Form NBC-IA-01
(August 2002)

CPSC-I-02-1369; MOD #26

National Business Center
Inter/Intra Agency Agreement

1. Agreement Number: ***13-6420-PPS-CPS-44***	2. Action Type: ***New***
3. Period of Performance: Start Date: ***10/01/2012*** End Date: ***09/30/2013*** 4. FY: ***2013***	
5. Customer Information	**6. NBC Information**
5a. Customer: ***CONSUMER PRODUCT SAFETY COMMISSION*** ***4330 EAST-WEST HIGHWAY*** ***ROOM 522*** ***BETHESDA, MD 20814-4408***	6a. Directorate/Division: ***CLIENT LIAISON & PRODUCT DEVELOPMENT DIVISION*** ***National Business Center*** ***7301 W. Mansfield Avenue*** ***Mail Stop D-2210, Attn: Agreements*** ***Denver, CO 80235-2230***
5b. Customer Reference Number: CPSC-I-02-1369; MOD #26	6b. Product Line: ***See Description of Services***
5c. Project Coordinator: ***Donna Simpson*** ***Phone: (301) 504-7218*** ***Fax: (301) 504-0432*** ***Email: dsimpson@cpsc.gov***	6c. Project Coordinator: ***Mishell R. English*** ***Phone: 303-969-5193*** ***Fax: 303-969-7151*** ***Email: mishell_r_english@nbc.gov***
5d. Customer Agency Location Code: ***61-00-0001*** TIN: 520978750	6d. NBC Agency Location Code: ***14-01-0001***
5e. Customer Appropriation Code: 61130100	6e. NBC Appropriation Code: ***14X4523***
5f. Customer Account Number: 61-0100	6f. Agreement Type: ***Fixed Price***
5g. Customer Obligating Doc Number: CPSC-I-02-1369; MOD #26	6g. NBC DUNS Number: ***608957460***
5h. Customer DUNS Number: ***069287522***	

7. Description

Tasks:	Original Amount	Modification Amount	Total
A. HR Application Services. Personnel and Payroll Operations	$155,148.65		$155,148.65
B. HR Application Services. E-Gov Initiatives	$44,209.70		$44,209.70
Total Price	**$199,358.35**		**$199,358.35**

8. Purpose of Agreement

The purpose of this Agreement is to document the terms of providing personnel, payroll, human resources and related services to the Consumer Products Safety Commission. Services to be performed are described in the Service Level Agreement (SLA).

MOD #26 to CPSC-I-02-1369 is being incrementally funded in the amount of $49,839.60 for the period 10/01/12 through 12/31/12. Additional funding will be provided, by modification, when funds become available.

Appro. Data: 0100A13DSE 2013 9994800000 EXIT002400 253P0

Form NBC-IA-01
(August 2002)

Agreement Number: ***13-6420-PPS-CPS-44***

9. Authority:

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 ***365*** 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: ***Brent Stevenson***
Telephone Number: ***303-969-5416***

12. Other Termsand Conditions/Miscellaneous:

No legal liability on the part of your agency (CPSC) arises until your appropriation is made available within your agency to fund this obligation/IA. Revisions to the terms of this agreement by either party will require a written modification to this agreement. Subject to availability of FY 2013 funding. Under a Continuing Resolution, billing will be at the prescribed CR daily rate with reconciliation to occur upon passage of a full year appropriation.

13. Approvals

13a. Customer Approval	13b. NBC Approval
Signature: Donna Hutton Date: 10/31/12	Lonalee Picardo Signature: Date: 08/02/2012
Name: Donna Hutton Title: Contracting Officer	Name: Lonalee Picardo Title: HRD Business Mgmt Ofc
Signature: Date:	Mishell R. English Signature: Date: 08/09/2012
Name: Title:	Name: Mishell R. English Title: Program Manager
13c. For NBC Internal Use Only	
	Signature: Date:
	Name: Jorge A Loa Title: Budget Analyst

Description of Services

13-6420-PPS-CPS-44

Service A - HR Application Services. Personnel and Payroll Operations

- HR Application Services. Personnel and Payroll Operations

Activity	Hours/Units	Amount
PERSONNEL/PAYROLL OPERATIONS & MAINTENANCE	Fixed	$124,740.00
• Base-level FPPS and Payroll operations support as stated n the SLA. Based on 660 W-2s at $198.00 per W-2 per year.		
QUICKTIME OPERATIONS & MAINTENANCE	Fixed	$25,830.00
• Time and Attendance support. Based on 630 W-2s at $41.00 per W-2 per year.		
EMPLOYEE EXPRESS	Fixed	$3,654.00
• Services provided through the OPM Employee Express program. Based on 630 W-2s at $5.80 per W-2 per year.		
DATAMART LICENSING MAINTENANCE	Fixed	$397.98
• Maintenance for Hyperion software licenses based on past usage.		
LEAVE AND EARNINGS STATEMENT (LES)	Fixed	$0.00
• LES printing and mailing costs. Based on 0% of 630 W-2s mailed at $10.50 per W-2 per year.		
TRAINING DATABASE	Fixed	$114.67
• Training database for clients to use for client-specific training needs.		
TRAINING	Fixed	$412.00
• Provide one training class		
Service A - Total		$155,148.65

