

AWARD OF INTERAGENCY AGREEMENT

4. AGENCY LOCATOR NO. 31000001	5. B & R NUMBER 9-7N-15-5H1363 ✓
7. JOB CODE N7152 ✓	8. APPROPRIATION SYMBOL 31X0200
9. BOC 253A ✓	10. DOCUMENT IDENTIFICATION NUMBER RQ CFO 09 383
11. NAME AND ADDRESS OF SERVICING AGENCY Department of the Interior/National Business Center 7301 W. Mansfield Ave. MS D2705 Attention: Agreements Denver, CO 80235-2230	

6. ISSUED BY
**U.S. Nuclear Regulatory Commission
T 9 E 2 Division of the Controller
Washington DC 20555**

MS2683

SEP 16 2009

PROJECT MANAGER
Mary Matheson

12. JOB CODE TITLE DOI/NBC Accounts Payable Services	13. AGREEMENT PERFORMANCE PERIOD	
	BEGIN 04/01/2009	END 12/31/2009

14. OBLIGATION AVAILABILITY PROVIDED BY	
A. THIS ACTION	\$ 90,000
B. TOTAL PLACED PRIOR TO THIS ACTION WITH THE PERFORMING ORGANIZATION UNDER THIS JOB CODE FOR THIS FISCAL YEAR	\$ 1,276,500
C. TOTAL ORDERS TO DATE FOR THIS JOB CODE FOR THIS FISCAL YEAR	\$ 1,366,500
D. TOTAL ORDERS TO DATE FOR THIS AGREEMENT	\$ 2,107,500

15. ATTACHMENTS

THE FOLLOWING ATTACHMENTS ARE MADE A PART OF THIS AGREEMENT

STATEMENT OF WORK

ADDITIONAL TERMS AND CONDITIONS

OTHER (Specify) NBC Form IA

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
Modification due to the increase in IPAC document processing

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

ENERGY REORGANIZATION ACT OF 1974, AS AMENDED OTHER (Specify)

THE ECONOMY ACT OF 1932

THE CLINGER-COHEN ACT OF 1996

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

21. ESTIMATED COST FOR FULL PERFORMANCE OF THIS AGREEMENT					
FY 2008	FY 2009	FY	FY	FY	TOTAL
\$ 741,000	\$ 1,366,500	\$	\$	\$	\$ 2,107,500

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.

FUNDS CERTIFICATION OFFICIAL (Typed Name) SIGNATURE DATE

Virginia Bolding *Virginia Bolding* **9/14/2009**

23. SIGNATURES

NRC ISSUING AUTHORITY (Typed Name and Title) J.E. Dyer, CFO	SIGNATURE <i>J.E. Dyer</i>	DATE 9/14/09
SERVICING AGENCY OFFICIAL/DESIGNEE (Typed Name and Title) See attached NBC form	SIGNATURE	DATE

FULL NAME		ADDRESS
TELEPHONE NUMBER	FACSIMILE NUMBER	
E-MAIL ADDRESS		

ADMINISTRATIVE:

FULL NAME		ADDRESS
TELEPHONE NUMBER	FACSIMILE NUMBER	
E-MAIL ADDRESS		

OTHER AGENCY'S CONTACTS:

TECHNICAL:

FULL NAME		ADDRESS
TELEPHONE NUMBER	FACSIMILE NUMBER	
E-MAIL ADDRESS		

ADMINISTRATIVE:

FULL NAME		ADDRESS
TELEPHONE NUMBER	FACSIMILE NUMBER	
E-MAIL ADDRESS		

BILLING INFORMATION: To receive reimbursement under this agreement, forward to NRC on a (check one):

monthly quarterly other _____ basis, an original and three copies of Standard Form

1081 in accordance with the Treasury Fiscal Requirements Manual, Bulletin No. 78-09, or, if possible, bill monthly through the OPAC system. Send reimbursement requests to the following address:

Payment Policy and Obligations Team
 Mail Stop: T-9 F30
 Division of Financial Services
 Office of the Chief Financial Officer
 U.S. Nuclear Regulatory Commission
 Washington, DC 20555-0001

Any NRC funds remaining unexpended at the end of a fiscal year may be carried over into future fiscal years unless otherwise notified by NRC.

