systems in Development
General	SSP Name	This is the name of your system. The name should be in the format FISMA ID + System Name. Example: NOAA50XX is the FISMA ID, and Data Communications is the name = "NOAA50XX – Data Communications".	Required
General	Alternate ID	Insert only the number portion of your FISAM ID into this field. Using the example above, we'd insert '50XX'. Please use 4 digits for the ID. (ex: 5001, 5300, 5303, 5311).	Required
General	Address for "Responsible Organization"	Please populate the "Address", "City", "State", "Zip Code", and "Country" fields. The organization responsible for the system should be used. This may not necessarily be the location where the actual system resides.	Required
General	System Mission/Purpose	Executive level description of your system's purpose. Narrative must be kept between 75 and 150 words. Minimize technical jargon. Imagine the DOC CIO using this narrative to gain an understanding of your system's role within DOC.	Required
General	System Type	Choices are "General Support System" or "Major Application."	Required
General	Operational Status	Choices are "Development", "Implementation", "Operational" and "Retired".	Required
General	Financial System	Choices are "Non-Financial", "Financial", or "Financial Mixed".	Required
General	Contractor System	Box checked for "Yes" and Unchecked for "No".	Required
General	UPI Code	This is the OMB-300/53 exhibit code which can be obtained from your	Required

Screen	Field	Requirements/Guidance	Systems in Development
		eCpic representative if needed.	
General	Investment Name	This is the Investment name from the system's OMB-300/53 entry, which can be obtained from your eCpic representative if needed.	Required
Info Types	Information Type(s)	Should match those identified in the documented FIPS 199 categorization. Justification must be provided for deviating from the recommended impact levels.	Required only if available.
Info Types	Classification	Choices: -Unclassified -SBU = Sensitive-but-unclassified non-national security (private data, Sensitive/Limited Official Use -Confidential -Secret -Top Secret -SCI = Sensitive Compartmented Information	Required only if available.
Locations	Location Name	Name of the system's physical location.	Required only if available.
Locations	Address	The system's physical location including building and room number, city, state, zip code, and country.	Required only if available.
Interfaces	Interface System	The system identification number or name (if the system is not a DOC system) of the interconnected system – for example, a DOC system is identified by the system ID assigned by the owning operating unit's CIO; an external system may have a specific name such as the Civil Applicant System; or general connections to the Internet would have no specific name but would state "Internet."	Required only if available.
Interfaces	Owner Org	The name of the entity/organization to which your system is connected – for example, Department of Justice (DOJ), National Finance Center (NFC), DOC/National Oceanic and	Required only if available.

Screen	Field	Requirements/Guidance	Systems in Development
		Atmospheric Administration (DOC/NOAA), or the Internet Service Provider business partner. Spell out all acronyms. For DOC operating units, be as specific as possible and include the line or program office title if known.	
Interfaces	Agreements	Upload agreements for connections external to the organization only.	Required only if available.
POCs	Name	A POC record should be in-place for the AO, SO and ISSO of the system. Name, Email and Telephone number at minimum should be defined for each role.	Required only if available.
Status	All fields	See Table 4 CSAM Security Status Update Guide in Appendix B.	The Next Due Date" field for Certification & Accreditation is required and all other information is required only if available.

Appendix B

The following table outlines the update schedule for each security activity listed in the CSAM Status screen. Some fields must be updated at the start of a security activity, at completion, or when the due date has expired. If an item must be updated based on the status of another security activity, identify that relationship in **bold text.** In addition, the structure of the table aligns visually with the placement of the fields in the CSAM Status screen.

Table 4 CSAM Security Status Update Guide

▲ Start ▼ Finish ◀ Expiration

Activity	CSAM Fields (Type)						
	Status (Selection)		Initiated (Date)	Date Completed	Next Due Date	Expiration Date	Artifacts (link to upload)
Annual Assessment/ Continuous Monitoring	Options: -(None) -Not Applicable -Not Started -In Progress -Completed -Expired	*Update*:* ▲ *at the start of the annual assessment.* ▼ *upon completion of the annual assessment.* ◀ *if annual assessment completion is overdue and expiration date has been reached.* **Also update **ST&E Status** with this status.*	*No update required.*	▼ *Update upon completion of annual assessment, also update **ST&E Date Completed** with this date.*	▼ *Update upon completion of annual assessment. Next due date is the one year anniversary of annual assessment completion date. Also update **ST&E Next Due Date** with this date.*	*No update required.*	▼ *Upload annual assessment report, all associated artifacts and any supporting documentation.*

