

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES
1 5

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

BPA NO. DR-09-06-131

1. DATE OF ORDER SEP 11 2007	2. CONTRACT NO. (if any) GS35F01255	6. SHIP TO:	
3. ORDER NO. 010	4. REQUISITION/REFERENCE NO. CFO-06-131	a. NAME OF CONSIGNEE U.S. Nuclear Regulatory Commission	
5. ISSUING OFFICE (Address correspondence to) U.S. Nuclear Regulatory Commission Div. of Contracts Attn: Adelis M Rodriguez, 301-415-5719 Mail Stop T-7-I-2 Washington, DC 20555		b. STREET ADDRESS Attn: Caroline Zabrocky Mail Stop: T9 C4	
7. TO:		c. CITY Washington	d. STATE DC
a. NAME OF CONTRACTOR AEGIS.NET INC		e. ZIP CODE 20555	
b. COMPANY NAME		f. SHIP VIA	
c. STREET ADDRESS 1616 ANDERSON RD		8. TYPE OF ORDER	
d. CITY MC LEAN	e. STATE VA	f. ZIP CODE 221021602	<input type="checkbox"/> a. PURCHASE <input checked="" type="checkbox"/> b. DELIVERY
9. ACCOUNTING AND APPROPRIATION DATA B&R: 77N-15-5H1-357 Job: N7242 BOC: 252A Approp.: 31X0200 Obligate: \$52,000.00 PFS: RQCFO-07-369 DUNS: 152858358		10. REQUISITIONING OFFICE CFO	

11. BUSINESS CLASSIFICATION (Check appropriate box(es))				12. F.O.B. POINT N/A
<input checked="" type="checkbox"/> a. SMALL	<input type="checkbox"/> b. OTHER THAN SMALL	<input type="checkbox"/> c. DISADVANTAGED	<input type="checkbox"/> g. SERVICE-DISABLED VETERAN-OWNED	
<input type="checkbox"/> d. WOMEN-OWNED	<input type="checkbox"/> e. HUBZone	<input type="checkbox"/> f. EMERGING SMALLBUSINESS		
13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)	16. DISCOUNT TERMS
a. INSPECTION destination	b. ACCEPTANCE destination			

17. SCHEDULE (See reverse for Rejections)

ITEM NO (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Aegis.net will provide IV&V services according to the requirements provided in the attached statement of work. The labor rates applicable are the ones agreed under the BPA DR-09-06-131, the estimated hours are according to your price proposal dated August 30, 2007 for Task order No. 010.					
001	Functional Expert - year 1				\$1,895.28	
002	Iv&V Technical Specialist - year 1				\$6,064.80	
003	Functional Expert - year 2				\$20,721.92	
004	Iv&V Technical Specialist - year 2				\$89,708.50	
005	Functional Expert - year 3				\$1,659.30	
	Iv&V Technical Specialist - year 3 Total Obligated Amount: \$52,000.00 Total Order Ceiling: not to exceed \$130,669.80 Period of Performance: 15 months from award.				\$10,620.00	

SEE BILLING INSTRUCTIONS ON REVERSE	18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.		17(h) TOTAL (Cont. pages) 17(i) GRAND TOTAL
	21. MAIL INVOICE TO:				
	a. NAME U.S. Nuclear Regulatory Commission Payment Team, Mail Stop T-7-I-2				
	b. STREET ADDRESS (or P.O. Box) Attn: DR-09-06-131 TO 10				
	c. CITY Washington	d. STATE DC	e. ZIP CODE 20555	\$52,000.00	

22. UNITED STATES OF AMERICA
BY (Signature)

Stephen Pool

23. NAME (Typed)
Stephen Pool
Contracting Officer
TITLE: CONTRACTING/ORDERING OFFICER

ADM002

AUTHORITY FOR REVISIONS
PREVIOUS EDITIONS ARE NOT USABLE

SUNSI REVIEW COMPLETE SEP 19 2007

OPTIONAL FORM 347 (REV. 4/2006)

**STATEMENT OF WORK FOR TASK ORDER NO. 010 TO PROVIDE
INDEPENDENT VERIFICATION AND VALIDATION SERVICES TO
PROVIDE SECURITY CERTIFICATION & ACCREDITATION SUPPORT FOR THE
BUDGET FORMULATION SYSTEM**

1.0 BACKGROUND

The Office of the Chief Financial Officer (OCFO) of the U.S. Nuclear Regulatory Commission (NRC) requires independent verification and validation (IV&V) services for the steady state OCFO financial management systems, systems under development, and legacy systems replacement efforts.

The NRC requires the support of a Contractor to perform independent verification and validation services for the OCFO financial management systems. The Contractor will use the Office of Information Services Management Directive 2.8, Project Management Methodology requirements or other requirements as directed by the NRC Project Officer to evaluate and support OCFO steady state systems, systems under development, and legacy systems replacement efforts. These services shall include but not be limited to (1) establishing a process for requirements and design reviews, (2) supporting the project team in resolving all software-related issues, (3) evaluation and support of test planning, test validation, execution, and reporting, and (4) providing reports on specific findings and recommendations for actionable items continuously throughout the process.

2.0 OBJECTIVES

The objective of this task order is to provide security certification and accreditation (C&A) support services. The IV&V activities will include review of information technology technical aspects of the Budget Formulation System (BFS) security plan and prepare security procedures for planned activities identified from the BFS system security plan. Specifically, the Contractor shall prepare procedures to support C&A requirements for the BFS. The contractor shall meet the following objectives:

- (1) Evaluate the security requirements as described in the security plan to ensure that critical security requirements are identified.
- (2) Prepare security procedures to address technical resolution identified in the security requirements.
- (3) Provide final procedures addressing technical resolution to correct security requirement deficiencies that resulted from security plan preparation during the security C&A process.

3.0 SCOPE OF WORK

IV&V services are needed for the OCFO Budget Formulation System (BFS) C&A support. The OCFO is currently finalizing the security requirements for the BFS in order to submit an authority to operate. As part of the security requirements, a system security plan (SSP) was produced based upon the National Institutes of Standards and Technology Special Publication 800-53. The SSP categorized NIST security controls into planned, in place and not planned. All planned activities require preparation of procedures to address security requirements. Attachment 1 details the NIST security requirement where security procedures need to be developed.

SPECIFIC TASK REQUIREMENTS

- 3.1.1 Task 1 – Provide Security Certification and Accreditation Support for the Budget Formulation System**

Requirements

The Contractor shall:

1. Develop an IV&V Plan to include a proposed work schedule showing milestones, critical activities, timeframes, and dependencies for the completion of work. The plan should also include estimated level of effort and required resources to perform testing.
2. Include any or all of the artifacts for each of the four (4) phases of the PMM or project life cycle processes. The PMM phases include Inception, Elaboration, Construction, and Transition.
3. Establish a baseline IV&V Plan prior to the start of the project task which should include their proposed methodology or approach that will be used, including a plan of the schedule for the development of each security procedure.
4. Prepare procedures in accordance with the NIST SP 800-53, NRC PMM, and existing BFS procedures.
5. Provide a final procedures addressing technical resolution to correct security requirement deficiencies that resulted from security plan preparation.