REPORTING REQUIREMENTS: Submit reports to the NRC in accordance with the statement of work. Submit financial status reports on a (check one):

monthly quarterly other _____ basis. These reports shall contain a brief letter status

which summarizes the expenditure of NRC funds. This report shall address the following categories, as applicable: (1) staff effort; (2) travel; (3) equipment and supplies; and (4) subcontract costs. Each report shall include by category: (a) costs for the previous month; (b) cumulative costs and uncosted obligations to date; and (c) projections for the remainder of the NRC obligated funds. The first monthly report shall provide the initial projections, and subsequent reports shall either indicate revised projections or indicate "no change in the cost and uncosted expenditure projection."

Submit these reports to the NRC Technical Contact by the 20th day of the month following the reporting period.

TERMINATING THE AGREEMENT: This agreement may be unilaterally terminated by either party generally upon 30 days' written notice to the other party. NRC will pay its share of any project expenses up to the termination date. Any expenses incurred in terminating this agreement will be paid by the party terminating the agreement. Any unexpended funds shall be returned to the NRC.

**IPAC Transaction Activity
FY 2008 - FY 2009**

Type	FY	FM	2008		FM	2009	
			Dollar Amount	Count		Dollar Amount	Count
PAY	2008	01	-\$10,505,990	290	01	-\$14,043,524	360
PAY	2008	02	-\$10,091,758	320	02	-\$12,108,476	367
PAY	2008	03	-\$11,316,349	305	03	-\$12,993,132	376
PAY	2008	04	-\$11,108,392	342	04	-\$12,120,732	367
PAY	2008	05	-\$10,418,846	313	05	-\$11,290,921	376
PAY	2008	06	-\$14,210,098	331	06	-\$14,686,232	426
PAY	2008	07	-\$12,358,516	336	07	-\$15,754,781	410
PAY	2008	08	-\$11,866,017	337	08	-\$13,793,350	424
PAY	2008	09	-\$13,160,543	370	09	-\$15,078,217	449
PAY	2008	10	-\$13,311,599	417	10	-\$19,799,067	461
PAY	2008	11	-\$13,604,780	383	11	-\$138,020	6
PAY	2008	12	-\$16,442,797	466			
			-\$148,395,685	4210		-\$141,806,452	4022
CB	2008	01	\$102,308	33	01	\$258,737	37
CB	2008	02	\$88,495	9	02	\$8,437	6
CB	2008	03	\$602,121	14	03	\$418,729	35
CB	2008	04	\$98,388	24	04	\$141,658	18
CB	2008	05	\$255,876	18	05	\$378,922	38
CB	2008	06	\$2,204	9	06	\$1,341,415	31
CB	2008	07	\$192,315	19	07	\$1,463,915	44
CB	2008	08	\$917,699	22	08	\$377,664	27
CB	2008	09	\$3,721,335	44	09	\$274,329	53
CB	2008	10	\$54,154	12	10	\$6,477,544	25
CB	2008	11	\$596,218	16	11	\$1,916	8
CB	2008	12	\$358,342	27			
			\$6,989,455	247		\$11,143,266	322

Matheson, Mary

From: Michael_J_Conkey@nbc.gov
Sent: Friday, September 11, 2009 9:29 AM
To: Matheson, Mary
Cc: Deborah_A_Baring-Schmidt@nbc.gov
Subject: Re: Additional funding
Attachments: 9-6620-FFS-NRC-36.pdf

Importance: High

Hi Mary! I sent that to you via our Customer Agreements System back in late August (the 20th, I think). I apologize that you didn't get it. I'll try a different method - scanning and attaching to this email.

It looks a bit strange because of the way we have to handle your agreement crossing fiscal years in our Customer Agreement System. The bottom line, the amount in the "Total" column is correct, although you don't see the \$90 K increase specifically in the "Modification Amount" column.

Again, sorry for the delay. Mike.

(See attached file: 9-6620-FFS-NRC-36.pdf)

From: "Matheson, Mary" <Mary.Matheson@nrc.gov>
To: "Michael J Conkey@nbc.gov" <Michael J Conkey@nbc.gov>, "Deborah A Baring-Schmidt@nbc.gov" <Deborah A Baring-Schmidt@nbc.gov>
Date: 09/09/2009 05:53 AM
Subject: Additional funding

Hi Mike,

I am not sure I have seen the document for additional funding. I was trying to get it obligated this FY.