Activity	**CSAM Fields (Type)**						
	Status (Selection)		**Initiated (Date)**	**Date Completed**	**Next Due Date**	**Expiration Date**	**Artifacts (link to upload)**
Assessment & Authorization (A&A)	Options: -Not Started -In Progress -IATO -ATO -Expired -Not Applicable -None	*Update:* ▲ *at the start of A&A effort.* ▼ *upon receipt of signed accreditation decision letter.* ◀ *if accreditation completion is overdue and expiration date has been reached.*	▲ *Update at the start of A&A effort.*	▼ *Update upon receipt of the signed ATO letter. Use the date of the signed ATO letter Also update the following with this date:* ***ST&E Date Completed, Annual Assessment Date Completed.***	▼ *Update upon receipt of the signed ATO letter. The signed ATO letter will specify the accreditation duration. Also update the follow~~ing wi~~th the 1 year anniversary of A&A Completion:* ***ST&E Next Due Date, Annual Assessment Next Due Date.***	▼ *Update upon receipt of the signed ATO letter. The signed ATO letter will specify the accreditation duration.*	▼ *Upload the signed accreditation decision letter (Letter may specify ATO, IATO, or DATO).*
Risk Assessment (RA)	Options: -Not Started -In Progress -Completed -Expired -Not Applicable	*Update:* ▲ *at start of Risk Assessment effort.* ▼ *upon completion of risk assessment.*	*No update required.*	▼ *Update upon completion of risk assessment.*	▼ *Update upon completion of risk assessment. Next due date is the one year anniversary of risk assessment completion date.*	▼ *Update upon completion of risk assessment. Next due date is the one year anniversary of risk assessment completion date.*	▼ *Upload final risk assessment and any supporting documentation.*

Activity	CSAM Fields (Type)						
	Status (Selection)		Initiated (Date)	Date Completed	Next Due Date	Expiration Date	Artifacts (link to upload)
System Security Plan (SSP)	Options: -Not Started -In Progress -Completed -Not Applicable	*Update:* ▲ *at the start SSP of development/ update effort.* ▼ *upon receipt of signed SSP.*	▲ *Update at the start of SSP development/ update effort.*	▼ *Update upon receipt of signed SSP.*	▼ *Update upon receipt of signed SSP. Next due date is the one year anniversary of signed/approved SSP.*	*No update required.*	▼ *Upload signed SSP and any supporting documentation.*
Security Test & Evaluation (ST&E)	Options: -Not Started -In Progress -Completed -Expired -Not Applicable	*Update*:* ▲ *at start of ST&E effort.* ▼ *upon completion of controls testing.* **Also update **Annual Assessment Status** with this status.*	*Not required*	▼ *Update upon completion of ST&E controls testing. Also update **Annual Assessment Date Completed** with this date.*	▼ *Update upon completion of ST&E controls testing. Also update **Annual Assessment Next Due Date** with this date.*	*Not required*	▼ *Upload final ST&E Report and any supporting documentation.*

Activity	CSAM Fields (Type)						
	Status (Selection)		Initiated (Date)	Date Completed	Next Due Date	Expiration Date	Artifacts (link to upload)
Contingency Plan (CP)	Options: -Not Started -In Progress -Completed -Tested -Expired (Plan) -Expired (Test) -Expired (Both) -Not Applicable	*Update:* ▲ *at start of CP development/ update effort.* ▼ *upon receipt of signed CP.* ▼ *upon completion of* ***CP test.*** ◀ *if CP completion is overdue and expiration date has been reached.* ◀ *if* ***CP test*** *completion is overdue and expiration date has been reached.*	▲ *Update at start of CP development/ update effort.*	▼ *Update upon receipt of signed CP.*	▼ *Update upon receipt of signed CP. Next due date is the one year anniversary of signed/approved CP.*	*Not required*	▼ *Upload signed CP and any supporting documentation.*
Contingency Plan (CP) Test	*No status field is provided for the CP Test. However, the status of the CP test must be recorded in the status field associated with the* ***Contingency Plan*** *(above).*		*Not required*	▼ *Update upon completion of contingency test.*	▼ *Update upon completion of contingency test. Next due date is the one year anniversary of contingency plan test completion date.*	*Not required*	▼ *Upload contingency plan test results and any supporting documentation.*
E-Authentication Risk Assessment (ERA)	Options: -Not Applicable -Not Started -In Progress -Completed	*Update:* ▲ *at the start of the ERA effort.* ▼ *upon completion of ERA.* ◀ *if ERA completion is overdue and expiration date has been reached.*	▲ *Update at the start of ERA effort.*	▼ *Update upon completion of ERA.*	▼ *Update upon completion of ERA.*	*Not required*	▼ *Upload ERA and supporting documentation.*