Standard

The contractor shall prepare a draft and final document for each procedure identified as a planned activity from the BFS SSP. The draft procedure template will comply with existing procedures in place for the BFS. Existing procedures will be used as a guide and will be provided during the task order kick-off meeting.

Deliverables

The contractor shall deliver the following:

Item	Name	Due Date
1	Draft Independent Verification and Validation Plan (including appendices for the artifacts specified in the PMM)	10 work days after task order award
2	Final Independent Verification and Validation Plan (including appendices for the artifacts specified in the PMM)	5 work days after NRC approval of draft
3	Draft Document for Each Procedure Required	15 work days prior to implementation due date
4	Final Document for Each Procedure Provided	5 work days after NRC approval of draft

Note: NRC approval will be received by the contractor five work days after receipt of a draft.

4.0 OVERALL PERFORMANCE STANDARDS AND DEDUCTION SCHEDULE:

The following processes will be used by NRC to motivate successful performance of the contract requirements stated herein:

Failure by the Contractor to comply with any of the procedures and/or contract requirements stated herein shall constitute a “**valid-deficiency**” under this contract, unless the failure can be shown to be caused by circumstances beyond the Contractor’s control.

No more than one (1) contract-deficiency shall be allowed by NRC per calendar-month period, in which the NRC-PO determines the discrepancy is a “valid-deficiency” for non-compliance with any Contract Requirements.

The Contractor shall invoice monthly with a single invoice that includes a breakdown of the cost of all support provided during the previous calendar-month’s period. For any month in which the Contractor fails to comply with the contract requirements stated herein, NRC reserves the right to deduct the following amounts from that month’s total monthly invoice payment:

- 0-1 Valid-deficiency’s per calendar-month period will result in no deduction;
- 2 Valid-deficiency’s per calendar-month period will result in 5% of the total monthly invoice being deducted;
- 3 Valid-deficiency’s per calendar-month period will result in 6% of the total monthly invoice being deducted;
- 4 Valid-deficiency’s per calendar-month period will result in 7% of the total monthly invoice being deducted;
- 5 Valid-deficiency’s per calendar-month period will result in 8% of the total monthly invoice being deducted;
- 6 Valid-deficiency’s per calendar-month period will result in 10% of the total monthly invoice being deducted.

NOTE: Under the Performance Incentives listed above, NRC will not deduct more than a total of 10% from the monthly invoice.

The deductions listed above do not prevent NRC from taking other appropriate actions to correct performance problems under this contract.

5.0 ACCEPTANCE CRITERIA

For Task 1 in Section 3.0 above, the Contractor shall prepare final security procedures in the appropriate format. The procedures should provide sufficient detail to ensure completeness, consistency, correctness, and accuracy of the work performed and compliance with NIST SP 800-53. All deliverable products shall be grammatically correct according to industry standard rules and contain correct spelling. All technical and financial terms shall be clearly defined to be understood by all readers. All final deliverable products will be approved in writing by the Project Officer or a designated representative.

6.0 MEETINGS AND TRAVEL

6.1.1 Kick-off Meeting

The Contractor shall participate in a kick-off meeting no later than five (5) business days after award to introduce the NRC Project Officer, the Task Manager, and other NRC representatives. The purpose of the meeting is to review and discuss the OCFO’s goals for the project and to establish Contractor/NRC communications report framework for the project. Further, discussion

shall include the corresponding deliverables as identified in Section 3.1.1, Deliverables. Internal NRC documents will be coordinated during this meeting.

6.1.2 Status Meetings

The Contractor shall participate in periodic status meetings to be conducted on a bi-weekly basis. Dates and times of status meetings will be mutually agreed upon by the NRC Task Manager and the Contractor during the kickoff meeting. The Contractor will have the discretion to attend via conference call from the Contractor place of work.

6.1.3 Travel

The Contractor shall complete work associated with these tasks at the Contractor's own facilities and/or NRC Headquarters in Rockville, MD. Travel to other locations will not be required.

7.0 GOVERNMENT FURNISHED MATERIALS AND EQUIPMENT

To facilitate the work to be performed, the NRC will, upon request, provide the Contractor with any and all materials documenting current applications systems, processes, requirements, and access to Government and other Contractor personnel as required.

8.0 PERIOD OF PERFORMANCE

The period of performance for task order No. 010 is 15 months.

Below is an excerpt from the BFS System Security Plan, dated August 17, 2007, identifying the security requirement based upon NIST SP800-53 requiring the preparation of documented procedures. See "Technical Resolution" sections in each security control requirement for a description of required procedure content.

Access Control Policy and Procedures (Main Control)

Security Control Requirement #:	SECCR1
Identifier:	AC-1 (M)
Class:	Technical
Description:	<p>The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.</p> <p>Supplemental Guidance: The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD-ICOD
Responsible System(s):	BFS-NSICD-TELECOMM-IDSSD-WINDOWS-LAN/WAN-DATABASE-DCS-NOVELL-DESKTOPS-RAS
Technical Resolution:	<p>BFS relies on the NSICD information system to provide guidance or restrictions related to agency-wide Access Control policies and procedures.</p> <p>BFS relies on the TELECOMM, IDSSD, WINDOWS, LAN/WAN, DATABASE, DCS, NOVELL, DESKTOPS and RAS information systems to provide formal, documented procedures to facilitate the implementation of the access control policy and associated controls.</p> <p>The agency-wide access control policy meets the needs of BFS.</p> <p>BFS does not currently have formal, documented access control procedures. The ISSO, in coordination with both the BFS Administrator and the Hyperion contractor, will review and update the BFS access control procedures annually when the BFS SSP is updated or when significant changes occur and will ensure that the procedures are stored in ADAMS and disseminated to BFS personnel.</p> <p>Planned Implementation Date: April 30, 2008</p>

Supervision and Review - Access Control (Main Control)

