

1. DATE OF ISSUE	2. AGREEMENT NUMBER <b>CFO-08-003</b>	3. MOD NO.
4. AGENCY LOCATOR NO. <b>31000001</b>	5. B & R NUMBER <b>77N-15-5H1363</b>	
7. JOB CODE <b>N7152</b>	8. APPROPRIATION SYMBOL <b>31X0200</b>	
9. BOC <b>253A</b>	10. DOCUMENT IDENTIFICATION NUMBER <b>RQ CFO 08318</b>	

**AWARD OF INTERAGENCY AGREEMENT**

ISSUED BY  
**U.S. Nuclear Regulatory Commission  
Washington, DC 20555-0001**

11. NAME AND ADDRESS OF SERVICING AGENCY  
**U.S. Department of the Interior  
National Business Center  
7301 W. Mansfield Avenue  
Mail Stop D2705, Attn: Agreements  
Denver, CO 80235-2230**

PROJECT MANAGER  
**Olga Kasaskeris**

12. JOB CODE TITLE  
**DOI/NBC Accounts Payable Services**

13. AGREEMENT PERFORMANCE PERIOD	
BEGIN	END
<b>12/17/2007</b>	<b>02/29/2008</b>

**14. OBLIGATION AVAILABILITY PROVIDED BY**

A. THIS ACTION	\$	<b>105,000</b>
B. TOTAL PLACED PRIOR TO THIS ACTION WITH THE PERFORMING ORGANIZATION UNDER THIS JOB CODE FOR THIS FISCAL YEAR	\$	<b>5</b>
C. TOTAL ORDERS TO DATE FOR THIS JOB CODE FOR THIS FISCAL YEAR	\$	<b>0</b>
D. TOTAL ORDERS TO DATE FOR THIS AGREEMENT	\$	<b>105,000</b>

**15. ATTACHMENTS**

THE FOLLOWING ATTACHMENTS ARE MADE A PART OF THIS AGREEMENT

- STATEMENT OF WORK
- ADDITIONAL TERMS AND CONDITIONS
- OTHER (Specify) **NBC Form IA-01**

**16. SECURITY**

- WORK ON THIS AGREEMENT INVOLVES CLASSIFIED INFORMATION
- WORK ON THIS AGREEMENT INVOLVES SENSITIVE UNCLASSIFIED INFORMATION
- WORK ON THIS AGREEMENT IS UNCLASSIFIED AND NOT SENSITIVE

17. FEE BILLABLE UNDER 10 CFR PART 170  YES  NO

**18. REMARKS**

To fund cross-servicing of travel payments.

**19. AUTHORITY TO ENTER INTO INTERAGENCY AGREEMENT (Check only one)**

- ENERGY REORGANIZATION ACT OF 1974, AS AMENDED
- THE ECONOMY ACT OF 1932
- THE CLINGER-COHEN ACT OF 1996
- OTHER (Specify)

20. ADVANCE PAYMENT  IS NOT AUTHORIZED  IS AUTHORIZED (Requires approval by Director, DFS/OCFO)

**21. ESTIMATED COST FOR FULL PERFORMANCE OF THIS AGREEMENT**

FY	FY	FY	FY	FY	TOTAL
\$ 105,000	\$	\$	\$	\$	\$ 105,000

**22. CERTIFICATION OF FUNDS**

This certifies that funds in the amount cited in Block 14.A. are available in the current fiscal year allowance for work authorized by this agreement.

ISSUING AGENCY CERTIFICATION OFFICIAL (Typed Name) **Virginia Bolding** SIGNATURE *Virginia Bolding* DATE **12/14/2007**

**23. SIGNATURES**

NRC ISSUING AUTHORITY (Typed Name and Title) **William M. McCabe** SIGNATURE *William M. McCabe* DATE **12/14/07**  
SERVICING AGENCY OFFICIAL/DESIGNEE (Typed Name and Title) SIGNATURE DATE

Form NBC-IA-01  
(1st 2002)

**National Business Center  
Inter/Intra Agency Agreement**

1. Agreement Number: <b>8-6620-FFS-NRC-28</b>		2. Action Type: <b>New</b>	
3. Period of Performance: Start Date: <b>12/17/2007</b> End Date: <b>02/29/2008</b> 4. FY: <b>2008</b>			
<b>5. Customer Information</b>		<b>6. NBC Information</b>	
5a. Customer: <b>NUCLEAR REGULATORY COMMISSION 11545 Rockville Pike ROCKVILLE, MD 20852-2747</b>		6a. Directorate/Division: <b>FINANCIAL MANAGEMENT - BUSINESS MANAGEMENT OFFICE, D2705 National Business Center 7301 W. Mansfield Avenue Mail Stop D2705, Attn: Agreements Denver, CO 80235-2230</b>	
5b. Customer Reference Number:		6b. Product Line: <b>See Statement of Work</b>	
5c. Project Coordinator: <b>Olga Kasaskeris Phone: 301-415-5975 Fax: 301-415-6562 Email: OHK1@nrc.gov</b>		6c. Project Coordinator: <b>Michael J. Conkey Phone: 303-969-5587 Email: michael_j_conkey@nbc.gov</b>	
5d. Customer Agency Location Code: <b>31-00-0001</b>		6d. NBC Agency Location Code: <b>14-01-0001</b>	
5e. Customer Appropriation Code: <b>31X0200</b>		6e. NBC Appropriation Code: <b>14x4523</b>	
Customer Account Number:		6f. Agreement Type: <b>Fixed Price</b>	
5g. Customer Obligating Doc Number:		6g. NBC DUNS Number: <b>131978129</b>	
5h. Customer DUNS Number: <b>040535809</b>			

**7. Description**

<b>Tasks:</b>	<b>Original Amount</b>	<b>Modification Amount</b>	<b>Total</b>
A. Financial Mgmt Sys Supt. Implement/Convert (IMP). Financial Assist Sys	\$25,000.00		\$25,000.00
B. Accounting Ops. Financial Trans Processing. TDY Travel	\$65,000.00		\$65,000.00
C. Accounting Ops. Financial Trans Processing. PCS Travel	\$15,000.00		\$15,000.00
<b>Total Price</b>	<b>\$105,000.00</b>		<b>\$105,000.00</b>

8. Purpose of Agreement  
*The NBC will provide to the NRC accounting operations services, specifically temporary duty and permanent change of station travel payment support. See the NBC proposal dated December 2007, for specific functions, tasks and responsibilities. "Refer to the Service Level Agreement attached for information regarding period of performance, performance metrics, NBC and Customer responsibilities, and contractual issues related to the specific services provided under the agreement."*

Form NBC-IA-01

(August 2002)

Document Number: 8-6620-FFS-NRC-28

9. Authority: (Please check all that apply. If other is checked, please add a description.)

Economy Act, 31 USC 1535

Working Capital Fund 43 USC 1467, 1468

Other

10. Termination Provisions: (Please check the appropriate block)

This agreement may be terminated before the end performance date by 180 days written notice from either party, followed by mutual agreement between the parties. The customer will be billed for all costs incurred at the time of the termination.

11. Billing Provisions: (Please check the appropriate blocks and fill in IPAC contact information)

The customer will be billed *Quarterly*

Bill Format: *IPAC*

NBC IPAC Contact Person

Name: *Gall Cunningham*

Telephone Number: *303-969-7190*

12. Other Terms and Conditions/Miscellaneous:

13. Approvals

13a. Customer Approval		13b. NBC Approval	
Signature:	Date:	<i>Connie M Sanborn</i>	
Name: <i>William M McCabe</i>	<i>12/14/07</i>	Signature:	Date: <i>12/13/2007</i>
Title: <i>Chief Financial Officer</i>		Name: <i>Connie M Sanborn</i>	
Signature:	Date:	Title: <i>Chief, Accounting Operations Division</i>	
Name:		Signature:	Date:
Title:		Name:	
		Title:	
13c. For NBC Internal Use Only			
		Signature:	Date:
		Name: <i>Andrew J Street</i>	
		Title: <i>Budget Analyst</i>	

**NATIONAL BUSINESS CENTER (NBC) INFORMATION TECHNOLOGY (IT)  
SECURITY SERVICES ADVISORY (SSA) FOR ALL NBC IT CUSTOMERS**

**I. AUTHORITY.**

This Security Services Advisory (SSA) satisfies the requirements of the Office of Management and Budget (OMB) Circular A-130, Appendix III. Its acceptance is assumed by the signatures of the appropriate representatives on the Inter-Agency Agreement (IAA) to which it is attached.