Description of Services

13-6420-PPS-CPS-44

Service B - HR Application Services. E-Gov Initiatives

- HR Application Services. E-Gov Initiatives

Activity	Hours/Units	Amount
HRMS INTEGRATION (FORMERLY W2 SURCHARGE)	Fixed	$5,512.50
• Human Resources Management System (HRMS) integration. Based on 6230W2-s at $8.75 per W-2 per year.		
WORKFORCE TRACKING AND TRANSFORMATION SYSTEMS/ENTRANCE ON DUTY SYSTEM (WTTS/EODS)	Fixed	$5,985.00
• Operations and Maintenance based on 630 W-2s at $9.50 per W-2 per year.		
MGS HIRING MANAGEMENT ENTERPRISE	Fixed	$12,527.00
• MGS Hiring Management Enterprise subscriptions, covers 11/01/12 - 10/31/13 (12 months) based on 556 Fedscope FTEs		
NBC ADMINISTRATION - MGS	Fixed	$8,523.00
• NBC administration fee charged each year		
MGS CERTIFICATION AND ACCREDITATION	Fixed	$844.20
• NBC charges to cover MGS system Certification and Accreditation on behalf of customers charged each year		
TALENT MANAGEMENT SYSTEM	Fixed	$10,818.00
• LMM licensing for 600 users at $2.03/user ($1,218) • O&M charges for 600 employee users @ $16.00/user ($9,600)		
Service B - Total		$44,209.70

National Business Center (NBC) Information Technology (IT)

Security Services Advisory (SSA) For All NBC IT Customers

1 Introduction

This Security Services Advisory (SSA) satisfies the requirements of the Office of Management and Budget (OMB) Circular A-130, Appendix III. Signing of the Inter-Agency Agreement (IAA) also agrees to this Security Services Advisory and the attached Rules of Behavior.

1.1 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. The NBC Information Security Division (ISD), hereinafter referred to as NBC IT Security consists of a staff of highly trained professionals whose sole function is to serve the Information Technology (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.

1.2 PURPOSE

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

1.3 RESPONSIBILITIES

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

2 NBC RESPONSIBILITIES AND EXPECTATIONS RELATING TO CUSTOMERS

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 upon 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 3, "Recommended Security Controls for Federal Information Systems and Organizations".
- 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.

- May employ a standard user ID, with minimal access and authority to applications used by a customer, for the purpose of monitoring application availability. An automated monitoring application would use the ID to log in to an application repeatedly during hours of operation. This provides NBC with the ability to quickly identify issues with application availability as well as to accurately report on availability metrics defined in the SLA.

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.

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.

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.

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.

3 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.

NBC PRODUCTS AND SERVICES WHERE COMPUTER AND INFORMATION SECURITY SERVICES ARE PROVIDED BY THE NBC

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

FFS FPPS CFS (Hyperion) QuickTime Gov Trip

Oracle Federal Financials Data Warehouse FBMS eOPF Momentum

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.

4 NBC IT SECURITY POINTS OF CONTACT

NAME	PHONE #	FAX #	E-MAIL
Customer Support Center	(888)-367-1622 or (303)-969-7777	(303)-969-7102	NBC_IT Services@nbc.gov
Chief Information Security Officer	(888)-367-1622 or (303)-969-7070	(303)-969-7102	NBC_IT Services@nbc.gov

5 DOI, NBC RULES OF BEHAVIOR

Rules of Behavior for

Office of the Secretary and National Business Center Users of Information Technology Resources

These rules are based on Office of Management and Budget (OMB) Circular A-130, Appendix III and Department of the Interior (DOI) and National Business Center (NBC) Information Security and Privacy Policies. These rules apply to all users of Office of the Secretary and National Business Center computer systems and individuals who access sensitive DOI and NBC information.

This document establishes the Rules of Behavior while using Information Technology

(IT) resources or accessing sensitive information that are owned, leased, or managed by the DOI, Office of the Secretary (OS) or the NBC. IT resources include, but are not limited to, computers, networks, data, communications media and transportable data storage media. Further, the Rules of Behavior outline the requirements for the protection of agency sensitive information, whether in electronic or paper format. Managers of Federal and contract employees must ensure that these rules are implemented in their organizations. All users must comply with these rules and DOI and NBC security policies and will be held accountable for their actions while using OS/NBC IT systems. Users are defined as any person accessing IT resources. Users include, but are not limited to, Federal employees, contractors and vendors.

Use of OS/NBC systems constitutes consent to monitoring, retrieval, and disclosure by authorized personnel.

Penalties:

Federal 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 personnel policies and the DOI Handbook of Charges and Penalty Selection for Disciplinary and Adverse Actions, DM 752 Handbook 1. Prior to taking adverse disciplinary action, supervisors must consult the Human Resources Office. Additionally, the Bureau/office Information Security Manager may remove or disable the user's access to systems.

Contractors and vendors must comply with all applicable Federal and DOI rules, procedures and guidelines. Failure to do so may result in: removal of access to DOI systems; removal from the contract; and criminal prosecution where appropriate.