Security Control Requirement #:	SECCR6
Identifier:	AC-13 (M)
Class:	Technical
Description:	<p>The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.</p> <p>Supplemental Guidance: The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST Special Publication 800-92 provides guidance on computer security log management.</p>
Status:	Planned
Responsible Organization(s):	OCFO-ICOD-BPIAD
Responsible System(s):	BFS-WINDOWS-DATABASE-DCS-NOVELL-DESKTOPS-RAS
Technical Resolution:	<p>BFS relies on the WINDOWS, DATABASE, DCS, NOVELL, DESKTOPS and RAS information systems to ensure that accounts are supervised and reviewed for inappropriate activities in accordance with organizational policies and procedures. Any unusual activities are investigated and periodic reviews of access authorizations changes are conducted. Individuals with significant information system roles and responsibilities are reviewed more frequently.</p> <p>Account reviews are not currently in place for BFS because the system is not yet in production. Upon receipt of ATO, the ISSO will begin reviewing the activities of users with respect to the enforcement and usage of BFS access controls. Should the ISSO discover any unusual BFS-related activities, the ISSO and OCFO will conduct appropriate investigations.</p> <p>During the review of BFS user accounts and audit logs, the ISSO will examine the following: access authorizations on an annual basis, checking them against need-to-know to ensure that they are consistent; user activity and system usage on a monthly basis; and activities of users with significant roles and responsibilities, particularly the BFS Administrator, on a bi-weekly basis.</p> <p>Planned Implementation Date: Upon receipt of ATO.</p>

Security Awareness and Training Policy and Procedures (Main Control)

Security Control Requirement #:	SECCR11
Identifier:	AT-1 (M)
Class:	Operational
Description:	<p>The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.</p> <p>Supplemental Guidance: The security awareness and training policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-16 and 800-50 provide guidance on security awareness and training. NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD
Responsible System(s):	BFS-NSICD
Technical Resolution:	<p>BFS relies on the NSICD information system to provide guidance or restrictions related to agency-wide Security Awareness and IT Security Training policies and procedures which address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with federal regulations, guidelines, and standards.</p> <p>The agency-wide security awareness and training policy meets the needs of BFS.</p> <p>BFS does not currently have formal, documented awareness and training procedures. The BFS system owner, in coordination with the ISSO, will develop formal, documented security awareness and training procedures for BFS that are consistent with NRC policy. The BFS ISSO will review and update the security awareness and training procedures for BFS annually when the BFS SSP is updated or when significant changes occur and will ensure that the procedures are disseminated to BFS personnel.</p> <p>Planned Implementation Date: October 31, 2008.</p>

Security Training (Main Control)

Security Control Requirement #:	SECCR13
Identifier:	AT-3 (M)
Class:	Operational
Description:	<p>The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) every other year thereafter.</p> <p>Supplemental Guidance: The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, adequate technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD
Responsible System(s):	BFS-NSICD
Technical Resolution:	<p>BFS relies on the NSICD information system to ensure that the organization identifies personnel that have significant information system security roles and provides appropriate IT Security Training.</p> <p>Personnel with significant Information system security roles and responsibilities, as well as a brief description of these users' roles and responsibilities, are identified on the Users Tab of the BFS Risk Assessment Spreadsheet (<V2.0 ML# TBD>).</p> <p>The agency-wide IT Security Training program meets the needs of BFS. In addition, BFS personnel with significant security roles and responsibilities will receive BFS-specific technical training as described at the end of this Technical Resolution. OCFO ensures that all BFS personnel receive appropriate security and technical training by tracking and monitoring training activities as discussed under the AT-4 control prior to granting them access to the system or allowing them to perform their assigned duties.</p> <p>With regard to the agency's IT security training, the system ISSO completed the NRC Managers and ISSOs Security Awareness Course and the BFS Administrator completed the NRC IT Administrators Awareness Course prior to assuming their duties and will complete refresher training at least every other year.</p> <p>Not all system administrators and power users have undergone all required training. BFS-specific training will be provided every three years to the BFS system administrator(s) and individuals assigned to the BFS power user role. Specifically, Hyperion will provide specialized power user and basic user training. Classroom training will include "Hyperion Planning For Interactive Users" and a review of the BFS User Manual. Training has been held and additional training sessions are planned after an ATO is obtained for the system.</p>

	Planned Implementation Date: October 31, 2007
--	---

Security Training Records (Main Control)

Security Control Requirement #:	SECCR14
Identifier:	AT-4 (M)
Class:	Operational
Description:	<p>The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.</p> <p>Supplemental Guidance: None.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD
Responsible System(s):	BFS-NSICD
Technical Resolution:	<p>BFS relies on the NSICD information system to document and monitor the agency-wide Security Awareness Training and IT Security Training programs.</p> <p>OCFO documents and monitors agency-level and system-specific security training activities, including security awareness training, security training, and technical training for BFS personnel. The Division of Financial Management (DFM) monitors agency security awareness and training activity by requesting from OIS a list of DFM users who have not completed the Annual Computer Security Awareness Training and/or the Annual Information Security Awareness Training. The Director emails these users with a reminder to complete the training before the agency deadline and notifies their supervisors. Supervisors follow-up with their direct reports until they receive confirmation from the NRC Security Awareness Training and IT Security Training Programs that their direct reports attended the training.</p> <p>A log of security training activities is not currently maintained. For BFS-specific security and technical training, the ISSO will keep track of training activities for the BFS staff by maintaining the IT Security Training Log.</p> <p>Planned Implementation Date: October 31, 2007.</p>

Audit and Accountability Policy and Procedures (Main Control)

Security Control Requirement #:	SECCR15
Identifier:	AU-1 (M)
Class:	Technical
Description:	<p>The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.</p> <p>Supplemental Guidance: The audit and accountability policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD-ICOD
Responsible System(s):	BFS-NSICD-WINDOWS-DATABASE-DCS-NOVELL-DESKTOPS-E-MAIL
Technical Resolution:	<p>BFS relies on the NSICD information system to provide guidance or restrictions related to agency-wide audit and accountability policies and procedures to include the audit and accountability controls, roles and responsibilities, and the frequency of reviews.</p> <p>BFS relies on the WINDOWS, DATABASE, DCS, NOVELL, DESKTOPS and E-MAIL information systems to provide formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated controls.</p> <p>The agency-wide audit and accountability policy meets the needs of BFS.</p> <p>BFS does not currently have formal, documented audit and accountability procedures. The system owner, in coordination with the ISSO, will develop formal, documented audit and accountability procedures for BFS that are consistent with NRC policy. The ISSO will review and update the BFS audit and accountability procedures annually when the BFS SSP is updated or when significant changes occur and will ensure that the procedures are stored in ADAMS and disseminated to BFS personnel.</p> <p>Planned Implementation Date: October 31, 2008</p>

Auditable Events (Main Control)

Security Control Requirement #:	SECCR16
Identifier:	AU-2 (M)
Class:	Technical
Description:	<p>The information system generates audit records for the following events:</p> <ul style="list-style-type: none"> User logons, both successful and failed Unsuccessful attempts to access objects (resources) or perform functions that are denied by lack of privileges or rights Successful accesses to security-critical objects (i.e., operating system files, data with high sensitivity) Changes to users' security privileges/profiles Changes to the system security configuration Modification of system-supplied software (if capability exists) Creation and deletion of objects Organization defined or application-specific events Activities of a specified user ID (as required) <p>Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverse the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD-ICOD
Responsible System(s):	BFS-NSICD-WINDOWS-DATABASE-DCS-NOVELL-DESKTOPS-E-MAIL
Technical Resolution:	<p>BFS relies on the NSICD information system to provide guidance or restrictions related to agency-wide auditable events.</p> <p>BFS relies on the WINDOWS, DATABASE, DCS, NOVELL, DESKTOPS and E-MAIL information systems to ensure that audit records are generated based on policy and a risk assessment detailing which events require auditing on a continuous basis and which events require auditing in response to specific</p>

situations.