**II. BACKGROUND.**

The NBC provides its customers with high quality, responsive and responsible computer and information security services commensurate with the sensitivity and criticality of customer data and applications. NBC IT Security consists of a staff of highly trained professionals whose sole function is to serve the IT Security needs of the NBC and its customers. The NBC operates under the premise that IT Security services involve shared responsibilities between the NBC and its customers. This premise is reflected throughout this document and in every service provided to NBC customers.

**III. PURPOSE.**

The purpose of this document is to clearly document the IT security services provided to customers by the NBC and to express security roles, responsibilities and behaviors the NBC expects on the behalf of customer organizations and users.

**IV. RESPONSIBILITIES.**

This SSA covers IT Security for General Support Systems (GSS) and Major Applications (MA) that are under the operational control of the NBC.

**A: NBC RESPONSIBILITIES AND EXPECTATIONS RELATING TO CUSTOMERS**

**1. The NBC:**

- Publishes policies, standards, and procedures relating to all aspects of computer and information security.
- Conducts continuity of operations planning to ensure the recoverability and continuity of services for all NBC customers in the event of a disaster or other unplanned outage.
- Establishes and maintains policies and procedures for performing and storing backups, and for securing sensitive or restricted information contained in backups from unauthorized access.
- Maintains systems security certification and accreditation (C&A) documentation for all GSSes and MAs for which the NBC is responsible. Copies of signed authority to operate (ATO) documents will be provided to customers on request.
- Conducts regular security assessments and tests as prescribed in the Federal Information Security Management Act (FISMA) of 2002 and the National Institute of Standards and Technology (NIST) Special Publication 800-26, Revision 1, "Security Self-Assessment Guide for Information Technology Systems."
- Ensures that appropriate background investigations are conducted for NBC employees and contractors.
- Ensures that all NBC employees and contractors receive initial security awareness training before being given access to NBC-managed computer systems, and annual follow-up security awareness training as required by OMB Circular A-130, Appendix III, Department of the Interior Departmental Manual 375, Chapter 19, and the NBC Computer and Information Security Policy (NBCM-CIO-6300-001).
- Endeavors to ensure through the use of policies and awareness training, that all NBC employees and contractors know how to identify sensitive or restricted information, and that they comply with requirements for marking, handling, disclosing, releasing, storing, retaining, copying or backing up, disposing of, sanitizing, or destroying such information.
- Provides customers with reasonable assurance that IT resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. Such controls include physical controls, (e.g., keeping computers in locked rooms to limit physical access), logical controls (e.g., security software programs designed to prevent or detect unauthorized access to sensitive files), and personnel controls (e.g., background checks, security clearances, etc.) as required by Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors.
- Follows stringent requirements of the Department of the Interior, and bureau-wide policies and guidelines requiring the use of firewalls, intrusion detection systems (IDS), and computer security incident response capabilities.
- Applies appropriate communications security, in accordance with OMB, FIPS, NIST and Departmental policies and standards.
- Uses antivirus software and ensures that current versions are used on all equipment, to include procedures for ensuring that portable devices such as laptops are updated as often as possible.
- Maintains a security management process designed to provide auditable records of request activity for access to customer data.

- Enforces the use of individually assigned User IDs and complex secret passwords that must be changed on a standardized cycle of password aging.
- Employs security procedures that apply when employees terminate employment or change jobs.
- Routinely monitors activity against sensitive application and system files to detect indicators of misuse or abuse and notifies customers whenever evidence of misuse or abuse of customer data has been detected.
- Provides ad hoc reporting to auditors and customers relating to various aspects of computer and information security.
- Acts as Subject Matter Experts for computer and information security matters for the NBC and its customers.
- Provides a Computer Security Incident Response Capability in the event of a successful penetration attack against an NBC system and notifies customers whenever a computer security incident occurs that involves or threatens the customer's application or data.

2. **NBC Customers who access NBC IT resources agree to be responsible for:**

- Establishing a security hierarchy to interface with the NBC IT Security staff in resolving problems or issues relating to the security and protection of NBC-managed computer systems, or of customer systems or data.
- Ensuring, when the customer will be using NBC-provided security services (e.g., adding, deleting or controlling access privileges of customer users to an NBC-managed system or application), that as a minimum, the customer must identify an individual, to perform the function of Data Owner (Data Custodian) and one or more Security Points of Contact (SPOCs). This requirement is satisfied through the completion of NBC forms (DEN-NBC-IT-01, 02 and 03).

Customers may elect to have one Data Custodian for the entire organization or may choose to designate separate individuals for each MA. Similarly, depending on the size of the organization, a Data Custodian may also perform the function of SPOC.

- Ensuring that appropriate background investigations are conducted for all customer employees and contractors who will access an NBC-managed computer system or application, in accordance with HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors.
- Ensuring that all customer employees and contractors, who have a business requirement to connect to and log on to an NBC-managed computer system or application, AND who are subject to the requirements of OMB Circular A-130, Appendix III or DOI Departmental Manual 375, Chapter 19, receive initial security awareness training before being given access to NBC-managed systems, and annually thereafter.

Some customer organizations are *not* subject to DOI or OMB computer security guidance. However, if the employees and contractors of such organizations have a business need to access (connect to and log on to), an NBC-managed computer system, the customer organization is responsible for ensuring that the employees and contractors of the organization are provided with appropriate security awareness training, as defined under applicable government guidelines or regulations.

- Acknowledging that the security of customer data is ultimately the responsibility of the customer organization. Except for the actions of customer end-users, the NBC is responsible for the security of customer data while it is housed and processed in the NBC data center. Customers are responsible for having an auditable internal process for documenting requests for access to customer data. According to the Federal Information System Controls Audit Manual (FISCAM) the process should include such things as:
  - Standard forms to document access requests. Request documentation should be retained in active archives for as long as the user remains with the organization.
  - A procedure to document the approval of access requests by senior managers or by designated access approval authorities within the organization.
  - A process to ensure secure transfer of access request documentation to customer security representatives.
  - Periodic reviews of access authorizations to determine if they remain appropriate.
- Informing the NBC, as part of the Interagency Agreement (IAA) process of:
  - Information sensitivity classification(s) associated with customer data, that exceed the information sensitivity classifications currently processed and managed by the NBC, (e.g., anything more restrictive than Privacy Act, Indian Trust, For Official Use Only (FOUO) or Sensitive But Unclassified (SBU). Also include any special handling requirements that exceed those currently being enforced by the NBC for its customers.
  - Information criticality level(s) associated with customer data, which would require disaster recovery restoration in less than 72 hours, which is the current NBC standard. Also include any special data backup requirements that would exceed the nightly and weekly data backup standard currently being provided for NBC customer data.

Also see Section B. relating to this subject.

- Reporting to NBC IT Security any security events or incidents at a customer site that might threaten or negatively impact the integrity or availability of the NBC network or of any NBC-managed computer system.
- Cooperating with the NBC Computer Security Incident Response Team (CSIRT) in the event of a successful security penetration or other breach so that evidence may be collected and preserved and the security of the network or system can be restored.

3. **The customer Data Custodian, for organizations whose employees and contractors have a business need to connect to and log on to an NBC-managed computer system or application, is responsible to:**

- Coordinate with NBC IT Security to establish and maintain security of data belonging to the customer organization.
- Identify appointments to NBC IT Security, in writing, for individuals to serve as Security Points of Contact (SPOCs) for the customer organization. (This requirement is satisfied through the completion of NBC forms (DEN-NBC-IT-02 and 03).
- Ensure that customer employees and contractors behave in a manner that is appropriate to the use and protection of NBC-managed computer systems and applications, based on applicable government security guidelines and recommendations.  
NOTE: Section VI of this SSA contains application-specific rules of behavior (ROB) for NBC-managed systems. These ROB are provided in compliance with OMB Circular A-130, Exhibit III, paragraph 3., a., 2), a). The ROB portion of this SSA should be removed by the customer and provided to the customer data custodian(s). The ROB may be used at the customer's discretion to ensure application users behave in a manner appropriate for the security and protection of federal computer systems.
- Authorize the NBC, in writing, to access customer data to the extent necessary to perform normal data center operational functions (e.g., system performance, system backup and recovery, resource utilization analysis), and normal database maintenance and support functions (e.g., database performance, database backup and recovery, database utilization analysis) as required.