Rules:

PROTECTION OF SENSITIVE INFORMATION

- Users must take appropriate measures to protect OS/NBC IT resources and sensitive documents/data. Sensitive documents/data are agency documents/data which, while not classified for national security reasons, require special protection due to the ***significant*** risk of harm that could result from their inadvertent or deliberate disclosure, alteration or destruction. Typically, the release of these documents/data to the public is prohibited by statute or regulation.
- Documents and data must be protected in all forms – electronic, verbal, and paper. All electronic files which include sensitive information must be protected by encryption, when available. All paper files which include sensitive information are to be protected from unauthorized disclosure through the use of appropriate locked containers and disposal procedures.
- Users must inform their supervisor when processing sensitive information on systems that previously did not contain sensitive information so that appropriate security measures can be implemented.
- Sensitive documents/data include, but are not limited to, the following categories:
    - Documents/data requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, e.g., individually-identified medical, benefit and personnel information.
    - Personally identifiable information maintained in files not protected by the Privacy Act.

- Information compiled for law enforcement, investigatory, or security purposes.
- Critical infrastructure (physical and information technology) information as defined in 444 DM 1, Department of the Interior Departmental Manual, dated 7/7/99, Physical Protectoin and Building Security and Homeland Security Act of 2002: Critical Infrastructure Information Act.
- Continuity of operations and other emergency preparedness plans.
- Indian Fiduciary Trust information.
- Credit card numbers.
- Attorney-client communications.

- No user may knowingly enter National Security Information (NSI Classified Data) into any OS/NBC computer system. Any user who discovers National Security Information that has been transmitted to an OS/NBC system must immediately contact the NBC Information Security Division, Computer Security Incident Response Team (CSIRT).
- Users must protect sensitive data to which they have authorized access and must not disclose, without proper authorization, sensitive data to individuals who have not been authorized to access the data. Sensitive information must be encrypted when electronically transmitted to prevent unauthorized disclosure of sensitive information.
- Users must only access sensitive data, such as personnel data, when there is an official business reason.
- 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.
- 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 supervisor or Security Points of Contact (SPOC) for assistance in protecting individual files.

SYSTEM USE AND PROTECTIONS

- Except as allowed by the DOI Policy on Limited Personal Use of Government Office Equipment, Government-owned or Government-leased computers, software, and telecommunications systems are to be used for work-related purposes only.
- All users must protect computing equipment, including mobile devices, from physical dangers. For example, users must not keep open drink containers near computing equipment and must ensure proper ventilation and cooling for computing equipment.
- Users must not move or reconfigure hardware components without approval from OS/NBC IT.
- Users must not create file shares on OS/NBC systems without approval from OS/NBC IT.

PASSWORDS

- To minimize the risk of having the system compromised as a result of poor password selection; users must select passwords that are complex and difficult to guess. Wherever technically supported by the system, as many as possible of the following password selection criteria should be

employed:

- Passwords must be at least twelve or more characters in length.
- Passwords should contain a mix of upper and lower case letters, numeric characters (0, 1, 2, 3...9) and special characters (#, $, %, etc.).
- New (changed) passwords must not be revisions of an old password (i.e., changing one character from the previous password).
- 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, pet names, and birthdays should not be used.
- Proper names, geographical locations, common acronyms, and slang should not be used.

• Passwords must be changed on a regular basis, 60 days for normal users and 30 days for accounts with elevated privileges.

• Passwords must be changed immediately if exposed or compromised. If your password is compromised, immediately notify your supervisor and the NBC Help Desk.

• User Identifiers (User IDs) are required for all users to access OS/NBC computer systems. Each user must be uniquely identified.

- 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 and system passwords.
  - Users must not share system passwords with anyone.
  - Users must not allow another user to use or share his/her logon session.
  - Users must lock the workstation or log off an active session when leaving the workstation to prevent unauthorized use of the user's logon session.
  - Users must not store system passwords in electronic files unless the password data is encrypted.
  - Users should avoid storing passwords in written form. If passwords must be stored in written form, users must ensure that passwords are stored in an appropriately secured location (i.e., safe, locked cabinet or locked drawer, etc.)
- 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 documented in an access request and approved.
  - If duties or job requirements change, accesses no longer needed must be promptly removed and new accesses must be requested. Supervisors must notify 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. The term Security Point of Contact refers to any individual who has been delegated security responsibilities for administering user accounts.

- Users must comply with the exit/clearance process on their last day of employment. When employment terminates, each OS/NBC system to which a user has access must be identified via the exit/clearance process and the access terminated. Supervisors must provide the notification of access termination to the appropriate SPOC in cases that precludes the user from performing the exit/clearance process.

UNAUTHORIZED ACCESS

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

- Users must not use sensitive data for anything other than "official Government business".

- Data requiring protection under the Privacy Act, proprietary data, other sensitive data or official Agency documents must not be copied or otherwise removed from OS/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.

- Users must not remove Government property from OS/NBC premises for personal use.

- Personally owned data or software must not be installed on or entered into an OS/NBC system, LAN, or personal computer.

- Personally owned removable storage media must not be used to download and store DOI documents, files, or data.

- All non-Government issued laptop computers must be inspected and authorization granted by OS/NBC IT prior to connecting to any OS/NBC network or computer resource. The inspection shall include scans and system checks to ensure all devices are safe and meet DOI standards. Authorizations for use must expire after five working days or after the laptop computer leaves the Government premises that issued the authorization.

- Non-Government owned Portable Electronic Devices (PED) must not be connected to any OS/NBC network or computer resource.