Mary

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

1. Agreement Number: 9-6620-FFS-NRC-36		2. Action Type: Modification Mod: E	
3. Period of Performance: Start Date: 10/01/2009 End Date: 12/31/2009 4. FY: 2010			
5. Customer Information		6. NBC Information	
5a. Customer: NUCLEAR REGULATORY COMMISSION 11545 Rockville Pike ROCKVILLE, MD 20852-2747		6a. Directorate/Division: FINANCIAL MANAGEMENT AND BUDGET - BUSINESS MANAGEMENT OFFICE, D2705 National Business Center 7301 W. Mansfield Avenue Mail Stop D2705, Attn: Agreements Denver, CO 80235-2230	
5b. Customer Reference Number:		6b. Product Line: See Description of Services	
5c. Project Coordinator: Mary Matheson Phone: 301-415-8748 Fax: 301-415-5387 Email: MMM1@nrc.gov		6c. Project Coordinator: Michael J. Conkey Phone: 303-969-5587 Email: michael_j_conkey@nbc.gov	
5d. Customer Agency Location Code: 31-00-0001		6d. NBC Agency Location Code: 14-01-0001	
5e. Customer Appropriation Code: 31X0200		6e. NBC Appropriation Code: 14X4523	
5f. Customer Account Number: TQCFO09315		6f. Agreement Type: Fixed Price	
5g. Customer Obligating Doc Number: CFO-08-004		6g. NBC DUNS Number: 131978129	
5h. Customer DUNS Number: 040535809			
7. Description			
Tasks:	Original Amount	Modification Amount	Total
A. Accounting Ops. Financial Trans Processing. TDY Travel	\$407,400.00	\$0.00	\$407,400.00
B. Accounting Ops. Financial Trans Processing. PCS Travel	\$116,400.00	\$0.00	\$116,400.00
C. Accounting Ops. Financial Trans Processing. Vendor Invoice Payment	\$636,300.00	\$0.00	\$636,300.00
D. Accounting Ops. Financial Trans Processing. Vendor Invoice Payment	\$206,400.00	\$0.00	\$206,400.00
Total Price	\$1,366,500.00	\$0.00	\$1,366,500.00
8. Purpose of Agreement <i>The NBC will provide to the NRC accounting operations services, specifically travel, intra-governmental and vendor payment support. See the NRC Statement of Work dated April 2008, for specific functions, tasks and responsibilities. Please 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. The dollar amounts that are included in this IAA include costs for only known requirements. If additional requirements for items unknown during the execution of the IAA develop during the performance period of the IAA there may be a need to amend for any additional costs. Examples, significant changes to Financial regulatory requirements, significant changes to IT Security. Modification A is to increase vendor payment funding by \$112,500.00 for 9 months of the IAA. Modification B: for internal purposes to close out FY09 in FFS Modification D: to carry forward to FY10 Modification E: Final customer copy for increase</i>			

(August 2002)

Agreement Number: 9-6620-FFS-NRC-36

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: **Janet Whittet**

Telephone Number: **303-969-5379**

12. Other Terms and Conditions/Miscellaneous:

13. Approvals

13a. Customer Approval

13b. NBC Approval

Signature:

Date:

J. E. Dyer 9/14/09

Signature:

Date:

Connie M Sanborn

Name: J. E. Dyer

Name: Connie M Sanborn

Title: Chief Financial Officer

Title: Chief, Accounting Operations Division

Signature:

Date:

Signature:

Date:

Name:

Name:

Title:

Title:

13c. For NBC Internal Use Only

Signature:

Date:

Name: Zacoyia L. Clark

Title: Budget Analyst

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

This Security Services Advisory (SSA) satisfies the requirements of the Office of Management and Budget (OMB) Circular A-

I. 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.

II. 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.

III. 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 800-53, Revision 2, "Recommended Security Controls for Federal Information 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, receive initial security awareness training before being given access to NBC-managed systems, and annually thereafter.
- 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 Controlled Unclassified Information (CUI)). Also include any special handling requirements that **exceed** those currently being enforced by the NBC for its customers.
 - 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, Appendix 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 Manager	FPPS	IDEAS	CFS (Hyperion)	QuickTime	Travel
Gov Trip	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), For Official Use Only (FOUO), and Controlled Unclassified Information (CUI).

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.