**4. The SPOC, for organizations whose employees and contractors have a business need to connect to and log on to an NBC-managed computer system or application, is responsible to:-**

- Coordinate local security administration activities between NBC IT Security and the assigned area of responsibility.
- Administer security on NBC-owned and managed systems, in accordance with all requirements of the NBC Rules of Behavior for SPOCs, which are completed during the SPOC assignment process.
- Submit customer requests for access to NBC IT systems or applications via NBC-approved methods (e.g., electronic or hardcopy forms, etc.) that are current at the time of the submission.
- Notify NBC IT Security when any customer employee or contractor who has access to an NBC-managed computer system terminates employment or for any other reason no longer requires access to an NBC-managed computer system.
- Participate in periodic security audits with NBC IT Security representatives to ensure that all User IDs have been assigned proper privileges (e.g., minimum access required to perform the user's duties), and that the User IDs are deleted when the users are separated, transferred, or for any other reason no longer require access to the NBC system.

**5. Whenever customer employees and contractors have a business need to access (e.g., connect to, and log on to) an NBC-managed computer system or application, customer agrees to be responsible for implementing and overseeing end-user compliance with appropriate security-related activities. For example, the customer agrees to endeavor to ensure that end-users:-**

- Use NBC-managed computer hardware, programs, and data for work-related purposes only.
- Do not share User ID or logon password with anyone at any time.
- Choose complex passwords that are difficult to guess, to minimize the risk of having the system compromised as a result of poor password selection.
- Change exposed or compromised passwords immediately.
- Contact the customer Security Point of Contact (SPOC) if problems are encountered with his/her User ID, password, or other access.
- Are personally accountable for all actions associated with the use of his/her assigned User ID.
- Lock the workstation keyboard or log off when leaving the workstation area to prevent unauthorized use of the User ID.
- Are responsible for the appropriate use and protection of sensitive information to which he/she has authorized access.
- Immediately report all computer security incidents (viruses, intrusion attempts, system compromises, etc.) to his/her SPOC.

**B: CUSTOMER-SPECIFIC REQUIREMENTS AND EXPECTATIONS RELATING TO THE NBC**

*Customer organizations with requirements for security services that exceed those which are already routinely provided with NBC-provided products should document those requirements and contact the individual within their organization who is responsible for negotiating the annual Interagency Agreement (IAA) with the NBC. IT Security services over and above those that are routinely provided will need to be included in the IAA and any necessary costs negotiated with the NBC. The cost of routinely provided security services is already included in the total dollar amount of the IAA.*

**1. NBC PRODUCTS AND SERVICES**

The following list exemplifies the most common products/services routinely provided by the NBC:

FFS	FPPS	IDEAS	CFS (Hyperion)	QuickTime	
Travel Manager	Oracle Federal Financials	Data Warehouse	FBMS	eOPF	Momentum

**2. INFORMATION SENSITIVITY**

The NBC routinely provides information security protections, controls and procedures suitable for processing, handling and disposing of Information sensitivity levels including Privacy Act, Indian Trust, Sensitive But Unclassified (SBU) and For Official Use Only (FOUO).

As noted at the beginning of this section, if customer data sensitivity requirements exceed these routinely provided security protections, controls and procedures, customers must document the specific requirements in the Interagency Agreement (IAA) between the NBC and the customer organization. Special requirements might include unique or unusual needs not normally associated with the above listed NBC products, such as:

- Special network or data isolation beyond that which currently exists.
- Special markings affixed to printed media beyond those already in use.
- Special employee security clearances above those already in place for NBC employees and contractors.
- Special disaster recovery timeframes of less than 72 hours.

V. NBC IT SECURITY POINTS OF CONTACT.

NAME	TITLE	PHONE #	FAX #	E-MAIL
June D. Hartley	OS/NBC CIO	(303) 969-7465	(303) 969-7102	June_D_Hartley@nbc.gov
Maria E. Clark	Acting OS/NBC Chief Information Security Officer (CISO)	(303) 969-5154	(303) 969-7102	Maria_E_Clark@nbc.gov
Mary H. Macleod	Acting Information System Security Officer, Denver	(303) 969-7126	(303) 969-7102	Mary_H_Macleod@nbc.gov
IT Service Center (Help Desk)	NBC Customer Service Center	(888) 269-0319 OR (303) 969-7777	(303) 969-5882	NBCDEN_ITSC@nbc.gov

VI. CUSTOMER APPLICATION RULES OF BEHAVIOR (ATTACHED).

**RULES OF BEHAVIOR FOR CUSTOMER USERS OF COMPUTER SYSTEMS AND APPLICATIONS HOSTED AND MANAGED BY THE  
DEPARTMENT OF THE INTERIOR, NATIONAL BUSINESS CENTER**

The following Rules of Behavior (ROB) apply to all customer users of applications and systems managed by the Department of the Interior (DOI), National Business Center (NBC). These ROB should be made available to all users before granting them access to an NBC-managed application system. They are intended to supplement any existing organizational ROB that might be in use by customer organizations.

**1. Applicability and Supporting Documentation**

**For customer users employed by a bureau of the DOI**, this ROB complies with OMB Circular A-130, Appendix III, and supplements DOI Departmental Manual 375, Chapter 19.

**For non-DOI customer users subject to OMB requirements**, this ROB complies with OMB Circular A-130, Appendix III, and is intended to supplement the customer organization's information security policies, standards and ROB.

**For non-DOI customers NOT subject to OMB directives**, this ROB should be considered as recommended behavior for customer users, to assist the NBC in maintaining the highest possible security protections for customer data, and for the NBC-managed computer systems hosting customer applications on behalf of all customer organizations.

**2. Universal Customer User ROB**

**2.1 User Identification**

A unique User ID is required for each individual user of an NBC-managed system or application. User IDs must never be shared between customer users. User IDs are added, changed, or deleted to NBC-managed systems or applications following receipt, by the NBC IT Security Administration Office, of an authorized e-mail request from a customer SPOC, or, in certain cases, of an authorized, signed Computer Center Access Request Form, ASC-14. Within the customer organization, application requests are routed through the customer SPOC to the NBC IT Security Administration Office. Where appropriate, application security administrators administer individual customer application User IDs.

Customer User IDs possess privileges that are tailored to the duties of the individual customer user's job and to the individual user's level of "need-to-know." Each change in access must be approved.

If duties or job requirements change, accesses no longer needed must be removed and new accesses must be requested. Supervisors are responsible for notifying the SPOC whenever such changes occur so that the user's accesses can be changed to suit the new duty or job requirements.

When employment terminates, for whatever reason (e.g., death, medical leave of absence, retirement, termination for cause, etc.), a user's access must be terminated. Supervisors are responsible for notifying the SPOC whenever a user leaves the organization, so that the user's access authorities can be removed. Under **no circumstances** may the logon account of a terminated user be given to another individual.

**2.2 Passwords**

- Are considered private and confidential. Users are prohibited from sharing the password(s) for any NBC-managed system or application with anyone.
- To minimize the risk of having the system compromised as a result of poor password selection, customer users are responsible for selecting passwords that are difficult to guess. Wherever technically supported, as many as possible of the following password selection criteria should be employed:
  - Passwords must be at least eight characters in length.
  - Passwords should contain a mix of both upper and lower case letters, except for mainframe passwords, where case is irrelevant.
  - Mainframe passwords must contain at least one numeric character (0, 1, 2, 3...9) in positions 2 through 7.
  - New (changed) passwords may not be revisions of an old password. Reuse of the same password with a different prefix or suffix (A, B, C, etc.) is not permitted.
  - Dictionary words, derivatives of User IDs, and common character sequences such as "123456" may not be used.
  - Personal details such as a spouse's name, license plates, social security numbers, and birthdays should not be used unless accompanied by additional unrelated characters.
  - Proper names, geographical locations, common acronyms, and slang should not be used.
  - If exposed or compromised, passwords must be changed immediately.