- Users must not install, activate or use Instant Messaging (IM), Internet Relay Chat (IRC), Web Conferencing, and Peer-to-Peer (P2P) without prior authorization.
  - Examples of IM software include, but are not limited to: AOL, Yahoo, and MSN Instant Messenger.
  - Examples of IRC include, but are not limited to: Undernet, Galaxynet and ERNet.
  - Examples of P2P software include, but are not limited to: Ares, Bearshare, Blubster, Cheetah, Crapster, DC++, Direct connect, eDonkey, File Miner, File Navigator, Filetopia, Freewire, Gnucleus,

Gnutella, GoMP3, Grokster, iMesh, KaZaA, Limewire, Morpheus, MyNapster, WinMX, PHEX, Piolet, Shareaza, Prune Baby, SwapNut, URLBlaze, XoLoX and Yaga.

- Users must 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.

- 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.

- Unless specifically authorized by the NBC Chief Information Security Officer (CISO), users 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.

- Users must not employ specialized system software mechanisms to bypass system security controls as a convenience measure. This includes attempts to access information on how to bypass security controls, such as searching online for ways to bypass corporate firewalls to access blocked web sites.

- Users must not test or probe security mechanisms at either the OS/NBC or external installations unless they have first obtained authorization from the NBC CISO.

COPYRIGHT LAWS AND LICENSE REQUIREMENTS

- 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. Users must not make or use unauthorized copies of copyrighted products from a DOI or NBC computer system.

- Users may only install commercial software that is acquired through an approved DOI or NBC procurement process. Vendor licensing requirements must be followed.

- Use of non-commercial software, such as freeware, shareware, and open source software, is prohibited without the written consent of the user's supervisor and OS/NBC IT. Also note that many freeware products are free only to individual persons and require purchase for commercial or government use.

CONNECTING TO THE INTERNET

OS/NBC personnel are provided with the equipment and Internet connection to accomplish the work of the OS/NBC. Limited personal use of the Internet is governed by the DOI Policy on Limited Personal Use of Government Office Equipment. Users may

make limited personal use of government equipment as long as it occurs on non-duty time, does not interfere with official business, does not adversely impact electronic systems, is not commercial gain activity or is not otherwise prohibited, and the expense to the government is negligible. The prohibited activities listed in the DOI Internet Acceptable Use Policy include but are not limited to:

- Using Government office equipment to conduct transactions for personal commercial gain/loss activity (e.g., using an office computer to purchase stock shares on the stock market or to conduct transactions and correspondence for a personal business outside of NBC/OS).
- 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") unless specifically authorized by the NBC/OS CISO.
- 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.
- Using Government-provided equipment for the creation, storage, or transmission of copyrighted material, such as ripping CDs to MP3, transmitting or sharing MP3, software, music, or video files.
- Unless authorized by the NBC/OS CISO, users shall not visit sites that discuss techniques for bypassing or testing security controls, such as hacking websites, forums, or other malicious behavior. Visiting news and discussion sites that discuss current events and threats is authorized, so long as those sites do not discuss the details of how to utilize those techniques to bypass or test security controls.

E-MAIL

- All email that contains sensitive information must be encrypted. Examples of sensitive information commonly transmitted via email:
  - Social Security Numbers, Credit Card Numbers and other non-public Personally Identifiable Information (PII).
  - Risk Assessments, vulnerability scan results
  - Security Incident information
  - IP addresses, port numbers, dial-in information
  - Passwords
- Users must not click on attachments with the following extensions. If you receive an email with one of the following attachments, DO NOT open the attachment. Immediately contact the Help Desk or Customer Support Center .

  ade, adp, bas, bas, bat, chm, cmd, com, cpl, crt, exe, hta, ins, isp, lnk, mda, mde, mdz, mp3, msc, msi, msp, mst, ocx, pcd, pif, reg, sct, shs

- Uses must not subscribe to non-business-related listservs.
- Users must not click on web links or open attachments contained in unexpected emails. These are common methods used to deliver malicious software to unsuspecting users.
- Users must use notepad or another text editor to open potentially hostile scripting files, such as .vb, .vbs, .js, etc.

HANDLING OF PRIVACY ACT RECORDS

This section outlines standards of conduct for personnel in implementing requirements of the Privacy Act of 1974 (5 U.S.C. 552a). Individuals to whom these standards are applicable include all personnel who have access to systems of records subject to the Privacy Act, such as Quicktime, or who are engaged in the development of procedures or systems for handling such records (i.e. those engaged in personnel management, records/paperwork management, computer systems development and operations, communications, statistical data collection and analysis, and program evaluation).

- Individuals must follow OPM, DOI and NBC Privacy Act policies.
- Program officials and system managers must ensure that no irrelevant or unnecessary personal information is collected.
- Individuals must make all reasonable efforts to maintain accurate and timely records.
- Individuals must protect the integrity, security, and confidentiality of these records.
  - o Minimum safeguards for hard copy (non-automated) records subject to the Privacy Act:
    - Records system areas must be posted with warnings to include access limitation, standards of conduct for employees in handling Privacy Act records, and possible criminal penalties for violations.
    - Access to records must be restricted at all times by storing the records in a locked metal file cabinet or locked room, except when the room is occupied by authorized personnel.
    - Where a locked room is the method of security, master keys must not be available to unauthorized personnel.
  - o Safeguards for automated records subject to the Privacy Act must follow National Institute of Standards and Technology (NIST) requirements.
  - o Appropriate safeguards must be taken when records subject to the Privacy Act are transferred within or outside the agency. Steps must be taken to assure the integrity and confidentiality of the records while in transit.
  - o Records subject to the Privacy Act must be disposed of in accordance with the provisions of National Archives and Records Administration regulations, 36 CFR 1228.74.
    - Records may be burned, shredded or pulped within the organization
    - Records may be pulped, macerated, or shredded by a wastepaper contractor; however, a Federal employee must witness the destruction.
- Individuals must protect personal information contained in systems of records subject to the Privacy Act from disclosure for any purpose other

than that for which the information was gathered, or under exceptions provided in the Privacy Act and to any external parties other than those specified in the applicable Privacy Act System of Records Notice.