IV. NBC IT SECURITY POINTS OF CONTACT

NAME	TITLE	PHONE #	FAX #	E-MAIL
D. June Hartley	OS/NBC CIO	(888) 367-1622	(303) 969-7102	June_D_Hartley@nbc.gov
Maria E. Clark	OS/NBC Chief Information Security Officer (CISO)	(888) 367-1622	(303) 969-7102	Maria_E_Clark@nbc.gov
Paul M. Kincaid	Alternate OS/NBC Chief Information Security Officer (ACISO)	(888) 367-1622	(303) 969-7102	Paul_M_Kincaid@nbc.gov
IT Service Center (Help Desk)	NBC Customer Support Center	(888) 367-1622 OR (303) 969-7777	(303) 969-5882	NBCDEN_ITSC@nbc.gov

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 and any specific applications ROB should be made available to all users before granting them access to an NBC-managed application or system. They are intended to supplement any existing organizational ROB that might be in use by customer organizations.

Rules of Behavior for National Business Center Users of Information Technology Resources

These rules are based on Office of Management and Budget (OMB) Circular A-130, Appendix III, Department of the Interior (DOI) Departmental Manual 375, Chapter 19 (375 DM 19), and the NBC Computer and Information Security Policy (NBC-CIO-POL-001). These rules apply to all users of NBC computer systems.

This document establishes a minimum set of rules of behavior while using IT (Information Technology) resources that are owned, leased, or managed by the Department of the Interior (DOI) or the National Business Center (NBC). IT resources include, but are not limited to, computers, networks, data, communications media, transportable data storage media, etc. Managers of Federal and contract employees are responsible for ensuring that these rules are implemented in their organizations and that all users are made aware of their responsibilities. All users are expected to comply with this and referenced DOI and NBC policies and will be held accountable for their actions while using NBC IT systems.

Employees who violate these Rules of Behavior may be subject to disciplinary action at the discretion of the appropriate DOI or NBC management in conformance with the DOI Handbook of Charges and Penalty Selection for Disciplinary and Adverse Actions, DM 752 Handbook 1. Additionally, the local IT Security Manager may remove or disable the user's access to systems in the event of a violation, in accordance with DOI and NBC IT Security policies referenced in these Rules of Behavior.

Network-based systems are inherently insecure and cannot guarantee privacy. In order to underscore this fact, all NBC computer systems display a logon warning banner that states, in part, that:

"Use of this system by any authorized or unauthorized user constitutes consent to monitoring, retrieval, and disclosure by authorized personnel. Users have no reasonable expectation of privacy in the use of this system. Unauthorized use may subject violators to criminal, civil, and/or disciplinary action."

Because network-based systems are inherently insecure, users should take appropriate measures to protect sensitive information. Refer to the NBC Information Classification Policy, NBC-CIO-POL-003 available on the NBC Web site at <http://www3.nbc.gov/employee/Security/NBC003.pdf>.

COMPUTER USE

- National Security Information (NSI Classified Data) may NOT be entered into any NBC computer system. In the event that National Security Information is accidentally transmitted to an NBC system, the local IT Security Manager must be contacted immediately.
- NBC and other DOI computer hardware, programs, and data are considered to be the property of the U.S. Government. Except as allowed by the DOI Policy on Limited Personal Use of Government Office Equipment (available on the DOI Web site at <http://www.doi.gov/ethics/docs/personaluse.pdf>), Government-owned or Government-leased computers, software, and telecommunications systems are to be used for work-related purposes only. Resources are not to be used to conduct or support a personal business; and no personally owned data or software shall be entered into an NBC system, LAN, or personal computer.
- Unofficial (personal) use of Government-owned IT resources – As noted above, the DOI Policy on Limited Personal Use of Government Office Equipment spells out the rules and conditions governing personal use of IT resources (e.g., computers, printers, E-mail, Internet, etc). This policy is available on the DOI Web site at <http://www.doi.gov/ethics/docs/personaluse.pdf>. Whenever there is a question or a doubt about the propriety of personal use of any Government-owned IT resource, refer to the DOI Policy on Limited Personal Use of Government Office Equipment or to the local IT Security Manager.