**2.3 General Customer User Responsibilities**

- Customer users are responsible for using NBC-managed computer systems and associated data for business purposes only.
- Customer users of NBC-managed systems and applications may not access, or attempt to access, data for which they are not authorized.
- Customer users are responsible for protecting the confidentiality of data associated with the NBC-managed system or application to which they have been granted access, based on the sensitivity of the data. Such data may not be given to unauthorized persons.

- Customer users should report suspected or actual security violations to their supervisor or Security Point of Contact (SPOC), and where appropriate, to the customer application security administrator.

## 2.4 SPOCs

Security Points of Contact (SPOCs) are normally designated for each customer organization. Access to customer production data is approved and controlled by the customer data owner, through the SPOC for each application or system. SPOCs are responsible for:

- Approving and coordinating all requests for customer user access to the systems or applications they control.
- Complying with the SPOC ROB, which is completed during the SPOC assignment process and returned to the NBC IT Security Administration Office.
- Implementing controls to provide reasonable assurance that:
  - ? Physical and logical access to NBC-managed systems and applications, using customer computer terminals, is restricted to authorized customer users.
  - ? Audit reports of system use, made available by the NBC, are regularly reviewed.
  - ? Computer Security Incident Response procedures are in use at the customer site for reporting incidents involving or impacting NBC-managed systems and applications.
  - ? Customer user access to NBC-managed systems and applications is properly authorized and assigned, and that segregation of duties is properly maintained.
- Reporting all suspected or actual security violations involving an NBC-managed system or application, to the NBC IT Security Administration Office.

## 3. Application-Specific Rules

Refer to this section for any application-specific ROB, for the NBC-managed application(s) approved for use by your customer organization. For any application that is not specifically listed, customer users are expected to adhere to the universal rules listed in the sections preceding this one.

### 3.1 Federal Financial System (FFS)

**FFS Users are responsible to:**

- Use the system and the data to conduct FFS application business only.
- Be personally accountable for all actions associated with the use of their assigned FFS application user ID.
- Not share their FFS user ID and password with anyone.
- Change their FFS application password at regular intervals.
- Change exposed or compromised passwords immediately.
- Not attempt to access FFS data, tables, or documents for which they are not authorized.
- Appropriately use and protect sensitive FFS information to which he/she has authorized access.
- Immediately report all computer security incidents (system and data compromises, access/password/User ID problems, etc.) to their security point of contact (SPOC).

**FFS Data Custodians/Data Owners are responsible to:**

- Ensure that the FFS ROB are made available to all FFS users in the customer organization.
- Establish in writing to the NBC IT Security Administration Office one or more individuals to serve as Security Points of Contact (SPOCs) for the FFS customer organization.
- Ensure that appropriate security access to all FFS data belonging to the customer is established and maintained in coordination with the Customer SPOC and the NBC IT Security Administration Office.

**FFS SPOCs are responsible to:**

- Administer FFS internal application security for FFS user IDs, tables, and documents.
- Approve and coordinate all FFS user requests for RACF user ID additions, changes, and deletions with NBC IT Security Administration Office.
- Review reports of security violations, audit trails, and logs generated from FFS CORE security and RACF security.
- Review reports of all customer FFS user IDs and data authorization permissions to ensure users are current to the application, with appropriate FFS data access authorizations.

### FFS Table and Document Data

- The FFS application security table (STAB) administrator controls access to FFS table and document data. Standardized FFS forms are utilized to authorize customer users access to FFS data. System activity is audited by the FFS application and appropriate action is taken by the customer FFS SPOC if improper use is detected.

### FFS Mainframe Data

- Access to FFS mainframe data is administered through the formally designated SPOC for each FFS application customer agency. Standardized security request forms or requests are utilized to authorize customer user access to FFS mainframe data (datasets, VSAM files, etc.). RACF mainframe security software audits system activity and appropriate action is taken by the customer FFS SPOC if improper use is detected.

## 3.2 Federal Personnel/Payroll System (FPPS)

**3.2.1. Auditing of customer user access and of on-line activity is tied directly to the FPPS User ID.** Users are accountable for all actions associated with the use of their assigned FPPS User ID and may be held responsible for unauthorized actions found to be intentional, malicious, or negligent. Each user must protect his/her FPPS User ID by:

- Never allowing another person to use or share his/her logon session. Because the logon session is directly associated with an individual User ID, the user is personally accountable for all actions performed with the User ID.

**NOTE:** In the process of remotely trouble-shooting a difficult customer problem over the telephone, an FPPS or other Help Desk Technician may require the employee to reveal their secret password and explain that the problem cannot be resolved via any other means. Employees who need the assistance of a Technician to solve an IT-related problem are not expected to know whether the advice or request of a Technician is valid or whether the Technician is accurately recording the problem and attempted solutions in the Help Desk log. Therefore, if the employee has any reason to question any aspects of the manner in which the Technician is handling or documenting the situation, he/she should request to speak with the Technician's supervisor before providing their secret password. In any event, if an employee does provide their secret password to the Technician as part of the problem resolution process, the employee is responsible for changing his/her secret password immediately following resolution of the problem.

**3.2.2. Customer FPPS users are responsible for adequately protecting any sensitive or Privacy Act data entrusted to them.** Users are prohibited from disclosing, without proper authorization, sensitive or Privacy Act information to individuals who have not been authorized to access the information.

**3.2.3. Casual browsing of sensitive or Privacy Act FPPS information, such as personnel data, is prohibited.** FPPS users should only access FPPS data when there is an official business reason.

## 3.3 Interior Department Electronic Acquisition System (IDEAS)

For customer organizations using this application, the universal ROB documented in Section 2 above provides adequate coverage for IDEAS.

## 3.4 Consolidated Financial Statement (CFS/Hyperion) System

For customer organizations using this application, the universal ROB documented in Section 2 above provides adequate coverage for CFS/Hyperion.

## 3.5 Travel Manager (TM) System

For customer organizations using this application, the universal ROB documented in Section 2 above provides adequate coverage for Travel Manager.

## 3.6 Electronic Freedom of Information Act Tracking System (EFTS)

The rules of behavior contained in this document are to be followed by all users of the EFTS. Users are expected to comply with this and all other DOI policies and will be held accountable for their actions while using the EFTS. Users must comply with the requirements of the Freedom of Information Act (FOIA) (5 U.S.C. 552), Privacy Act (PA) (5 U.S.C. 552a), Federal Records Act (44 U.S.C. Chapters 31 and 33), Computer Security Act (Pub L. 100-235), Government Information Security Reform Act, Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR Part 2635), and DOI's implementing regulations. The EFTS is covered by three DOI PA system of records notices: DOI-71, Electronic FOIA Tracking System and FOIA Case Files; DOI-69, FOIA Appeals; and DOI-57, Privacy Act Files (available at [http://www.access.gpo.gov/su\\_docs/aces/1999\\_pa.html](http://www.access.gpo.gov/su_docs/aces/1999_pa.html)) An employee's failure to comply with the requirements of the PA could lead to civil or criminal penalties and questions regarding suitability of the individual for that position. If an employee violates these Rules of Behavior, he or she may be subject to disciplinary action. Either the OCIO or the IT Directorate of the National Business Center (ITD/NBC) may revoke a person's system access for a specific period of time if an employee violates these Rules of Behavior. In addition, disciplinary actions may be taken in accordance with the Department's Handbook of Charges and Penalty Selection for Disciplinary and Adverse Actions, DM 752 Handbook 1, dated 6/27/01.).

Under the PA system of records notice DOI-71, DOI FOIA Officers and Coordinators in headquarters and field offices are the system managers for the data input into and maintained on the EFTS for their respective organizations. As such, they are responsible for complying with the system manager requirements under the PA and the Computer Security Act.

The EFTS application resides on a Windows 2000 server, which is behind its own firewall separated from other Departmental offices.

**Connection to the Internet** – The EFTS is accessed through the Internet and the user is governed by the following policies regarding

Internet use. Limited personal use of the Internet is governed by the Department of the Interior (DOI) Policy on Limited Personal Use of Government Office Equipment (available on the DOI home page at <http://www.doi.gov/ethics>). Briefly, this policy states that employees on non-duty time are allowed to use the Internet for personal use as set forth in and in accordance with the Internet Acceptable Use Policy (IRM Bulletin 1997-001, available on DOI home page, <http://www.doi.gov/erim/bulletins>).