- Individuals must not alter or destroy a record subject to the Privacy Act unless it is undertaken in the course of his/her regular duties, required by a decision under the Department's regulations, or pursuant to a court decision.

- Any officer or employee who knowingly and willfully makes an unauthorized disclosure of records subject to the Privacy Act, or who willfully maintains a system of records without meeting the Privacy Act's notice requirements, is guilty of a misdemeanor and may be fined up to $5,000.

RECORD RETENTION REQUIREMENTS

- Users must follow DOI and NBC records management policies. 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. Salazar 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. Salazar litigation; or
  - Administration of Individual Indian Money (IIM) accounts.

- Users must print and file the weekly e-mail notification of the backup of e-mail records. The subject of this email is titled "Notification of Capture of E-mail Messages on Backup Media".

- All official records, including printed copies of emails, must be turned over to the employee's supervisor or other designated individual at termination of employment.

MEDIA LABELING AND SANITIZATION

- Users must ensure that all sensitive data, electronic and printed, is labeled with the appropriate sensitivity and handling label.

- All sensitive information, both electronic and printed, must be properly sanitized, stored, or disposed of when no longer needed.

COMPUTER SECURITY INCIDENTS

- Users must promptly report all computer security incidents to their local Information Security Manager, the NBC Information Security Division, CSIRT or their Help Desk or Customer Support Center . Examples of computer security incidents include, but are not limited to, unauthorized disclosure of information, computer viruses, theft of equipment, software or information, inappropriate use, and deliberate alteration or destruction of data or equipment.

- Federal Agencies are required to report all incidents involving Personally Identifiable Information (PII) to U S CERT within one hour of discovering the incident. Agencies must not distinguish between suspected and confirmed breaches and must report all incidents involving PII in electronic or physical form. Users must immediately report all PII incidents to

the NBC Information Security Division, CSIRT so that NBC can meet the required OMB reporting requirement.

- For additional assistance, users may contact their local Help Desk or Customer Support Center .

- Users must cooperate fully with the NBC Information Security Division, CSIRT during the investigation of a computer security incident. The CSIRT Incident Manager is authorized to confiscate any and all government owned equipment deemed necessary during the course of the investigation. If the CSIRT confiscates equipment, the user's supervisor will be informed and alternate computing resources will be arranged.

SPECIAL CONSIDERATIONS FOR REMOTE ACCESS

Access to agency resources from a location not under the direct control of the Office of the Secretary or the National Business Center is considered "Remote Access". New technical solutions are being implemented to secure and protect agency data, especially if it is being carried outside of the OS/NBC's physically protected areas. With these new requirements also come new responsibilities for user behavior regarding the protection of agency data. Users must secure and protect agency data as follows:

- Users must physically protect all hardware or software based tokens entrusted to them for authentication or encryption purposes. (A token is usually a physical device that an authorized user is given to provide additional higher level security and to verify the user is who they say they are when logging in to the network.)

- Users must encrypt all agency data stored on any equipment, including but not limited to computers, external hard drives, PDAs, and thumb/flash drives, anytime they are outside of OS/NBC protected facilities. This requirement is only applicable once NBC or the Office of the Secretary provides an encryption solution for end-users.

- Per OMB requirements, users must ensure that all agency data downloaded using remote access is erased after 90 days or when it is no longer needed. Where more stringent requirements are defined by organizational policies, users must follow the more stringent requirements.

- Users should refer to their Information Security Manager for standards and approved methods for encrypting and deleting data.

- Users must use only an OS/NBC approved method of remote connectivity, such as a Virtual Private Network (VPN).

REFERENCES:

DOI:

http://www.doi.gov/ethics/docs/personaluse.pdf

DOI Policy on Limited Personal Use of Government Office Equipment

http://elips.doi.gov/app_dm/index.cfm?fuseaction=home

DOI DM 375, Chapter 19, Information Technology Security Program

DOI DM 383, Policies and Procedures for Implementing the Privacy Act of 1974

NBC:

https://mynbc.nbc.gov/PFTGF/policies/policies.cfm?LOB=ITD

NBC Computer and Information Security Policy (NBCM-CIO-6300-001)

OS/NBC Information Classification and Handling Policy (NBCM-CIO-6300-003)

CONTACTS:

NBC Customer Support Center	1-888-FOR-1NBC (1-888-367-1622)

5.1 Individual Computer User's

5.1.1 ACKNOWLEDGEMENT OF RESPONSIBILITY

5.2 For Use of OS/NBC Computer Systems

I understand that when I use any of the Office of the Secretary's (OS) or National Business Center's (NBC) computer systems or Information Technology (IT) resources or gain access to any information therein, such use of access shall be limited to official Government business (except as allowed by the DOI Policy on Limited Personal Use of Government Office Equipment). Further, I understand that any use of the aforementioned systems or information that violates these Rules of Behavior may result in disciplinary action consistent with the nature and scope of such activity.