PASSWORDS AND USER IDS

- Passwords for all NBC computer systems:

- Are considered private and confidential. Users are prohibited from sharing any of their system passwords with anyone.
 - To minimize the risk of having the system compromised as a result of poor password selection, 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 or more characters in length.
 - Passwords should contain a mix of both upper and lower case letters.
 - There must be at least one numeric character (0, 1, 2, 3...9).
 - New (changed) passwords must 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.
 - **User Identifiers (User IDs)** are required for all users for access to NBC computer systems. Each user must be uniquely identified. **The User ID possesses privileges that are tailored to the duties of the individual 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 Security Point of Contact (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, each NBC system to which a user has access must be identified and the access terminated. This is accomplished on the checkout form completed by the user and supervisor on the last day of employment during the exit/clearance process. When employment termination is involuntary, is a result of natural or accidental death, or is caused by any other circumstance that precludes the user from performing the exit/clearance process, then it is the responsibility of the employee's immediate supervisor to expediently provide the notification(s).
- NOTE:** The terms "Security Point of Contact" and "SPOC" refer to any individual who has been delegated security responsibilities for administering user accounts (User IDs, passwords, access authorities, etc.), regardless of platform. When the user is a contractor, the Government responsible manager or Contracting Officer's Representative is the supervisor for the purposes of these Rules of Behavior.
- If problems are encountered with a User ID, the supervisor or SPOC must be contacted.

For details, refer to the NBC Computer and Information Security Policy, NBC-CIO-POL-001, available on the NBC Web site at <http://www3.nbc.gov/employee/Security/NBC001.pdf>.

USER ACCOUNTABILITY

- **Auditing of user access and of on-line activity is tied directly to the User ID.** Users are accountable for all actions associated with the use of their assigned User ID and may be held responsible for unauthorized actions found to be intentional, malicious, or negligent. Each user must protect his/her User ID by:
 - Never allowing another person to use or share his/her logon session. Because the logon

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.

- Locking the workstation or logging off an active session when leaving the workstation for any reason (e.g., going to a meeting, lunch, restroom, etc.) to prevent unauthorized use of the user's logon session. A password-controlled screensaver is an acceptable means for satisfying this requirement, provided the screensaver is activated before leaving the workstation and the screensaver password complies with the password rules spelled out in the Passwords and User IDs section above.

AUTHORIZED ACCESS

- **Users are responsible for the appropriate use and protection of sensitive information to which they have authorized access.** The use of such information for anything other than "official Government business" is expressly prohibited. 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.
- **Due to the high sensitivity of Individual Indian Trust Data (IITD) and Tribal Trust Data (TTD),** users must take extra care and precautions to protect any files or data entrusted to them related to IITD/TTD from unauthorized access.
- Casual browsing of sensitive or Privacy Act information, such as personnel data, is not appropriate and is prohibited. Users should only access this data when there is an official business reason.

For details, refer to the NBC Computer and Information Security Policy, NBC-CIO-POL-001, and the NBC Information Classification Policy, NBC-CIO-POL-003 available on the NBC Web site at <http://www3.nbc.gov/employee/Security/NBC003.pdf>.

UNAUTHORIZED ACCESS

- **Users are prohibited from accessing or attempting to access systems or information for which they are not authorized.** Users are prohibited from changing access controls to allow themselves or others to perform actions outside their authorized privileges. Users may not imitate another system, impersonate another user, misuse another user's legal user credentials (User IDs, passwords, etc.), or intentionally cause a computer or network component to function incorrectly. Users may not read, store, or transfer information for which they are not authorized.

DATA PROTECTION

- **Users are prohibited from intentionally adding, modifying, or deleting information or programs** on any NBC computer system or component thereof without a documented and approved form or request for the addition, modification, or deletion.

NOTE: This prohibition is not intended to include user-owned work files on individual workstations or on shared storage devices designated specifically for nonproduction use by individual users or groups. Nor is it a prohibition on user modifications to customizable software features such as "Preferences" or "Options", etc., unless such customization is not allowed by local policies, procedures, or standards. When unsure, users should consult with their supervisor or SPOC.

- **Users who establish individual files** must ensure that security of the files is commensurate with the sensitivity or criticality of their content. Users should contact their supervisors or SPOCs for assistance in protecting individual files.

- **Data requiring protection under the Privacy Act**, proprietary data, other sensitive data or official Agency documents may not be copied or otherwise removed from NBC systems for the purpose of sharing such data outside the authorized user's immediate work group, unless the information sharing has been authorized in writing by the Data Owner. Refer questions regarding Privacy Act information to the Departmental Privacy Officer at (202) 219-0868, or the Office of the Secretary Privacy Officer at (202) 208-6045.

DENIAL OF SERVICE

- **Users may not initiate actions, which result in limiting or preventing other authorized users or systems from performing authorized functions**, by deliberately generating excessive network traffic, and thereby limiting or blocking telecommunications capabilities. This prohibition includes the creation or forwarding of unauthorized mass mailings such as "chain letters", or messages instructing the user to "send this to everyone you know", or any messages with excessively large attachments or embedded graphics that consume large quantities of network bandwidth.