OCFO has identified important events that need to be audited because they are significant and relevant to the security of BFS and are adequate to support after-the-fact investigations of security incidents. In addition, OCFO has determined the frequency (continuous basis or in response to specific situations) with which these events are audited based on a risk assessment. The specific component that carries out auditing activities is Hyperion Planning. Audit trails are saved for viewing in the Hyperion Planning SQL server repository (HQ2K3BPWPB). The audit records are stored in SQL server repository table HSP_AUDIT_RECORDS. The following information is captured:

- Type of object being audited
- Name of specific object being audited
- User who triggered the modification event
- Action performed (*add, modify, delete, and execute*)
- Name of a property of the object being audited
- Old Value prior to modification
- New value after modification

The following BFS tables are selected for auditing:

- Dimension administration
- Alias Table administration
- Form Definition
- Form Folder Administration
- Workflow
- Copy version
- Security
- Users Administration
- Groups Administration

Refer to the AU-3 control for information on the content of audit records and the AU-9 control for the protection of audit information.

The detailed list of events that are audited by BFS, corresponding frequency, the detail captured, and auditing configuration settings are not formally documented. The BFS Admin Guide will include a detailed list of the events that are audited by BFS, corresponding frequency, the detail captured, and auditing configuration settings.

Planned Implementation Date: April 30, 2008

Audit Storage Capacity (Main Control)

Security Control Requirement #:	SECCR18
Identifier:	AU-4 (M)
Class:	Technical
Description:	<p>The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.</p> <p>Supplemental Guidance: The organization provides sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements. Related security controls: AU-2, AU-5, AU-6, AU-7, SI-4.</p>
Status:	Planned
Responsible Organization(s):	OCFO-ICOD-BPIAD
Responsible System(s):	BFS-WINDOWS-DATABASE-DCS-NOVELL-DESKTOPS-E-MAIL
Technical Resolution:	<p>BFS relies on the WINDOWS, DATABASE, DCS, NOVELL, DESKTOPS and E-MAIL information systems to ensure that sufficient audit record storage capacity is allocated and the system is configured to reduce the likelihood of such capacity being exceeded.</p> <p>The allocation of audit record storage capacity is managed by the System Administrator. BFS server disk volumes provide for approximately 4 gigabytes of free space for audit log files. It is estimated that BFS will generate approximately 1200 MB per year in database logs and less than 12 MB per year for application logs. BFS has the capacity to store log data for 2 to 3 years.</p> <p>Refer to the AU-5 control for the actions that BFS takes when audit storage capacity is exceeded.</p> <p>Currently, BFS is configured to retain log files indefinitely. This could result in audit storage capacity being depleted. BFS will be configured to automatically truncate log and archive log files. Audit log truncation will be performed, at most, annually with monitoring on a monthly basis. Audit log archiving will be performed on an as-needed basis. Procedures for configuring audit log truncation and archiving will be documented.</p> <p>Planned Implementation Date: October 31, 2008</p>

Continuous Monitoring (Main Control)

Security Control Requirement #:	SECCR29
Identifier:	CA-7 (M)
Class:	Management
Description:	<p>The organization monitors the security controls in the information system on an ongoing basis.</p> <p>Supplemental Guidance: Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls is based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or grounds for confidence) that the organization must have in determining the effectiveness of the security controls in the information system. The organization establishes the selection criteria and subsequently selects a subset of the security controls employed within the information system for assessment. The organization also establishes the schedule for control monitoring to ensure adequate coverage is achieved. Those security controls that are volatile or critical to protecting the information system are assessed at least annually. All other controls are assessed at least once during the information system's three-year accreditation cycle. The organization can use the current year's assessment results obtained during continuous monitoring to meet the annual FISMA assessment requirement (see CA-2).</p> <p>This control is closely related to and mutually supportive of the activities required in monitoring configuration changes to the information system. An effective continuous monitoring program results in ongoing updates to the information system security plan, the security assessment report, and the plan of action and milestones-the three principle documents in the security accreditation package. A rigorous and well executed continuous monitoring process significantly reduces the level of effort required for the reaccreditation of the information system. NIST Special Publication 800-37 provides guidance on the continuous monitoring process. NIST Special Publication 800-53A provides guidance on the assessment of security controls. Related security controls: CA-2, CA-4, CA-5, CA-6, CM-4.</p>
Status:	Planned
Responsible Organization(s):	OCFO-ICOD-BPIAD
Responsible System(s):	BFS-CTF-DATABASE-DCS-NOVELL-DESKTOPS-E-MAIL-RAS-TELECOMM-IDSSD-WINDOWS-LAN/WAN
Technical Resolution:	<p>BFS relies on the CTF, DATABASE, DCS, NOVELL, DESKTOPS, E-MAIL, RAS, TELECOMM, IDSSD, WINDOWS and LAN/WAN information systems to ensure that controls being provided by the system are monitored on an ongoing basis.</p> <p>OCFO monitors the security controls in BFS on an ongoing basis through:</p> <ul style="list-style-type: none"> - Baseline configuration management and control of information system components (Refer to the CM-2 control for additional information baseline configuration and inventory); and - Status reporting on findings, including those from reviews of user access, user

	<p>accounts, and logs.</p> <p>The BFS ISSO provides a security status report based on the results of continuous monitoring activities on a quarterly basis, or when a significant vulnerability is identified, to the SITSO, DAA, and any other impacted system owners of interfacing systems, so they can monitor the progress in correcting deficiencies. In addition, the BFS Administrator and ISSO update the BFS Risk Assessment, Security Plan, and Corrective Action Plan to reflect the results of all of the continuous monitoring activities.</p> <p>Continuous monitoring is not currently in place because the system is currently undergoing certification. OCFO will conduct ongoing assessments of security control subsets. The level of effort that will be applied to the ongoing assessment of security control subsets for BFS will be commensurate with the FIPS 199 "Low" security category. OCFO will establish the selection criteria for control subsets and the schedule/frequency for rotating control subsets to ensure adequate coverage is achieved. Using the criteria, the BFS ISSO will subsequently select a subset of the security controls as reviewed and approved by the System Owner. A different subset of security controls will be assessed each year to ensure that all of the security controls are assessed during the three-year accreditation cycle. Controls that are volatile or critical to protecting the information system will be assessed at least annually.</p> <p>Planned Implementation Date: October 31, 2008</p>
--	---