NOTE: Security policy infractions committed by contractors or vendors who are working for, and being paid by, the OS or the NBC will be handled in accordance with the provisions of their respective contracts concerning disciplinary or punitive actions, except in the case of criminal acts, which will be turned over to local law enforcement or Federal investigators.

I have been provided with and have read the "Rules of Behavior" (ROB) for Office of the Secretary and National Business Center Users of Information Technology Resources, Version 2.0.3 dated April 17, 2012. I understand these Rules of Behavior and agree to comply with these Rules.

Federal Employee ☐ Contractor or Vendor ☐

Print Full Name: _____

Signature: _____

Date: _____

Directorate, Division, Branch: _____

Company Name (for Contractors/Vendors): _____

Signature: _____

Contractors – COTR's Name: _____

SERVICE LEVEL AGREEMENT

BETWEEN THE
HUMAN RESOURCES DIRECTORATE
NATIONAL BUSINESS CENTER
DEPARTMENT OF THE INTERIOR

AND

CONSUMER PRODUCT SAFETY COMMISSION

FOR FISCAL YEAR: 2013

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 Consumer Product Safety Commission (CPSC) pursuant to the Government Management Reform Act (GMRA) of 1994 and under authority of the Interior Franchise Fund legislation: Pub. L. No. 104-208, div. A, § 101(d) [§ 113], as amended, which established the Department of the Interior Franchise 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's Human Resources Directorate (HRD). See Section IV below for the specific services to be provided. This standard Service Level Agreement (SLA) also establishes service levels, 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 (IA). The IA is issued to fund the specific services identified in this document. This SLA will remain in effect until the IA is amended, replaced, or terminated by signed, mutual agreement of both organizations. The IA that provides funding for the services must be renewed annually to ensure continuation of services. In advance of each fiscal year, service listings and cost figures will be sent to each customer for confirmation and budget planning.

IV. LIST OF SERVICES

The NBC provides an array of payroll and personnel processing applications and services, and human resources and human capital services. Personnel and payroll applications and services are delivered in compliance with the Financial Systems Integration Office, OPM's Enterprise Human Resources Integration (EHRI), and Human Resources and Payroll Systems Requirements for payroll management activities. Human Resources Operations and Human Capital programs meet all OPM and Office of Management and Budget (OMB) policies and regulations with regard to human resources practices. All Human Resources and Payroll systems and services are delivered in conjunction with guidance from OPM's Human Resources Line of Business (HRLoB) program.

Each service is provided specifically at the request of the customer and is costed separately. Upon purchase of additional services, the IA and SLA will be modified to reflect the new services provided.

X	Federal Personnel and Payroll System (FPPS) - HRMS Integration

	- LES Printing and Mailing
	Human Resources Cross-Servicing Support and/or Human Capital Services (see detailed services list in Section IV B.)
X	DataMart Data Warehouse Query usage
X	OPM's Employee Express Self-Service
X	Quicktime Time & Attendance System
	webTA Time & Attendance System/Kronos
X	Workforce Transformation Tracking/Entry on Duty System
	USA Staffing Licenses/OPM
X	Monster Government Solutions Hiring Management Enterprise subscriptions/MGS
X	Talent Management System: Learning Management, Performance Management Modules/SAP
X	FPPS Training Database
	Exit Interview System
	Historical Data Storage
	Labor Cost System Processing and Support
X	HR LoB Application Training, after initial implementation
	Labor Cost System Processing and Support
	Client-Specific Special Project
	Client-Specific Auxiliary Systems
	Client-Specific Interface Development/Implementation/Maintenance
	Client-Specific Software Modifications
	Client-Specific Data Network Services
	Client-Specific Data Network Services, Disaster Recovery Site

The services purchased by the client under the IA and supporting SLA are indicated by a checkmark

A. FPPS BASE LEVEL SERVICES

As an FPPS customer, the following FPPS and Payroll Operations Services are included as baseline services:

FPPS General System

- Integrated personnel and payroll system
- Online editing
- Real-time updates
- Table-driven Order of Precedence
- Ticklers sent through a customer's e-mail system
- Help desk support for end users

Security & Performance

- Maintenance of security and integrity of the database and client data, and management of system-level user IDs, passwords, and access authorities
- Mainframe Security Access
- Security Access profiles
- Audit trail capabilities

- Route Path Maintenance Process allows the paths to be established for routing of SF-52, WGI notifications, and probationary notifications
- Database server software and physical database installation and upgrades
- Database performance optimization
- Database backup and recovery
- Provision and management of a Disaster Recovery program, including: development and maintenance of a Contingency of Operations Plan (COOP) that covers FPPS and T&A system production environments; provision and management of an off-site storage; provision and management of a hot site facility; performing disaster recovery backups; and scheduling, coordination, and support of a disaster recovery testing process. The results can be made to the client after the test has been completed. The Disaster Recovery Plan can be made available to the client on request.
- Provision of and management of a "health and well-being" monitoring system for FPPS and T&A system environments.
- Management of a monitoring and reporting system of FPPS and T&A activity and performance levels
- Provision of and management of a physically secure hosting facility, meeting federal government policies and standards for both physical and logical security