MALICIOUS (HOSTILE) SOFTWARE

- **Users must not intentionally write, compile, copy, propagate, execute, or attempt to introduce** any computer code designed to self-replicate, damage, or otherwise hinder the performance of any DOI or NBC computer system. Examples of these would be computer viruses, worms, and Trojan horses. For details, refer to the NBC Computer and Information Security Policy, NBC-CIO-POL-001, available on the NBC Web site at <http://www3.nbc.gov/employee/Security/NBC001.pdf>.

BYPASSING SYSTEM SECURITY CONTROLS

- **Unless specifically authorized by the NBC IT Security Manager**, NBC workers must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls. Examples of such tools include those that defeat software copy protection, discover (crack) secret passwords, or identify security vulnerabilities, etc. Additional examples include employing specialized system software mechanisms to bypass system security controls as a convenience measure.
- **Workers must not test or probe security mechanisms** at either the NBC or external installations unless they have first obtained permission from the NBC IT Security Manager.

COPYRIGHT LAWS AND LICENSE REQUIREMENTS

- **Commercially developed software.** Commercially developed software must be treated as the proprietary property of its developer. Title 17 of the U.S. Code states that it is illegal to make or distribute copies of copyrighted material without authorization. The only exception is the user's right to make a backup for archival purposes assuming the manufacturer does not provide one. It is illegal to make copies of software for any other purposes without the written permission of the copyright owner. Making or using unauthorized copies of copyrighted products from a DOI or NBC computer system is illegal and is expressly prohibited.
- **DOI and NBC-owned computer systems.** Users may only install commercial software that is acquired through an approved DOI or NBC procurement process. Vendor licensing requirements must be followed.
- **Personally owned software.** Users may not install personally owned software on DOI or NBC-owned computer systems. This includes but is not limited to personally owned screensaver software. An employee who has any doubt as to the appropriateness of installing personally owned software on a DOI or NBC-owned computer system should check with his or her supervisor for guidance.

CONNECTING TO THE INTERNET

NBC personnel are provided with the equipment and Internet connection to accomplish the work of the NBC. Limited personal use of the Internet is governed by the DOI Policy on Limited Personal Use of Government Office Equipment (available on the DOI Web site at <http://www.doi.gov/ethics/docs/personaluse.pdf>). Workers on **nonduty** time are allowed to use the Internet for personal use in accordance with the DOI Internet Acceptable Use Policy (available on the DOI Web site at <http://www.doi.gov/ethics/docs/internet.html>). Except as prohibited by the DOI Internet Acceptable Use Policy, workers are allowed minimal personal purchases through the

and is limited to official breaks, lunch, and before and after duty hours. When making such purchases, however, employees must arrange for the purchases sent to a non-Government address. Employees are prohibited from using Government office equipment at any time to make purchases for personal commercial gain activity. The prohibited activities listed in the DOI Internet Acceptable Use Policy include but are not limited to:

- Using Government-provided access to the Internet to present their personal views in a way that would lead the public to interpret it as an official Government position.
- Using the Internet as a radio or music player (e.g., use of "streaming audio or video").
- Using "push" technology on the Internet or other continuous data streams, unless they are directly associated with the employee's job.
- Using Government-provided E-mail for personal use except as authorized by Departmental policy as referenced in these Rules of Behavior.
- Using Government office equipment at any time for activities that are illegal (e.g., gambling) or that are inappropriate or offensive to co-workers or the public, such as the use of sexually explicit material, material or remarks that ridicule others on the basis of race, creed, religion, color, sex, disability, age, national origin, or sexual orientation.

RECORD RETENTION REQUIREMENTS

- **Users must follow DOI and NBC records management policies** (available on the DOI Web site at <http://www.doi.gov/ocio/records>). 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 E-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.

COMPUTER SECURITY INCIDENTS

- **Users and management are required to report all computer security incidents** (viruses, intrusion attempts, system compromises, offensive E-mail, inadequate protection of sensitive data, etc.) to their local IT Security Manager as follows:

Denver	(303) 969-7126
Reston	(703) 390-6726
Main Interior Building	(703) 390-6726
Boise	(208) 433-5050

- For additional assistance, users may contact the NBC Customer Service Center (CSC) at (303) 969-7777.
- **Users are responsible for cooperating with NBC IT System Administration and IT Security staff and the local IT Security Manager** during the investigation of a computer security incident.