**Protection of copyright licenses (software)** – The EFTS was designed and licensed as a FOIA tracking system and portions may not be downloaded or used for other purposes. There will be audits conducted on this system.

**Record Retention Requirements** - Users must follow DOI's records management policies. Any documents or e-mail created may be considered Federal records that must be preserved by being printed and filed and may not be deleted from the system before being saved in the system's backup process.

**Record Retention Requirements for Cobell v. Norton litigation** – Users must print and file, in accordance with applicable Court and Departmental directives, any documents they have or create and any electronic mail messages they send or receive, including attachments, that relate to the Three Functional Areas of:

- American Indian trust reform, including the High-Level Implementation Plan or any of its subprojects;
- The Cobell v. Norton litigation; or
- Administration of Individual Indian Money (IIM) accounts.

In addition, users must to the best of their abilities protect any files or data related to individual Indian trust data from unauthorized access.

**Unofficial use of government equipment** - Users should be aware that the DOI Policy on Limited Personal Use of Government Office Equipment governs personal use of information resources (e.g., computers, printers, e-mail, Internet, etc).

**Unique user name** – Each person logging onto the system will have a unique user name.

**Use of passwords** - Users are to establish and maintain passwords of a length specified by the EFTS system administrator. The user's password should consist of a mix of 8 characters—uppercase, lowercase, and a number or other character, e.g., Ap7ples# or 1Ap7ples.

**System privileges** - Users are given access to the EFTS based on a need to perform specific work. Users are to work within the confines of the access allowed and are not to attempt access to systems or applications to which access has not been authorized.

**Individual accountability** - While using the EFTS, users will be held accountable for their actions. If an employee adversely impacts the operation of the EFTS, OCIO/NBC may remove the employee's access without notice to ensure the operation and availability for the rest of DOI.

**Restoration of service** - The availability of the EFTS is a concern to all users, and the NBC will endeavor to ensure that the system is available at all times during normal working hours. However, Bureaus and Offices are responsible for ensuring that they are able to provide critical services in the event the system is unavailable in accordance with continuity of operation plans. In addition, users are asked to cooperate with the systems management staff during outages, so that service can be restored for all users in a timely manner.

#### 4. Consequences for Non-Compliance with these ROB

The consequences of Federal employee or contractor behavior not consistent with these rules may result in revocation of access to the associated NBC-managed system or application, and wherever such actions may be applicable, disciplinary action consistent with the nature and scope of the infraction may be applied.

## Statement of Work

8-6620-FFS-NRC-28

Service A - Financial Mgmt Sys Supt. Implement/Convert (IMP).Financial Asslst Sys

- Implementation and Conversion

Activity	Hours/Units	Amount
<b>PROCESS TEMPORARY DUTY TRAVEL VOUCHERS</b>	Fixed	\$25,000.00
<ul style="list-style-type: none"> <li>• Perform work taskings necessary to transition temporary duty (TDY) and permanent change of station (PCS) travel payment processing to the NBC. Services can include travel and payroll costs for client site visits, obtaining access to client system, obtaining proper delegations, meetings and conferences between client client and the NBC prior to implementation date, and any other items inherent to the successful migration of cross-serviced tasks within established timeframes.</li> </ul>		
<b>Service A - Total</b>		<b>\$25,000.00</b>

## Statement of Work

8-6620-FFS-NRC-28

Service B - Accounting Ops. Financial Trans Processing. TDY Travel

- Accounting Ops. Financial Trans Processing. TDY Travel

Activity	Hours/Units	Amount
<b>PROCESS TEMPORARY DUTY TRAVEL VOUCHERS</b>	Fixed	\$65,000.00
<ul style="list-style-type: none"><li>Record and maintain transactions for temporary duty (domestic and foreign) travel payment processing in client agencies financial system, with proper internal controls and segregation of duties. Audit and certify travel payments in accordance with client policy and federal travel regulations. Certify client agency travel payments with Treasury. Respond to and resolve traveler questions concerning payments. Perform periodic reviews of financial transactions to ensure correctness.</li></ul>		
<b>Service B - Total</b>		<b>\$65,000.00</b>

## Statement of Work

8-6620-FFS-NRC-28

Service C - Accounting Ops. Financial Trans Processing. PCS Travel

- Accounting Ops. Financial Trans Processing. PCS Travel

Activity	Hours/Units	Amount
<b>PROCESS PERMANENT CHANGE OF STATION TRAVEL VOUCHERS</b>	Fixed	\$15,000.00
<ul style="list-style-type: none"> <li>Record and maintain transactions for permanent change of station travel payment processing in client agencies financial system, with proper internal controls and segregation of duties. Serve as relocation coordinators, calculate relocation income tax allowance and prepare and send W-2s to travelers. Audit and certify travel payments in accordance with client policy and federal travel regulations. Certify client agency travel payments to Treasury. Respond to and resolve traveler questions concerning payments. Perform periodic reviews of financial transactions to ensure correctness.</li> </ul>		
<b>Service C - Total</b>		\$15,000.00





Department of the Interior  
National Business Center

## **Proposal to Provide Accounting Operations Services**

December 11, 2007

Prepared for:

U. S. Nuclear Regulatory Commission





---

TABLE OF CONTENTS

1. INTRODUCTION ..... 3  
2. ACCOUNTING SYSTEM ..... 3  
3. ACCOUNTING OPERATIONS SERVICES ..... 3  
    3.1 Payment Services.....3  
    3.2 Other Considerations.....5  
    3.3 Conversion of Processing to NBC.....6  
4. COST PROPOSAL..... 6  
    4.1 Accounts Receivable Cost Estimate ..... 6  
    4.2 Conversion Cost Estimate..... 7



## 1. INTRODUCTION

The Department of the Interior's National Business Center (NBC) is pleased to submit our proposal for providing travel payment services to the US Nuclear Regulatory Commission (NRC). The NBC proposes a comprehensive service solution as defined in detail in section 3 of this proposal.

The NBC has over twenty years of experience cross-servicing administrative systems for Federal agencies. Approximately twenty-one of NBC's current clients are receiving fiscal operations support, similar to the services the NRC is considering cross-servicing to the NBC.

The NBC will assign an experienced program manager who will be responsible for the overall execution of the project. The program manager will ensure that the NRC's expectations are met or exceeded and will keep management informed of the project status.

## 2. ACCOUNTING SYSTEM

The NRC will provide the designated NBC accounting staff appropriate access to the NRC's accounting system. All transactional data processed by the NBC will be in NRC's accounting system.

## 3. ACCOUNTING OPERATIONS SERVICES

### 3.1 Travel Payment Services

Travel payment-related services (Permanent Change of Station and Temporary Duty) being offered by the NBC to NRC include the following:

- **Receipt of Travel Vouchers.** The NRC will notify all employees designating the NBC as the paying office. The NBC accounting staff will receive travel vouchers from the NRC. All travel vouchers will be date stamped.
- **Tracking of Travel Vouchers.** The NBC accounting staff will enter travel vouchers, within 2 business days, into a travel log.
- **Vendor Information.** The NBC accounting staff will query NRC's accounting system for valid vendor record. If employee is not in the accounting system or an



update to the vendor record is required, the NBC accounting staff will update or change the vendor data in the accounting system.

- **Obligations.** The designated NRC personnel will obligate travel documents and will send to the NBC accounting staff a copy of all obligating documents. The NBC will maintain a log and file of all obligation documents. During the conversion stage when NBC will need a copy of all outstanding obligations, a hard-copy or scanned copy of the obligating documents will be acceptable.

**Matching of Voucher to the Obligation.** Upon receipt of a travel voucher, the NBC accounting staff will query the NRC's accounting system for a valid obligation. If obligation exists and sufficient funds are available on the obligation, the NBC will process the voucher referencing the obligation. If an obligation does not exist or the obligation does not have sufficient funds available to process the voucher, the NBC will contact the appropriate NRC personnel for a valid obligation or a modification to an existing obligation, to be entered into the NRC accounting system and to provide a copy of the obligation. The NBC accounting staff will not make payment in the NRC accounting system on any travel voucher that does not have a valid obligation with sufficient funds available.