Personnel Processing

- Processing for SF-52/50 personnel actions. Allows capability for managers to initiate and route SF-52s
- Capability to set up routing of SF-52/50 for specific types of action within the Requesting Office (RO) and Servicing Personnel Office (SPO)
- Command-driven system that combines data elements for the specific personnel function being processed
- System allows individuals to sign off on SF-52 as a concurrer, like budget or Equal Employment Opportunity (EEO) directors
- System allows individuals limited view-only access
- System allows a RO or SPO to send an automated courtesy copy of SF-52s to other individuals in an office
- Capability for SPO to put a SF-52 on hold with comments as to why System sends notification to requestor/authorizer that action is on hold
- Users within the same office may reassign SF-52s to another in their office
- SPO has the capability of fast copying multiple SF-52s when hiring large number of individuals for same type of position.
- On-line help function for commands and field level help
- Data element definitions and processing actions assistance on each screen. Majority of FPPS data elements are contained in tables for easy update.
- Ability to enter Health Benefit information function for Standard Form 2809 (SF-2809) Employee Health Benefits Election Form and Standard Form 2810 (SF-2810) Notice of Change in Health Benefits.
- SF-50s generate the payments for Administratively Uncontrollable Overtime, Availability Pay, Awards, Relocation Incentives, Recruitment Incentives, Retention incentive and Separation Incentives.

- Annual Pay Raise processed by FPPS
- Generation of ticklers based on nature of actions processed
- Generation of Probationary Certifications and Within-Grade Certifications. Notifies user through email when the certification has been forwarded to their queue.
- Generation of WGI nature of actions once time period has been met. FPPS also adjusts waiting period based on any excess Leave Without Pay.
- Generation of Career Tenure nature of action
- Capability to view an employee record on-line for verification. This also includes history information.
- Capability to view completed and pending SF-50 actions on-line
- Ability to track the SF-52/50 transactions which allows RO and SPO to determine who has signed the SF-52 and where it currently is located
- View an employee's history on-line
- Interfaces daily to the retirement system
- Interfaces daily to eOPF
- Accommodation of dual positions (employee has two different positions simultaneously in the same or different agencies)
- Mass change capability, such as reorganizations, realignments, and awards
- Automatic accumulation of non-paid hours for Leave Without Pay, Within Grade Weeks, or Appointment Limits (day, weeks, or dollars)
- Electronic generation of standard reports (Standard Form 113A and G, Monthly Report of Fulltime Equivalent/Work Year Civilian Employment), OPM's eOPF, Central Personnel Data File (CPDF), and EHRI
- Generation of Work Year and Personnel Cost Report (A93).
- Users are alerted of important information from NBC through Message of the Day command.
- On-line CPDF edits are run against the SF-52/50

Pay Processing

- Pay processing, including all calculations of gross-to-net pay; processing of pay and leave adjustments; government additives; applying hourly, bi-weekly, and annual limitations; maintenance of data for current and future reporting; and production and distribution of reports.
- Automatic deferral of payments that exceed the aggregate pay limitation, and automatic generation of those payments in the following year or upon the employee's separation
- Entitlements for items, such as uniform allowance, fringe benefits, recruitment and relocation incentives, and bonuses
- Entitlements and allowances for employees in foreign duty stations
- Prior pay period re-computations resulting from changes in T&A data, personnel actions, or retroactive regulatory changes. Changes within the last 26 pay periods are automated; older changes are calculated manually and then processed through FPPS as one-time adjustments
- Computation and disbursement of back pay provisions of settlement cases, including payment and Form 1099 reporting of interest, as authorized

- Leave buy back related to periods of Office of Worker's Compensation Program (OWCP) are computed, collected, and the records adjusted accordingly
- Supplemental payments via a Pay Daily process
- Physician Comparability Allowance payments
- Administratively Uncontrollable Overtime payments
- Law Enforcement Availability Pay payments
- Standby payments
- Student Loan repayments as hiring incentives
- Automated processing of Transportation pre-tax deductions and Fringe Benefits
- Computation, deduction, disbursement and reporting for federal, state, and local taxes, as well as Old Age Survivor's Disability Insurance (OASDI) and Medicare. Perform all tax accounting, reconciliation, 941, W2, W2c as well as 1099 reporting for interest and beneficiaries. Maintain separate tracking and reporting of prior year OASDI and Medicare transactions.
- Accounting, disbursement, reconciliation, and reporting of deductions and government contributions, as applicable, for Civil Service Retirement System (CSRS) and Federal Employee Retirement System (FERS), life insurance, health insurance, TSP, thrift loans, and military service credit deposits
- Disbursement of net pay via electronic funds transfer and Treasury checks; accounting and disbursement of deductions, including savings allotments, discretionary allotments, quarters deductions, savings bonds, charities, union dues, association dues, commercial garnishments, child support, alimony, bankruptcies, education loans, Long-Term Care premiums, Flexible Spending Account deductions, Health Savings Account deductions, and Dental and Vision Care premiums
- Union deductions based on flat amounts, table lookups, or percentages of gross or base pay
- Payment of union dues and distribution of detailed union deduction information to unions and, if requested, labor relations officials
- Government Quarters Housing deductions, including appropriate tax treatment for required Quarters occupancy
- Separation processing; generation of lump sum payment based on Nature of Action (NOA) code; issuance and certification of Standard Form 1150 (SF-1150) Record of Leave Data report; submission of retirement packages; closeout of retirement cards and automated severance pay, if applicable
- Processing of taxable wage information from client finance offices for inclusion on the employees W2 (e.g., taxable travel payments, Permanent Change of Station reimbursements)
- Automated W2 processing, including ability to update W2 information after the final pay period for the year; automated W2c processing; and on-line generation of duplicate W2s
- Association and fitness dues deduction processing
- Automated deceased employee beneficiary pay