USER RESPONSIBILITY

- **Users are responsible for following all the general computer use and IT security rules included in these Rules of Behavior** and for implementing appropriate controls to protect the resources and information under their control (as described in policies referenced in these Rules of Behavior). Each local NBC organizational unit or system may require additional levels of security controls. Resources permitting, users are responsible for implementing controls as requested by the local IT Security Manager.
- **Individual accountability.** Users will be held accountable for their actions on DOI and NBC IT

be removed without notice to ensure the operation and availability for the rest of the system users.

End:

Description of Services

9-6620-FFS-NRC-36

Service A - Accounting Ops. Financial Trans Processing, TDY Travel

- Accounting Ops. Financial Trans Processing, TDY Travel

Activity	Hours/Units	Amount
PROCESS TEMPORARY DUTY TRAVEL VOUCHERS	Fixed	\$407,400.00
<ul style="list-style-type: none">• 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.		
Service A - Total		\$407,400.00

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

- Accounting Ops. Financial Trans Processing. PCS Travel

Activity	Hours/Units	Amount
PROCESS PERMANENT CHANGE OF STATION TRAVEL VOUCHERS	Fixed	\$116,400.00
<ul style="list-style-type: none">• 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.		
Service B - Total		\$116,400.00

Service C - Accounting Ops. Financial Trans Processing. Vendor Invoice Payment

- Accounting Ops. Financial Trans Processing. Vendor Invoice Payment

Activity	Hours/Units	Amount
PROCESS VENDOR PAYMENTS/DISBURSEMENTS	Fixed	\$636,300.00
<ul style="list-style-type: none"> • Record all necessary transactions for vendor/federal disbursement processing in client agencies financial system, with proper internal controls and segregation of duties. Audit and certify vendor payments in accordance with client policy and federal payment regulations. Certify client agency vendor payments with Treasury. Respond to and resolve vendor questions concerning payments. Perform periodic reviews of financial transactions to ensure correctness. Maintain all financial transactions and supporting documentation in accordance with NARA standards. 		
Service C - Total		\$636,300.00

Service D - Accounting Ops. Financial Trans Processing. Vendor Invoice Payment

- Accounting Ops. Financial Trans Processing. Intra-governmental Payments (IPAC) and Grants

Activity	Hours/Units	Amount
PROCESS VENDOR PAYMENTS/DISBURSEMENTS	Fixed	\$206,400.00
<ul style="list-style-type: none"> Record all necessary transactions for vendor/federal disbursement processing in client agencies financial system, with proper internal controls and segregation of duties. Audit and certify vendor payments in accordance with client policy and federal payment regulations. Certify client agency vendor payments with Treasury. Respond to and resolve vendor questions concerning payments. Perform periodic reviews of financial transactions to ensure correctness. Maintain all financial transactions and supporting documentation in accordance with NARA standards. Process Grant drawdowns. 		
Service D - Total		\$206,400.00

MEMORANDUM OF UNDERSTANDING

AND

SERVICE LEVEL AGREEMENT

BETWEEN THE

**NATIONAL BUSINESS CENTER
DEPARTMENT OF THE INTERIOR**

AND

U.S. NUCLEAR REGULATORY COMMISSION

FINANCIAL MANAGEMENT SYSTEMS AND OPERATIONAL SUPPORT SERVICES

FOR FISCAL YEAR 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 U.S. Nuclear Regulatory Commission (NRC) 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 specific services and support provided to the NRC by the NBC with regard to financial management systems and operational support services and serves as a Service Level Agreement (SLA) and Memorandum of Understanding (MOU) between NRC and NBC. (See Section IV below). This document also establishes service levels and metrics, monitoring methods, and organizational responsibilities as applicable.

III. PERIOD OF PERFORMANCE

This MOU/SLA is effective upon signature by all parties and becomes part of the corresponding Inter/Intra Agency Agreement (IAA) issued to fund the services identified in this document. This MOU/SLA will remain in effect until September 30, 2008, unless it or 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 rules and regulations with regard to information technology operations and security, accounting practices, generally accepted accounting principles and standards (GAAP), and internal and management controls.

The NBC intends for this document to supplement the annual IAA to explain the specific services to be provided.

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 NRC under this MOU/SLA and supporting IAA.