Configuration Management Policy and Procedures (Main Control)

Security Control Requirement #:	SECCR30
Identifier:	CM-1 (M)
Class:	Operational
Description:	<p>The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.</p> <p>Supplemental Guidance: The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD
Responsible System(s):	BFS-NSICD
Technical Resolution:	<p>BFS relies on the NSICD information system to provide guidance or restrictions related to agency-wide configuration management policies and procedures.</p> <p>The agency-wide configuration management policy meets the needs of BFS.</p>

	<p>BFS does not currently have formal, documented configuration management procedures. The BFS system owner, in coordination with the ISSO, will develop formal, documented configuration management procedures for BFS that are consistent with NRC policy. These procedures will be documented in the BFS CCB charter and BFS configuration management plan. The System Administrator and BFS Integrator will review and update BFS configuration management procedures annually when the BFS SSP is updated or when significant changes occur. The System Administrator will ensure that the procedures are available in ADAMS and disseminated to BFS personnel.</p> <p>Planned Implementation Date: October 31, 2007</p>
--	---

Baseline Configuration (Main Control)

Security Control Requirement #:	SECCR31
Identifier:	CM-2 (M)
Class:	Operational
Description:	<p>The organization develops, documents, and maintains a current baseline configuration of the information system.</p> <p>Supplemental Guidance: This control establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives. The baseline configuration of the information system is consistent with the Federal Enterprise Architecture. Related security controls: CM-6, CM-8.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD
Responsible System(s):	BFS-NSICD
Technical Resolution:	<p>BFS relies on the NSICD information system to store the information system's current baseline configuration.</p> <p>Installation and configuration requirements and procedures for Hyperion Planning are provided in the Hyperion Planning Installation Guide for Windows (Chapter 2 for Requirements and Chapters 3-9 for Installation).</p> <p>The configuration baseline is not currently documented. This will be remedied with the creation and approval of the BFS Design Document, which will contain BFS development and production environment specifications, define the standard software load for BFS components, the components' logical placement within the information system architecture, and the specification to which the information system is built.</p> <p>The BFS baseline configuration will be loaded, maintained, and securely stored in the NSICD system in the Rational database that implements the change control process. The Rational toolset will provide the configuration baseline at any point in time for capture for the deliverable.</p> <p>The System Administrator, with contractor support, will update the BFS baseline</p>

	<p>configuration in the NSICD Rational suite as modifications, enhancements, or changes are approved and made to the system to ensure its baseline configuration remains current and documents any deviations to the BFS configuration baseline specification in support of mission needs/objectives.</p> <p>The BFS CCB will ensure that the BFS baseline configuration is consistent with NRC security configuration guidelines.</p> <p>Planned Implementation Date: October 31, 2007</p>
--	---

Contingency Planning Policy and Procedures (Main Control)

Security Control Requirement #:	SECCR34
Identifier:	CP-1 (M)
Class:	Operational
Description:	<p>The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.</p> <p>Supplemental Guidance: The contingency planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-34 provides guidance on contingency planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD-ICOD
Responsible System(s):	BFS-NSICD-DATABASE-DCS-NOVELL-DESKTOPS-E-MAIL-RAS-TELECOMM-IDSSD-WINDOWS-LAN/WAN
Technical Resolution:	<p>BFS relies on the NSICD information system to provide guidance or restrictions related to agency-wide contingency planning policies and procedures.</p> <p>BFS relies on the DATABASE, DCS, NOVELL, DESKTOPS, E-MAIL, RAS, TELECOMM, IDSSD, WINDOWS and LAN/WAN information systems to provide formal, documented procedures to facilitate the implementation of the contingency planning policy and associated controls.</p> <p>The agency-wide contingency planning policy meets the needs of BFS.</p> <p>BFS does not currently have formal, documented contingency planning procedures. While BFS is a listed system and does not require a formal contingency plan, the system must still have limited contingency planning procedures, such as documented procedures for reconstituting the system to a known secure state after a disruption or failure, which required to support the CP-10 (M) control, which applies to listed systems and cannot be fully inherited. The BFS system owner, in coordination with the ISSO, will develop formal, documented contingency planning procedures for the BFS that are consistent with NRC policy. The System Administrator will review and update the contingency planning procedures for BFS annually when the BFS SSP is updated or when significant changes occur and will ensure that the procedures are stored in</p>

	ADAMS and disseminated to applicable BFS personnel. Planned Implementation Date: April 30, 2008.
--	---

Information System Recovery and Reconstitution (Main Control)

Security Control Requirement #:	SECCR38
Identifier:	CP-10 (M)
Class:	Operational
Description:	<p>The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.</p> <p>Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.</p>
Status:	Planned
Responsible Organization(s):	OCFO
Responsible System(s):	BFS
Technical Resolution:	<p>Mechanisms and supporting procedures do not currently exist for recovering and reconstituting the BFS to a known secure state after disruption or failure. BFS mechanisms and supporting procedures, which will be documented in the BFS Contingency Plan, will be established to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure, including the following BFS recovery and reconstitution activities:</p> <ul style="list-style-type: none"> - Reset all system parameters - Reinstall system patches - Reestablish configuration settings - Reinstall application and system software - Access information from the most recent backups - Test the system after it is reconstituted - Ensure system documentation and operating procedures are available electronically in ADAMS. <p>As part of defining these BFS recovery and reconstitution activities, for example, accessing backups or testing the system after reconstitution, OCFO will coordinate with the Data Center Services to clarify roles and responsibilities and to ensure adequate procedures are defined.</p> <p>Planned Implementation Date: October 31, 2007</p>

Identification and Authentication Policy and Procedures (Main Control)

Security Control Requirement #:	SECCR39
Identifier:	IA-1 (M)
Class:	Technical
Description:	<p>The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.</p> <p>Supplemental Guidance: The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and Special Publications 800-73, 800-76, and 800-78; and (ii) other applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-63 provides guidance on remote electronic authentication.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD-ICOD
Responsible System(s):	BFS-NSICD-WINDOWS-LAN/WAN-DATABASE-DCS-NOVELL-DESKTOPS-E-MAIL-RAS
Technical Resolution:	<p>BFS relies on the NSICD information system to provide guidance or restrictions related to agency-wide identification and authentication policies and procedures.</p> <p>BFS relies on the WINDOWS, LAN/WAN, DATABASE, DCS, NOVELL, DESKTOPS, E-MAIL and RAS information systems to provide formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated controls.</p> <p>The agency-wide identification and authentication policy meets the needs of BFS.</p> <p>BFS does not currently have formal, documented identification and authentication procedures. The BFS system owner in coordination with the ISSO, will develop formal, documented identification and authentication procedures for BFS that are consistent with NRC policy. The BFS System Administrator will review and update the BFS identification and authentication procedures annually when the BFS SSP is updated or when significant changes occur and will ensure that the procedures are stored in ADAMS and disseminated to BFS personnel.</p> <p>Planned Implementation Date: April 30, 2008.</p>