- **Approval of Voucher.** The travel voucher will be matched to the proper obligating document by the NBC accounting staff.
- **Schedule of Payment to Treasury.** The NBC accounting personnel will process the daily listing of certified payments scheduled to be paid to Treasury.
- **Payment Certification to Treasury.** The NBC will certify payments with Treasury on the Secure Payment System (SPS).
- **Unallowable Expenses.** The NBC accounting staff will be responsible for notifying and working with employees on resolution of unallowable expenses. On occasion, the NBC accounting staff may need NRC's assistance in the resolution.
- **Year End PCS Reporting** After calendar year-end, NBC will send RITA packages to eligible employees. All employees with PCS vouchers will receive a summary of taxable and non-taxable income.



- **PCS Travel Forms.** After processing a PCS voucher or a payment to a moving company for shipment or storage of household goods, NBC will send three documents to the traveler: Notice of Action, PCS Form 3-255 and a copy of the payroll memorandum. NRC to notify travelers of the change to these three standard forms.
- **Travel Payments.** All travel voucher rejects will be identified by the NBC and NBC staff will contact the responsible NRC offices for resolution. Temporary Duty (TDY) travel vouchers will be processed within seven business days. Permanent Change of Station (PCS) travel vouchers will be processed with 20 business days. PCS vouchers are paid through the NRC accounting system and taxable and nontaxable amounts are sent to payroll operations for any tax adjustments and Form W-2 reporting. Vouchers received after payroll operations calendar year-end cutoff are audited and ready for processing in January.
- **Other Payment-Related Items**
  - Government Bills of Lading (GBLs) receipt, review, and payment will also be performed by the NBC. All travel payments are to be 100% audited prior to payment. Payments returned by Treasury and any erroneous payments will be handled by the NBC. Any excess weight charges billings will be sent to the employee by NBC.

### 3.2 Other Considerations

- **Work Count Estimates.** This proposal was based on the following annual work count estimates provided by the NRC:
  - **TDY Travel:** 19,000
  - **PCS Travel:** 500
- **Internal Controls.** The NBC will ensure that there are relevant internal control standards, including adequate segregation of duties. This will be validated by the annual NBC A-123 and SAS-70 audits and a Statement of Assurance to this effect will be sent annually by the Chief Financial Officer of the NBC.
- **Audit Assistance.** The NBC accounting staff will work with NRC personnel and auditors to provide documentation and answer questions on transactions made by the NBC accounting staff. The NBC will provide to NRC auditors' copies of all



requested documents requested on the provided-by-client (PBC) list within 2 working days of auditors' request.

- **Records Management.** The NBC accounting staff will maintain an orderly filing system, ensuring compliance with all record retention requirements in accordance with NARA standards. Develop or update written policies and procedures.
- **Communications.** The NBC and NRC will establish regularly scheduled meetings to discuss issues for the services covered in this proposal.

### 3.3 Conversion of Processing to NBC

- **Accounting and Finance Conversion.** The NBC staff will learn NRC's business processes and work closely with NRC personnel on transition of the work to the NBC. To obtain the training and to learn NRC business processes, NBC personnel will travel to the NRC accounting office within 30 days prior to conversion.
- **Processing Procedures.** The NBC has formally documented standard accounting procedures. Unique aspects of NRC's travel accounts payable processing will be formally documented by the NBC, within 90 days after the interagency agreement is signed.
- **Phased Approach.** The NRC has expressed a desire to transition fiscal services in a phased approach:
  - **January 1, 2008.** All Travel Payments (TDY and PCS).
  - **March 1, 2008.** Intra-governmental Payments (IPAC).
  - **May 1, 2008.** Commercial Payments.

This proposal only addresses the first phase (travel payments).

## 4. COST PROPOSAL

### 4.1 Accounting Operations Services Cost Estimate

The NBC Accounting Operation's reimbursable support agreement for Accounting Operations Services with the NRC will be fixed price and is estimated as follows:



Function	Monthly Cost	Annual Cost
Travel Payments (TDY and PCS)	\$ 40,000	\$ 480,000
Total	\$ 40,000	\$ 480,000

As the above is an estimate and includes records management and oversight/supervision/project management costs. There may be necessary negotiated adjustments in subsequent interagency agreements, up or down, once the overall business process has been in place and operating smoothly. Should significant differences be realized between estimated and actual work counts, subsequent interagency agreements will reflect these variances. Any changes to the Standard Service Level Agreement may result in changes to the cost estimate. This estimate is based on our understanding of the level of service that has been presented to us by the NRC. Should changes in specific requirements be identified after acceptance of the proposal, the scope and cost of the proposal could change.

#### 4.2 Conversion Cost Estimate

The NBC Accounting Operation's reimbursable support agreement for the one-time costs to convert processing from NRC to the NBC will be based upon fixed price as follows:

Function	Estimated One-Time Cost
Training/Business Process Review/Procedures/Equipment	\$15,000
Travel Cost	10,000
Total Conversion Costs	\$25,000

**SERVICE LEVEL AGREEMENT**  
**BETWEEN THE**  
**NATIONAL BUSINESS CENTER**  
**DEPARTMENT OF THE INTERIOR**  
**AND**  
**NUCLEAR REGULATORY COMMISSION**

**FINANCIAL MANAGEMENT SYSTEMS AND OPERATIONAL SUPPORT SERVICES**

**FOR FISCAL YEARS: 2007 and 2008**

---

## **FINANCIAL MANAGEMENT SYSTEMS AND OPERATIONAL SUPPORT SERVICES**

### **I. STATEMENT OF LEGAL AUTHORITY**

The National Business Center (NBC), Office of the Secretary, Department of the Interior agrees to provide services and/or product support as outlined below to the Selective Service System pursuant to authority 43 U.S.C. § 1467 and 1468, which established the Department of the Interior Working Capital Fund. Other authorities under which the NBC operates include the Economy Act, 31 U.S.C. 1535.

### **II. PURPOSE**

The purpose of this document is to identify the services and support provided to the customer by the NBC with regard to financial management systems and operational support services. (See Section IV below for the specific services to be provided). This SLA also establishes service levels and metrics, monitoring methods, and organizational responsibilities as applicable.

### **III. PERIOD OF PERFORMANCE**

This SLA becomes effective upon signature by all parties of the corresponding Inter/Intra Agency Agreement (IAA). The IAA is issued to fund the specific services identified in this document. This SLA will remain in effect until the IAA is amended, replaced, or terminated by signed or mutual agreement of both organizations. The IAA that provides funding for the services must be renewed annually to ensure continuation of services.

### **IV. LIST OF SERVICES**

The NBC offers an array of core financial accounting and business management systems and operational support services. These products and services meet all U.S. Treasury, Office of Management and Budget, Government Accountability Office, and Comptroller General policies and regulations with regard to information technology operations and security, accounting practices, generally accepted accounting principles and standards (GAAP), and internal and management controls.

Following is a listing of financial and business management services offered by the NBC. The items checked are the specific services that will be provided to the customer under the IAA and this supporting SLA.

**A. FINANCIAL MANAGEMENT SYSTEMS – OPERATIONS AND MAINTENANCE**

	Administration, operation, and maintenance of core financial accounting systems and supporting management systems, including application hosting, on-line and off-line storage, operating system backups, system security, printing capability, review, testing and installation of software fixes, patches and updates, Help Desk support, and disaster recovery
	Federal Financial System (FFS)
	Oracle Federal Financials
	Momentum Financials
	Hyperion
	eTravel
	Quarters
	NIMS
	Other:
	System file management consultation
	Daily, monthly, annual processing of scheduled jobs
	Report production
	System file management and maintenance
	Application security
	Client unique telecommunication support
	Other telecommunication services, such as advice and support regarding capacity, equipment, encryption, backups, etc.

**B. FINANCIAL MANAGEMENT SYSTEMS – IMPLEMENTATION**

	Implementation of a Financial Systems Integration Office-certified financial accounting system (e.g., Oracle Federal Financials, Momentum Financials, mySAP, Hyperion)
	Requirements analysis
	Business process reengineering
	Conversion and implementation support
	Custom report specification writing and programming
	Development and implementation of value-added applications, e.g., fixed assets, procurement, etc.
	Development and implementation of interfaces, e.g., bank card, eTravel, payroll or custom interfaces
	Development of documentation, policies, and procedures
	e-Travel software implementation, including development of an interface to the core accounting system
	Implementation of Momentum Acquisitions.
	Implementation of Oracle iProcurement and Procurement Contracts.