Activity	CSAM Fields (Type)						
	Status (Selection)		Initiated (Date)	Date Completed	Next Due Date	Expiration Date	Artifacts (link to upload)
Privacy Threshold Analysis (PTA)	Options: -Not Started -In Progress -Completed	*Update:* ▲ *at the start of the PTA effort.* ▼ *upon receipt of signed PTA.* *Also, **PII Status, SORN Status** and **PIA Status** depend on results of the PTA (**See PII, PIA and SORN**).*	*Not required*	▼ *Update upon receipt of signed PTA.*	*Not required*	*Not required*	▼ *Upload signed PTA and any supporting documentation.*
Personally Identifiable Information (PII)	Options: -No -Yes -HR -Legacy -National Security	▼ ***PTA**: Update based on results of **PTA**.*	*Not required*	*Not required*	*Not required*	*Not required*	*Not required*
Privacy Impact Assessment (PIA)	Options: -Not Applicable -Not Started -In Progress -Completed	*Update:* ▼ *based on results of **PTA**. If PII does not exist PIA Status is "Not Applicable".* ▲ *at the start of the PIA effort (if applicable).* ▼ *upon completion of PIA (if applicable).* *Also, **SORN Status** depends on results of the PIA (**See SORN**).*	*Not required.*	▼ *If applicable, update upon completion of PIA. If not applicable, leave blank.*	*Not required*	*Not required*	▼ *If applicable, upload signed PIA containing the internet link to the PIA and any supporting documentation.*
System of Record Notice (SORN)	Options: -Not Applicable -Not Started -In Progress -Completed	*Update:* ▼ *based on results of **PTA**. If PII does not exist SORN Status is "Not Applicable"* ▼ *based on results of **PIA**. SORN may or may not be require. If SORN is not required, SORN Status is "Not Applicable."*	*Not required*	▼ *If applicable, update upon completion of SORN. If not applicable*	*Not required*	*Not required*	▼ *If applicable, upload text file containing the internet link to SORN and any supporting documentation.*

Activity	CSAM Fields (Type)					
	Status (Selection)	**Initiated (Date)**	**Date Completed**	**Next Due Date**	**Expiration Date**	**Artifacts (link to upload)**
	▲ *at the start of the SORN effort (if applicable).* ▼ *upon completion of SORN (if applicable).*		*leave blank.*			

Appendix C

The following table identifies the relationship between security related activities and the OMB Exhibit 300 process. It also includes references for locating security related information necessary for that process.

Table 5 Reference for OMB Exhibit 300s - Security and Privacy Tables

Security Related Activity/Information	OMB Exhibit 300		Answer/Reference
	Section/Sub-Section	Question/Field	
New or Planned System	Security and Privacy/ Security: Planned Systems	Agency/ or Contractor Operated System?	CSAM Location: General Screen/System Attributes/Contractor System (Checked means "Yes", Unchecked means "No").
		Planned Operational Date	
		Date of Planned A&A Update (for existing mixed life cycle systems) or Planned Completion Date (for new systems).	CSAM Location: Status Screen/Certification & Accreditation IAW/Next Due Date.
FIPS 199 Assessment	Security and Privacy/ Security: Operational Systems	NIST FIPS 199 Risk Impact Level.	CSAM Location: General Screen/System Attributes/System Category.
Security Test and Evaluation (ST&E) OR Annual Assessment/Continuous Monitoring	Security and Privacy/ Security: Operational Systems	What standards were used for Security Controls tests?	FIPS 200/NIST 800-53
		Date completed Security Control Testing.	This is either the ST&E or Annual Assessment date recorded in CSAM, whichever occurred is more recently. CSAM Location: Status Screen/ST&E/Date Completed and Status Screen/Annual Assessment/Date Completed.
ATO	Security and Privacy/ Security: Operational Systems	Has C&A been completed, using NIST 800-37?	Yes
		Date Completed C&A.	CSAM Location: Status Screen/Certification & Accreditation IAW/Date Completed.
Contingency Plan Test	Security and Privacy/ Security: Operational Systems	Date contingency plan tested.	CSAM Location: Status Screen/Contingency Plan Test/Date Completed.
Privacy threshold	Security and Privacy/	Is this a new system?	

Security Related Activity/Information	OMB Exhibit 300		Answer/Reference
	Section/Sub-Section	Question/Field	
analysis (PTA) and the following if they apply: Privacy Impact Assessment (PIA) & System of Records. Notice (SORN)	Privacy: Planned & Operational Systems	Is there at least one Privacy Impact Assessment (PIA) that covers this system?	CSAM Location: Status Screen/Personally Identifiable Information/Status & Date Completed (if applicable).
		Internet link or explanation	If applicable, link may be found at the following CSAM location: Status Screen/Personally Identifiable Information/Artifacts. If PIA is required but not completed then state "The Draft PIA is under review at DOC." If no PIA is required then state "This system does not contain or process PII".
		Is a System of Records Notice (SORN) required for this system?	CSAM: Status Screen/System of Record Notice/Status & Date Completed (if applicable).
		Internet link or explanation	If applicable, link may be found at the following CSAM location: Status Screen/System of Record Notice/Artifacts. If SORN is required but not completed state that "SORN currently under review." If no SORN is required and no PII is on the system then state "No because there is no PII and the system is not a Privacy Act system of records." If no SORN is required but PII exists on the system then state "No because the system is not a Privacy Act system of records."

Approval Page

Document Number: NQP-3407, Revision 2.1	
Document Title Block: **NESDIS FISMA Inventory Management Policy and Procedures**	
Process Owner: NESDIS Chief Information Division	Document Release Date: September 28, 2012

Prepared by:

Erica Boyd

Erica Boyd
Ambit- Associate Consultant
NESDIS Chief Information Office

3/26/15
Date:

Approved by:

Irene Parker

Irene Parker
Assistant Chief Information Officer - Satellites

3/26/15
Date:

Document Change Record

VERSION	DATE	CCR #	SECTIONS AFFECTED	DESCRIPTION
01	**March 26, 2015**	**----**	**ALL**	**Baseline NQP-3407**