Incident Response Policy and Procedures (Main Control)

Security Control Requirement #:	SECCR45
Identifier:	IR-1 (M)
Class:	Operational
Description:	<p>The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.</p> <p>Supplemental Guidance: The incident response policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-61 provides guidance on incident handling and reporting. NIST Special Publication 800-83 provides guidance on malware incident handling and prevention.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD-ICOD
Responsible System(s):	BFS-NSICD-DESKTOPS
Technical Resolution:	<p>BFS relies on the NSICD information system to provide guidance or restrictions related to agency-wide incident response policies and procedures.</p> <p>BFS relies on the DESKTOPS information system to provide formal, documented procedures to facilitate the implementation of the incident response policy and associated controls.</p> <p>The agency-wide incident response policy meets the needs of BFS.</p> <p>BFS does not currently have formal, documented incident response procedures. The BFS system owner, in coordination with the ISSO, will develop incident response procedures for BFS that are consistent with NRC policy. The System Administrator will review and update the BFS incident response procedures annually when the BFS SSP is updated or when significant changes occur and ensure that the procedures are stored in ADAMS and disseminated to BFS personnel.</p> <p>Planned Implementation Date: October 31, 2008</p>

Incident Handling (Main Control)

Security Control Requirement #:	SECCR46
Identifier:	IR-4 (M)
Class:	Operational
Description:	<p>The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.</p> <p>Supplemental Guidance: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly. Related security controls: AU-6, PE-6.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD
Responsible System(s):	BFS-NSICD
Technical Resolution:	<p>BFS relies on the NSICD information system to implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.</p> <p>OCFO implements an incident handling capability for BFS security incidents that includes preparation, detection and analysis, containment, eradication, and recovery as described below:</p> <p>Preparation</p> <p>BFS implements the following measures to prevent and prepare for security incidents: continuous monitoring activities (CA-7); baseline configuration (CM-2); security configuration settings (CM-6); patch management and flaw remediation (SI-2); routine and controlled maintenance (MA-2); malicious code protection (SI-3); security awareness and training (AT-2 and AT-3); and boundary protections (SC-7).</p> <p>Detection and Analysis</p> <p>BFS security incidents are detected by BFS users. Upon detecting a BFS security incident, the individual notifies the BFS ISSO and the System Administrator. BFS users and staff report any unusual activity, such as systems that appear to be running slowly, files with dates last modified that may be inaccurate, new files they do not recognize, and warning messages from the anti-virus applications on their desktops to both the BFS ISSO and the System Administrator and the NRC Customer Support Center (CSC).</p> <p>BFS security incidents are also detected through malicious code protection software (refer to the SI-3 control); routine review of logs; and physical access monitoring (refer to the PE-6 control). As discussed under the SI-5 control, the BFS ISSO receives security incident information through participation in various email notification lists and regularly checking the US-CERT website for security alerts and bulletins. The BFS ISSO and the System Administrator analyze each incident to first determine if it is legitimate and then to determine appropriate containment, eradication, and recovery actions. Upon receiving notification of an incident, the System Administrator conducts an initial analysis to identify the extent of damage. The System Administrator reviews performance data,</p>

	<p>migrations of software modifications, connections to interfacing systems, and other factors previously tracked in Rational to determine the cause.</p> <p>Containment, Eradication, and Recovery</p> <p>After incidents are identified, the System Administrator determines remedial actions to contain, eradicate, and recover from the incidents, as well as the resources required. The System Administrator notifies users via email of expected downtime or any other residual effects they may experience as a result of the incident. Refer to the IR-6 control for information on the reporting of BFS security incidents.</p> <p>Incident response procedures incorporating lessons learned from ongoing incident handling activities are not currently implemented. BFS personnel will incorporate the lessons learned from ongoing incident handling activities into the incident response procedures, which are addressed under the IR-1 control, and will implement the procedures accordingly.</p> <p>Planned Implementation Date: October 31, 2008</p>
--	---

System Maintenance Policy and Procedures (Main Control)

Security Control Requirement #:	SECCR49
Identifier:	MA-1 (M)
Class:	Operational
Description:	<p>The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.</p> <p>Supplemental Guidance: The information system maintenance policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>
Status:	Planned
Responsible Organization(s):	OCFO-ICOD-BPIAD
Responsible System(s):	BFS-CTF-DATABASE-DCS-NOVELL-DESKTOPS-E-MAIL-RAS-TELECOMM-IDSSD-WINDOWS-LAN/WAN-NSICD
Technical Resolution:	<p>BFS relies on the CTF, DATABASE, DCS, NOVELL, DESKTOPS, E-MAIL, RAS, TELECOMM, IDSSD, WINDOWS and LAN/WAN information systems to provide formal, documented procedures to facilitate the implementation of the system maintenance policy and associated controls.</p> <p>BFS relies on the NSICD information system to provide guidance or restrictions related to agency-wide maintenance policies and procedures.</p> <p>Agency-wide maintenance policy as provided by NSICD meets the needs of the BFS.</p> <p>BFS does not currently have formal, documented system maintenance procedures. The BFS system owner, in coordination with the ISSO, will develop formal, documented procedures for BFS that are consistent with NRC policy. The System Administrator will review and update the BFS information system maintenance procedures for BFS annually when the BFS SSP is updated or when significant changes occur. The System Administrator will ensure that the procedures are stored in ADAMS and disseminated to BFS personnel.</p> <p>Planned Implementation Date: October 31, 2008</p>

Controlled Maintenance (Main Control)

Security Control Requirement #:	SECCR50
Identifier:	MA-2 (M)
Class:	Operational
Description:	<p>The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.</p> <p>Supplemental Guidance: All maintenance activities to include routine, scheduled maintenance and repairs are controlled; whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks all potentially impacted security controls to verify that the controls are still functioning properly.</p>
Status:	Planned
Responsible Organization(s):	OCFO-ICOD
Responsible System(s):	BFS-TELECOMM-IDSSD-WINDOWS-LAN/WAN-DCS-DESKTOPS
Technical Resolution:	<p>BFS relies on the TELECOMM, IDSSD, WINDOWS, LAN/WAN, DCS and DESKTOPS information systems to schedule, perform, document, and review records of routine preventative and regular maintenance (including repairs) on the system's components in accordance with manufacturer or vendor specifications and/or organizational requirements.</p> <p>The Project Manager approves the requests for removal and/or replacement of BFS components and then submits these requests to the OCFO IT Coordinator who in turn forwards the request to CSC. The OCFO IT Coordinator and the System Administrator track the removal and/or replacement of BFS components and ensure the removal of all information from associated media, using approved NRC procedures, when BFS components require off-site repair.</p> <p>Procedures do not currently exist for checking security features after maintenance is performed. Procedures for checking security features after maintenance is performed will be documented in the BFS configuration management plan (addressed under the CM-1 control). The System Administrator will upload the results of security functionality testing in Rational ClearQuest.</p> <p>Planned Implementation Date: April 30, 2008</p>