	Interior Department Electronic Acquisition System, Procurement Desktop (IDEAS-PD) implementation, including development of an interface between IDEAS-PD and the accounting system
	Data Warehouse – design, implement, and maintain a data warehouse for ad hoc query and reporting purposes
	System training
	System testing
	Consulting services
	Other systems implementations (e.g. Maximo, Portal, Dashboard, etc.)

### C. ACCOUNTING OPERATIONS SERVICES

	<p>Administrative Control of Funds and Accounts Payable</p> <ul style="list-style-type: none"> <li>○ Record commitments, obligations, reserve funds, receipt of goods and services, and payroll accruals, as applicable</li> <li>○ Maintain vendor payment files</li> <li>○ Process vendor and other payments/disbursements in accordance with Prompt Payment regulations</li> </ul>
	<p>Temporary Duty (TDY Travel)</p> <ul style="list-style-type: none"> <li>○ Determine entitlements, compute advances, pay vouchers, monitor outstanding advances, certify customer's travel payments with Treasury, and audit selected sample of vouchers</li> <li>○ Respond to and resolve vendor and traveler questions concerning payments</li> </ul>
	<p>Permanent Change of Station (PCS) Travel</p> <ul style="list-style-type: none"> <li>○ Determine entitlements, compute advances, pay vouchers, monitor outstanding advances, certify customer's travel payments with Treasury, and audit selected sample of vouchers</li> <li>○ Respond to and resolve vendor and traveler questions concerning payments</li> </ul>
	<p>Accounts Receivable/Reimbursements/Central Collections Processing</p> <ul style="list-style-type: none"> <li>○ Prepare and/or process Intra-Governmental Payment and Collection (IPAC) billings</li> <li>○ Manage collection program, to include Bills of Collection, Dunning Notices for delinquent debts, Treasury Offset Program, Salary Offset indebtedness; Write-Offs (uncollectible debts)</li> <li>○ Respond to and resolve issues concerning collections</li> </ul>
X	<p>General Accounting</p> <ul style="list-style-type: none"> <li>○ Reconcile general ledger subsidiary transactions and research abnormal general ledger balances</li> <li>○ Reconcile Fund Balance with Treasury</li> <li>○ Perform miscellaneous reconciliations (i.e., electronic interfaces to the core accounting system)</li> <li>○ Monitor funds availability within the customer financial system</li> <li>○ Prepare and analyze customer's regulatory reports within prescribed due dates</li> <li>○ Record all necessary transactions for amounts due the government</li> </ul>

	<ul style="list-style-type: none"> <li>○ Perform appropriated, reimbursable, and trust accounting function, using the Standard General Ledger</li> <li>○ Prepare and analyze mandatory and/or ad-hoc reports as required by regulatory agencies and/or the customer</li> <li>○ Maintain customer's accounting history in compliance with records retention requirements</li> <li>○ Provide training of payment rules and regulations to customer, upon request</li> <li>○ Perform financial analyses</li> <li>○ Perform operational activities associated with the year-end accounting cycle closing</li> </ul>
<b>X</b>	<p>Financial Statement Preparation and CFO Activities</p> <ul style="list-style-type: none"> <li>○ Maintain all financial supporting documentation in accordance with NARA standards</li> <li>○ Prepare all required CFO compliant Financial Statements including accompanying footnotes and supplementary information</li> <li>○ Prepare and submit the Treasury Report of Receivables</li> <li>○ Monitor, reconcile, and report Cash/Fund Balance with Treasury in accordance with US Treasury Standards (SF-224)</li> <li>○ Reconcile data in financial statements to the accounting system</li> <li>○ Provide information to and perform reconciliation of intra-governmental transactions per the client's requirements</li> <li>○ Support audit and internal control processes</li> </ul>

**D. E-APPLICATIONS SERVICES**

	<p>Web Application Development</p> <ul style="list-style-type: none"> <li>○ Provide project management, system analysis, and design with an emphasis on functional and security requirements, source code development, system testing, quality assurance, and implementation and post production support</li> </ul>
	<p>Web Design and Implementation</p> <ul style="list-style-type: none"> <li>○ Design and implement new websites and web pages.</li> <li>○ Implement and adhere to industry best practices.</li> <li>○ Post new or updated content provided by the information owner.</li> <li>○ Perform routine website maintenance including monitoring of orphan files and dead links</li> </ul>
	<p>Web Application and Website Hosting</p> <ul style="list-style-type: none"> <li>○ Administration, operation, and maintenance of an application, including application hosting, on-line and off-line storage, operating system backups, system security, printing capability, installation of approved and funded software fixes, technical analysis, physical and systems security, firewall security, use of intrusion detection software, administration of all software on the server, monitoring of feedback messages received from the Web site, and backup and disaster recovery</li> </ul>

## **V. RESPONSIBILITIES**

### **A. CUSTOMER RESPONSIBILITIES**

- Provide knowledgeable contacts to respond to questions related to services provided by the NBC.
- Acquire and install remote (peripheral) hardware as needed to access NBC systems and complete required Interconnect Security Agreement with the NBC prior to system implementation.
- Ensure compliance with NBC specific security requirements, including the requirement to install encryption software on the desktop of each customer user with access to any NBC system or application.
- Retain ownership and control of financial data contained in the accounting system.
- Prepare and maintain a Business Recovery Plan that identifies how the customer will resume operations of its business functions should a disaster at the customer's facility occur. The plan shall specifically address where the customer organization will be relocated and replacement of customer-provisioned network circuits to the NBC and NBC hot site.
- Participate, as mutually agreed upon, in annual testing of the financial system disaster recovery plan at the NBC hot site.

### **B. NBC RESPONSIBILITIES**

- Protect system data in accordance with applicable laws, regulations, guidelines, and Department of the Interior security requirements.
- Disclose the customer's financial data only to authorized personnel as instructed in writing by the customer.
- Assure that the security for systems hosted by the NBC is compliant with Federal Information Technology (IT) security requirements, including certification and accreditation (C&A), and Federal Information Security Management Act (FISMA) reporting. NBC will ensure that a C&A is performed as required every three years and/or when major changes/upgrades are conducted. NBC will also make the C&A documentation available to customers for review at a designated NBC location.
- Provide a copy of both the certification and accreditation letters for systems hosted at the NBC from the NBC Designated Approving Authority.
- On an annual basis, ensure that an independent third party conducts a Statement on Auditing Standards (SAS) No. 70 review of the major financial systems (e.g., FFS, FPPS, Oracle, Momentum, mySAP, Hyperion) hosted by the NBC. The SAS 70 review is an auditing standard developed by the American Institute of Certified Public Accountants (AICPA) and indicates the NBC's compliance with IT control objectives and activities as examined by an independent accounting and auditing firm.
- Conduct testing at the transaction level in compliance with OMB Circular, A-123, Appendix A for those customers for which the NBC performs financial transactions processing.

- Provide required financial, internal control, and FISMA certifications and assertions as required by OMB for the customer's annual financial statement assurance, including copies of applicable SAS 70 reviews. In mid-July, the NBC will provide assurances over financial reporting; this assurance will include the results of the SAS 70 and FISMA reviews, as well as applicable financial transactions testing. In mid-October, the NBC will provide assurances over program internal controls.
- Provide competent, trained, and certified staff and management for systems and services to be provided.
- Provide a Help Desk to respond to questions from clients that are related to services provided by the NBC.
- Provide support to the customer in response to audit findings related to NBC-provided services.
- Prepare and maintain a Business Recovery and Continuity of Operations plan and perform annual testing of the plan.
- Notify customers by telephone and/or email within 4 hours in the event of a disaster or other contingency that disrupts the normal operation of any hosted system.

## **VI. PERFORMANCE MEASUREMENT**

The NBC has identified measures of performance for the financial and business management systems and services provided to customers. These metrics are identified in this SLA. Many of these measures have been identified by the Office of Management and Budget or the Department of Interior as a necessary part of meeting the President's Management Agenda or other applicable financial laws and regulations. Others have been designated as the NBC's planned service levels to ensure high product quality services to customers. See Attachment A for the performance measures and service levels applicable to the customer.

## **VII. SECURITY**

Security roles, responsibilities, and procedures related to this document are defined in the Security Services Advisory (SSA) that is provided as a separate document to the customer if required. If there are no special security roles, responsibilities, and procedures related to the services to be provided to the customer by the NBC, then the SSA will not be necessary.