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, installation of software fixes, Help Desk support, and disaster recovery
√	Federal Financial System (FFS)
	Oracle
	Momentum
	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, Momentum, mySAP)
	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 or custom interfaces
	Development of graphical user interfaces
	Development of documentation, policies, and procedures
	e-Travel software implementation, including development of an interface to the core accounting system
	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
	Hyperion – implementation support for financial statement production
	System training
	System testing
	Consulting services

C. ACCOUNTING OPERATIONS SERVICES

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

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

D. E-APPLICATIONS SERVICES

	<p>Web Application Development - 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</p>
	<p>Web Design and Implementation - Design and implement new websites and web pages. Implement and adhere to industry best practices. Post new or updated content provided by the information owner. Perform routine website maintenance including monitoring of orphan files and dead links</p>
	<p>Web Application and Website Hosting - 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</p>

V. RESPONSIBILITIES

A. NRC 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 financial systems and complete required Interconnect Security Agreement with the NBC.
- 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 NRC's financial data only to authorized personnel as instructed in writing by the NRC.
- 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 control objectives and activities as examined by an independent accounting and auditing firm.
- Conduct financial transactions testing at the transaction level in compliance with OMB Circular, A-123, Appendix A.

- Provide required financial, internal control, and FISMA certifications and assertions as required by OMB for the agency'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 management systems and services provided to customers. These metrics are identified in this MOU/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 specific financial management systems and services performance measures and service levels provided to the NRC.

VII. SECURITY

Security roles, responsibilities, and procedures related to this document are defined in the Interconnect Security Agreement (ISA) between the NRC and NBC that is provided as a separate document to the customer if required.

The technical details of the interconnection will be documented in an 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 system or the interconnecting medium 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 MOU/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 agency on a monthly basis for time and materials agreements and on a quarterly basis for fixed price agreements unless otherwise specified in the IAA.

All activities pursuant to this MOU/SLA are subject to the availability of appropriated funds and each agency's budget priorities. This MOU/SLA is neither a fiscal nor a funds obligation document. Nothing in this MOU/SLA authorizes, nor is intended to obligate, either agency to expend, exchange, or reimburse funds, services, or supplies, or transfer or receive anything of value, or enter into any contract, assistance agreement, interagency agreement, or other financial obligation. This MOU/SLA is strictly for the NBC and NRC internal management purposes. This MOU/SLA is not legally enforceable and shall not be construed to create any legal obligation on the part of either party. This MOU/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 MOU/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 NRC 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 MOU/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 NRC 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 and agree on a resolution to the dispute unless the issue warrants immediate attention such as for security incidents or events impacting sensitive or personally identifiable information (PII), which 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 the customer.

XI. NBC POINT OF CONTACT

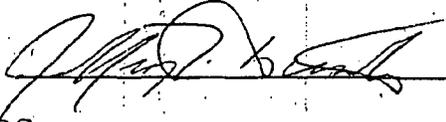
Name: Barbara Walters
Title: Chief, Functional Support Branch
Phone: (303) 969-5814
Email: Barbara_M_Walters@NBC.gov

XII. APPROVAL

This MOU/SLA accompanies the IAA and is considered mutually binding for the NBC and the NRC.

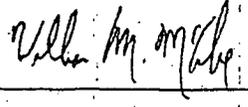
For the NBC:

Name: Jeffrey T. Hunter
Title: Chief, Finance and Procurement Systems Division

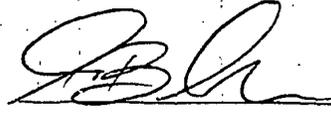
Signature:  Date: September 5, 2007

For the NRC:

Name: William M. McCabe
Title: Chief Financial Officer

Signature:  Date: 9/9/07

Name: Darren B. Ash
Title: Chief Information Officer

Signature:  Date: 5/5/08

**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) and supporting Interagency Agreement (IAA).

	MEASURE	PERFORMANCE METRIC
√	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 (6:00 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 is 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	<p>95% of billings are generated on or before the requested process date with end user authorization and concurrence and without reruns.</p> <p>95% of reports are made available in the INFONIMS (DocDirect) repository within 2 business days of the scheduled run.</p> <p>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.</p> <p>95% of demand letters are created and mailed on a monthly basis</p> <p>95% of referrals are done on a regularly scheduled basis of once monthly.</p> <p>NIIMS database is updated with status of referrals on a timely basis 85% of the time.</p>
	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 agency 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 agency 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 agency 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