Maintenance Personnel (Main Control)

Security Control Requirement #:	SECCR52
Identifier:	MA-5 (M)
Class:	Operational
Description:	<p>The organization allows only authorized personnel to perform maintenance on the information system.</p> <p>Supplemental Guidance: Maintenance personnel (whether performing maintenance locally or remotely) have appropriate access authorizations to the information system when maintenance activities allow access to organizational information or could result in a future compromise of confidentiality, integrity, or availability. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD-ICOD
Responsible System(s):	BFS-DATABASE-DCS-NOVELL-DESKTOPS-NSICD-E-MAIL-RAS-TELECOMM-IDSSD-WINDOWS-LAN/WAN
Technical Resolution:	<p>BFS relies on the DATABASE, DCS, NOVELL, DESKTOPS, NSICD, E-MAIL, RAS, TELECOMM, IDSSD, WINDOWS and LAN/WAN information systems to ensure that only authorized personnel are allowed to perform maintenance on the information system.</p> <p>Maintenance activities that allow access to BFS information and could result in a future compromise of confidentiality, integrity, or availability are restricted to authorized personnel who are IT-I access approved. Maintenance of the BFS application is restricted to the BFS System Administrator and OIS Database Administrator. Access restrictions associated with changes to BFS are enforced through Rational.</p> <p>In the event maintenance personnel do not have needed access authorizations, OCFO personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on BFS.</p> <p>A list of personnel authorized to perform maintenance on BFS does not currently exist. The System Administrator will maintain a list of personnel authorized to perform maintenance on BFS.</p> <p>Planned Implementation Date: April 30, 2008</p>

Media Protection Policy and Procedures (Main Control)

Security Control Requirement #:	SECCR53
Identifier:	MP-1 (M)
Class:	Operational
Description:	<p>The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.</p> <p>Supplemental Guidance: The media protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD-ICOD
Responsible System(s):	BFS-NSICD-TELECOMM-DCS-NOVELL-DESKTOPS
Technical Resolution:	<p>BFS relies on the NSICD information system to provide guidance or restrictions related to agency-wide media protection policies and procedures.</p> <p>BFS relies on the TELECOMM, DCS, NOVELL and DESKTOPS information systems to provide formal, documented procedures to facilitate the implementation of the media protection policy and associated controls.</p> <p>The agency-wide media protection policy and procedures meet the needs of BFS.</p> <p>BFS does not currently have formal, documented media protection procedures. The BFS system owner, in coordination with the ISSO, will develop media protection procedures for the BFS that are consistent with NRC policy. The System Administrator will review and update the media protection procedures for BFS annually when the BFS SSP is updated or when significant changes occur and will ensure that the procedures are stored in ADAMS and disseminated to applicable BFS personnel.</p> <p>Planned Implementation Date: October 31, 2008</p>

Security Planning Policy and Procedures (Main Control)

Security Control Requirement #:	SECCR67
Identifier:	PL-1 (M)
Class:	Management
Description:	<p>The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.</p> <p>Supplemental Guidance: The security planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-18 provides guidance on security planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD-ICOD
Responsible System(s):	BFS-NSICD-WINDOWS-CTF-DATABASE-DCS-NOVELL-DESKTOPS-RAS
Technical Resolution:	<p>BFS relies on the NSICD information system to provide guidance or restrictions related to agency-wide planning policies and procedures.</p> <p>BFS relies on the WINDOWS, CTF, DATABASE, DCS, NOVELL, DESKTOPS and RAS information systems to provide formal, documented procedures to facilitate the implementation of the planning policy and associated controls.</p> <p>BFS does not currently have formal, documented security planning procedures. The BFS system owner, in coordination with the ISSO, will develop formal, documented security planning procedures for BFS that are consistent with NRC policy. The BFS ISSO will review and update the planning procedures for BFS annually when the BFS SSP is updated or when significant changes occur and will ensure that the procedures are disseminated to BFS personnel.</p> <p>Planned Implementation Date: October 31, 2008</p>

Rules of Behavior (Main Control)

Security Control Requirement #:	SECCR70
Identifier:	PL-4 (M)
Class:	Management
Description:	<p>The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.</p> <p>Supplemental Guidance: Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST Special Publication 800-18 provides guidance on preparing rules of behavior.</p>
Status:	Planned
Responsible Organization(s):	OCFO-ICOD-BPIAD
Responsible System(s):	BFS-CTF-DCS-NSICD
Technical Resolution:	<p>BFS relies on the CTF, DCS and NSICD information systems to establish and make readily available to all users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. A signed acknowledgement from users indicating that they have read, understand, and agree to abide by these rules must be received before users are authorized to access the system and its resident information.</p> <p>BFS does not currently have formal, documented rules of behavior. The BFS system owner, in coordination with the ISSO, will establish rules of behavior for authorized BFS users. The BFS Rules of Behavior will comply with MD 12.5 and describe users' responsibilities and expected behavior with regard to information system usage. The BFS Rules of Behavior will be distributed to authorized BFS users when they are given their user account and have been trained. OCFO will ensure that authorized BFS users read and sign the Rules of Behavior document indicating they have read, understand, and agree to abide by the rules of behavior prior to being granted access to BFS.</p> <p>Planned Implementation Date: One month after ATO is granted.</p>

Personnel Security Policy and Procedures (Main Control)

Security Control Requirement #:	SECCR72
Identifier:	PS-1 (M)
Class:	Operational
Description:	<p>The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.</p> <p>Supplemental Guidance: The personnel security policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD-ICOD
Responsible System(s):	BFS-NSICD-WINDOWS-DATABASE-DCS-NOVELL
Technical Resolution:	<p>BFS relies on the NSICD information system to provide guidance or restrictions related to agency-wide planning policies and procedures.</p> <p>BFS relies on the WINDOWS, DATABASE, DCS and NOVELL information systems to provide formal, documented procedures to facilitate the implementation of the personnel security policy and associated controls.</p> <p>The agency-wide personnel security policy meets the needs of BFS.</p> <p>BFS does not currently have formal, documented personnel security procedures. The BFS system owner, in coordination with the ISSO, will develop personnel security procedures for BFS that are consistent with NRC policy. The BFS ISSO will review and update the personnel security procedures for BFS annually when the BFS SSP is updated or when significant changes occur and will ensure that the procedures are stored in ADAMS and disseminated to BFS personnel.</p> <p>Planned Implementation Date: April 30, 2008</p>