An Interconnect Security Agreement (ISA) is established between the NBC Information Technology Services Line of Business and non-DOI customers having a computer system or network interconnected with the NBC. The technical details of the interconnection are documented in the ISA. The parties agree to work together to develop the ISA, which must be signed by both parties before the interconnection is activated. Proposed changes to either the system or interconnecting medium by either the customer or NBC must be reviewed and evaluated to determine the potential impact on the interconnection. The ISA will be renegotiated before such changes are implemented.

## **VIII. FUNDING**

Under the provisions of the Economy Act, the NBC is required to recover all direct and indirect costs for services provided. The official funding document that supports this SLA is the IAA. On an annual basis, both parties will approve funding to ensure continuation of services by signing an IAA. Failure to sign the IAA in a timely manner may result in a discontinuation of services by the NBC. The NBC will bill the customer on a monthly basis for time and materials agreements and on a quarterly basis for fixed price agreements unless otherwise specified in the IAA.

This SLA is neither a fiscal nor a funds obligation document. Nothing in this SLA authorizes nor is intended to obligate either the customer or the NBC to expend, exchange, or reimburse funds, services, or supplies; transfer or receive anything of value; or enter into any contract, assistance agreement, interagency agreement, or other financial obligation. This SLA is strictly for the NBC and the customer's internal management purposes. This SLA is not legally enforceable and shall not be construed to create any legal obligation on the part of either party. This SLA shall not be construed to provide a private right of action for or by any person or entity.

## **IX. TERMINATION CLAUSE**

Termination provisions are included in Block 10 of the IAA. The IAA and SLA may be terminated before the end of the performance period by providing at least 180 calendar days written notice from either party or by mutual agreement between the parties. The customer is responsible and will be billed for all costs incurred until the time of termination. If either or both parties terminate the IAA pursuant to Block 10 of the IAA, this SLA shall be considered to be terminated automatically on the date that the IAA is terminated.

## **X. DISPUTE RESOLUTION**

Issues unable to be resolved informally between the NBC and the customer will be handled as follows:

- Either party may submit a formal request in writing to the other party. The formal request will be elevated internally to the appropriate management level for review/concurrence. The parties then have 60 days to reach an agreed upon resolution to the dispute. If the issue warrants immediate attention such as for security incidents or events impacting sensitive or personally identifiable information (PII), it will be resolved with urgency.
- In the event those officials cannot resolve the dispute within 60 days, they will designate a mutually acceptable, independent third party to review the facts and recommend a fair resolution. This independent third party must define the recommended resolution within 60 days, which both disputing parties agree to accept, with a suggested timeframe for implementation of said resolution. The costs for the third party review will be paid equally by the NBC and customer.

**XI. APPROVAL**

This SLA accompanies the IAA and is considered mutually binding for the NBC and the customer.

**PERFORMANCE MEASURES  
FINANCIAL SYSTEMS AND ACCOUNTING OPERATIONS SERVICES**

*The items checked below are the specific measures and metrics that will be provided to the customer under this service level agreement (SLA) which supports the Inter/Intra Agency Agreement (IAA).*

	<b>MEASURE</b>	<b>PERFORMANCE METRIC</b>
	Application Availability	Production system is available 24/7/365 except during established periods of maintenance, pre-approved downtime, and downtime requested by the customer, 99% of the time.
	Application Performance	Average internal system response time is 3 seconds or less from the time a new transaction enters the NBC internal network until the point of egress from the hosting center internal perimeter, 95% of the time. Latency caused by internet, intranet, or dial-up connections is not factored into transaction response times as they are outside of the scope of control of the NBC.
	Application Access	Users will be granted access to the application within 3 business days of request, Monday through Friday, excluding Federal holidays, 99% of the time.
	Help Desk Support	The NBC Help Desk responds to calls during hours of operations (8:00 a.m. to 8:00 p.m. ET). Provides Level 1 Help Desk to respond to questions and problems related to services provided by the NBC, 95% of the time. Severity 1 - 15 minutes (system down) Severity 2 - 2 hours (business impacted, workaround exists) Severity 3 - 8 hours (minimal impact on operations)
	Website Updates	95% of requests are processed within 4 business hours of confirmation of the detailed requirements. Confirmation may determine that more than 4 business hours are required to process the website update.
	eTravel System	eTravel interface will be available and functioning during contracted hours, excluding vendor downtime, 95% of the time.
	Quarters	95% of regional rental rate survey reports are issued 60 calendar days after survey data is collected with no significant errors. Housing training classes are provided annually in each of the regions surveyed during the past year. Assurance that students' training objectives were satisfied is measured by training evaluation forms. Training classes have a 90% satisfaction rate. NBC staff provides correct answers, courteous help, and useful and production information to user calls and information requests. Calls are answered within 24 hours, 95% of the time.

MEASURE	PERFORMANCE MEASURE
NIIMS	95% of billings are generated on or before the requested process date with end user authorization and concurrence and without reruns.
	95% of reports are made available in the INFONIIMS (DocDirect) repository within 2 business days of the scheduled run.
	80% of accounts are reconciled among NIIMS, FFS, and the Department of Treasury on a daily basis. A log is kept updated with dates when an out-of-balance condition cannot be explained by a timing issue.
	95% of demand letters are created and mailed on a monthly basis
	95% of referrals are done on a regularly scheduled basis of once monthly.
	NIIMS database is updated with status of referrals on a timely basis, 85% of the time.
TDY Vouchers	95% of travel vouchers are paid within 5 business days for automated vouchers (e.g., Travel Manager, e-Travel) and within 7 business days for paper vouchers. Travel vouchers are returned after the 7th business day if proper information (such as ACH, proper account code, proper signatures, etc.) has not been received to process payment.
PCS Vouchers	98% of obligations are posted in the accounting system within 5 business days. 98% of payments are processed within 20 business days.
Vendor Payments (Domestic Non-Federal)	98% of vendor payments are processed in accordance with the Prompt Payment regulations upon timely receipt of valid documentation.
Vendor Payments (Federal IPAC)	98% of vendor payments are processed within 10 business days and in accordance with Treasury standards for Statement of Differences (none over 6 months old).
Interest Paid	Interest paid does not exceed 3% of total applicable monthly payments provided supporting documentation is received timely.
Billings and Collections	Collections are processed in accordance with billing documentation 98% of the time.
Suspense Accounts	98% of suspense transactions are researched and posted to the appropriate obligating document within 30 calendar days after deposit in suspense.
Percentage of Payments by EFT	98% of invoices are paid by electronic funds transfer.
Regulatory Reporting	100% of all regulatory reports are submitted in accordance with customer deadlines and/or Treasury schedules.
Eliminations	100% of eliminations are reported quarterly by the end of the month following the end of the quarter.
Debt Referral	95% of outstanding debt is referred to Treasury in accordance with customer deadlines and/or Treasury schedules.
Outstanding Debt	100% of debt greater than two years is reclassified or written off. Aging of outstanding debt by dollar amount and number of transactions categorized as 1-2 years and greater than 2 years as reported on the quarterly Treasury Report on Receivables (TROR).
General Ledger	100 % of general ledger accounts (e.g., Fund Balance with Treasury, SF 224, etc) are reconciled monthly or quarterly or in accordance with customer deadlines and/or Treasury deadlines.

MEASURE	PERFORMANCE METRIC
General Ledger (Property)	100% of general ledger accounts reconcile to subsidiary property systems by year end.
IRS Form 1099's	100% of paper 1099 forms will be delivered to customers within IRS prescribed deadlines. Electronic files are sent to regulatory authorities within the prescribed deadlines.
Undelivered Orders (UDO)	100% of UDOs are validated and adequately documented.
Comparison of Budgetary to Proprietary Accounts	100% of accounts are reconciled and resolved with the exception of parent/child relationships.
Abnormal Balances	100% of abnormal balances at the Hyperion Adjusted Trial Balance level are reconciled.
Variance Analysis	100% of significant variances are supported or corrected on all general ledger accounts.
Fund Balance with Treasury	Total cash balances are reconciled to Treasury to ensure that differences are less than \$10 million monthly and less than \$1 million at year end. 100% of corrections are posted within 30 days.
Unreconciled Cash Balances	100% of Statements of Differences are reconciled within 6 months