Position Categorization (Main Control)

Security Control Requirement #:	SECCR73
Identifier:	PS-2 (M)
Class:	Operational
Description:	<p>The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations annually.</p> <p>Supplemental Guidance: Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD
Responsible System(s):	BFS-NSICD
Technical Resolution:	<p>BFS relies on the NSICD information system to define risk designations based on job roles and responsibilities and establish screening criteria for individuals filling those positions. The organization reviews and revises position risk designations annually.</p> <p>BFS-specific risk designations are consistent with NRC policy. The risk designation identifies the level of access authorization (Q-Top Secret Clearance, L(H)-High Public Trust Secret Clearance, L- Secret Clearance, or IT Level I) required for that position. NRC access authorizations and corresponding investigation types are described in Exhibit 6 "Security Clearances/Access Types" of MD 12.3.</p> <p>The BFS ISSO reviews and revises BFS position risk designations annually.</p> <p>BFS roles, sensitivity criteria, and corresponding access authorizations are not currently documented. The BFS roles, sensitivity criteria, and corresponding access authorizations will be documented at the time the security access to the BFS is established and granted.</p> <p>Planned implementation date: October 31, 2007.</p>

1Risk Assessment Policy and Procedures (Main Control)

Security Control Requirement #:	SECCR80
Identifier:	RA-1 (M)
Class:	Management
Description:	<p>The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.</p> <p>Supplemental Guidance: The risk assessment policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-30 provides guidance on the assessment of risk. NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>
Status:	Planned
Responsible Organization(s):	OCFO-ICOD-BPIAD
Responsible System(s):	BFS-IDSSD-NSICD
Technical Resolution:	<p>BFS relies on the IDSSD information system to provide formal, documented procedures to facilitate the implementation of the risk assessment controls.</p> <p>BFS relies on the NSICD information system to provide guidance or restrictions related to agency-wide risk assessment policies and procedures.</p> <p>The agency-wide risk assessment policy meets the needs of the BFS information system.</p> <p>BFS does not currently have formal, documented risk assessment procedures. The BFS system owner, in coordination with the ISSO, will develop risk assessment procedures for BFS that are consistent with NRC policy. The BFS ISSO will review and update the risk assessment procedures for BFS annually when the BFS SSP is updated or when significant changes occur and will ensure that the procedures are disseminated to applicable BFS personnel.</p> <p>Planned Implementation Date: October 31, 2008</p>

Information System Documentation (Main Control)

Security Control Requirement #:	SECCR88
Identifier:	SA-5 (M)
Class:	Management
Description:	<p>The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.</p> <p>Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non-existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.</p>
Status:	Planned
Responsible Organization(s):	OCFO
Responsible System(s):	BFS
Technical Resolution:	<p>System documentation is not yet complete. OCFO will develop adequate BFS documentation in accordance with NRC policy. The system documentation will be stored, protected, and made available to authorized personnel through Rational ClearCase. The BFS Administrator will be responsible for maintaining BFS documentation and ensuring BFS users have access to it.</p> <p>A BFS administrator guide, which will include procedures for installing, configuring, optimizing the system's security features, and administering BFS, is currently under development. A BFS user manual is also under development and will include procedures for operating BFS. In addition, there is vendor-supplied documentation for the Hyperion software, which includes the Hyperion Planning Administrator's Guide, Hyperion External Authentication Configuration Guide, and installation guides for Hyperion Planning, Reports, and Essbase Analytic Services. The Hyperion documentation provides general instructions for installing, configuring, and administering Hyperion products. BFS software and hardware inventory was initially captured in the System Assets Tab of the BFS risk assessment, and will be maintained in Rational.</p> <p>Planned Implementation Date: October 31, 2007</p>

System and Communications Protection Policy and Procedures (Main Control)

Security Control Requirement #:	SECCR92
Identifier:	SC-1 (M)
Class:	Technical
Description:	<p>The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.</p> <p>Supplemental Guidance: The system and communications protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD-ICOD
Responsible System(s):	BFS-NSICD-CTF-DATABASE-DCS-NOVELL-DESKTOPS-E-MAIL-RAS-IDSSD-WINDOWS-LAN/WAN
Technical Resolution:	<p>BFS relies on the NSICD information system to provide guidance or restrictions related to agency-wide system and communications protection policies and procedures.</p> <p>BFS relies on the CTF, DATABASE, DCS, NOVELL, DESKTOPS, E-MAIL, RAS, IDSSD, WINDOWS and LAN/WAN information systems to provide formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated controls.</p> <p>The agency-wide system and communications protection policy meets the needs of BFS.</p> <p>BFS does not currently have formal, documented system and communications protection procedures. The BFS system owner, in coordination with the ISSO, will develop formal, documented system and communications protection procedures for BFS that are consistent with NRC policy. The BFS System Administrator will review and update the BFS system and communications procedures annually when the BFS SSP is updated or when significant changes occur and will ensure that the procedures are stored in ADAMS and disseminated to BFS personnel.</p> <p>Planned Implementation Date: October 31, 2008</p>

System and Information Integrity Policy and Procedures (Main Control)

Security Control Requirement #:	SECCR97
Identifier:	SI-1 (M)
Class:	Operational
Description:	<p>The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.</p> <p>Supplemental Guidance: The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>
Status:	Planned
Responsible Organization(s):	OCFO-BPIAD-ICOD
Responsible System(s):	BFS-NSICD-IDSSD-WINDOWS-DATABASE-DCS-NOVELL-DESKTOPS-RAS
Technical Resolution:	<p>BFS relies on the NSICD information system to provide guidance or restrictions related to agency-wide systems and information integrity policies and procedures.</p> <p>BFS relies on the IDSSD, WINDOWS, DATABASE, DCS, NOVELL, DESKTOPS and RAS information systems to provide formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated controls.</p> <p>The agency-wide system and information integrity policy meets the needs of BFS.</p> <p>BFS does not currently have formal, documented system and information integrity procedures. The BFS system owner, in coordination with the ISSO, will develop formal, documented integrity procedures (including procedures for the identification, reporting, and correction of system flaws) for BFS that are consistent with NRC policy. The System Administrator will review and update the BFS system and information integrity procedures annually when the BFS SSP is updated or when significant changes occur and will ensure that the procedures are stored in ADAMS and disseminated to BFS personnel.</p> <p>Planned Implementation Date: April 30, 2008</p>