Time and Attendance Processing

- FPPS T&A Module provides for collection of leave and work hours, information on shift, overtime, and other premiums, exceptions to bi-weekly and hourly limits, project numbers, comprehensive editing at time of input, on-line help, and table look-ups. Timesheet processing includes on-line storage of timesheet data, and an on-line audit trail of changes.
- Continuous T&A editing once T&As have been submitted to FPPS, and proactive interactions with timekeepers, personnel offices, and supervisors to resolve T&A errors before payroll calculation. An on-line error correction process used by the Payroll Office allows for cleaner T&A data to be sent to FPPS pay calculation.
- Automated leave processing of all regulatory leave types, including annual, sick, restored, military, leave under the Family and Medical Leave Act (FMLA), bone marrow/organ donations, administrative, and numerous agency-unique leave types. FPPS also supports credit hours, compensatory time, time-off awards, home leave, and shore leave. Leave processing includes applying accruals, maintaining balances, applying regulatory maximums, and reporting.
- Automated leave share and leave bank programs, including donations and receipts, accrual of special leave accounts per regulations, automated return of unused donations upon case closure.
- Automated support for worker's compensation and continuation of pay cases with quarterly reporting.
- Certification of SF 1150s for separated employees, performing summary leave audits, performed by Payroll Operations staff
- Providing advice and guidance on premium pay and leave administration matters to supervisors, timekeepers, and/or employees in accordance with regulation
- Audit and correct employee leave records in the event that there is an error
- Develop and distribute updates on OPM leave and attendance policy changes
- Transfer in new employee leave. Communicates with User Group member regarding various pay and leave issues during the leave year or as needed
- Inactivate separating employee profiles through the appropriate system

DataMart

- Comprehensive HR/Payroll system data warehouse for analytics and reporting
- On-line query
- Library of standard queries as a baseline for customized queries
- Ad hoc and modifiable queries
- EEO and MD-715 reporting
- User-friendly query software and DataMart
- Available for export to many applications
- Help desk support for end users

Debt Processing

- Management of salary-related debts, including issuing bills, providing due process, and issuing collection notices in accordance with the Debt Collection Improvement Act; negotiating repayment schedules; initiating involuntary collections; accruing interest; establishing amortization schedules; and

adjudicating waiver requests. Monthly reports to serviced agencies are produced to assist them in tracking their debt status and activity. Names and phone numbers of payroll contacts are printed on each bill to assist employees when questions arise.

- Processing collections for other debts, providing employee notice and enforcing regulatory maximums for collection of other agency debts, child support, bankruptcies, commercial garnishments, education loans, alimony and tax levies. Support of the Treasury Offset Program and Delinquent Credit Card Offset program. Deducting travel advances or other non-salary related internal debts at the request of the employing agency.

Payroll Accounting

- Creation of labor cost file for interface to client labor cost system or accounting system. Creation of detail and summary accounting reports. Reconciliation of labor cost file with payroll disbursements. Assistance to client accounting offices on payroll accounting issues.
- Collection, deposit, reporting, and crediting of employee records for check and cash receipts, including receipts for bills, military service credit deposits, OWCP buyback, and advance payments of health benefit premiums.
- Collection Subsystem that tracks and accounts for receipts of cash or checks.
- Tracking, accounting and re-issue of returned payments, savings bonds, and Treasury credits, including Limited Payability credits. Resolution of lost/stolen paychecks and savings bonds and other post-issuance problems. Issue replacement checks and track the status of funds.
- Reissue/Re-certification process provides replacement payments to employees within a day.

Benefits Support

- Maintenance of retirement records (both service history and fiscal data), military service credit deposit records and providing for check payment or payroll deduction of military service credit deposits.
- Health Benefit submissions to carriers and quarterly reconciliation program
- Automated Retirement and Insurance Transfer System (RITS) reporting with capability to include external transactions
- Thrift Lost Earnings pass-through from the TSP record keeper to client agency via labor cost file.

Miscellaneous

- Duplicate Leave and Earning Statements (LES) can be issued immediately upon request. LES' can include broadcast messages and individual messages, such as expiration of compensatory time and restored leave, update of Within Grade Increases (WGIs), and changes in pay.
- Supports necessary interface files with government and vendor entities
- Employment verification via The Work Number by the TALX Corporation
- Unemployment reporting via the TALX Corporation's UC-Express

- Imaging of documents to eliminate the need for stored paper documents and allow for imaged document retrieval.
- Medicare Data Match
- Payroll Operations Employee Hotline

B. webTA BASE LEVEL SERVICES

As a webTA customer, the following services are included as baseline services:

webTA General System

- Web enabled time and attendance system
- Online editing
- Real-time updates
- Ticklers sent through a customer's e-mail system
- Automated file interface to FPPS
- Help desk support

Security & Performance

- Maintenance of security and integrity of the database and client data, and management of system-level user IDs, passwords, and access authorities
- Mainframe Security Access
- Security Access profiles
- Audit trail capabilities
- Database server software and physical database installation and upgrades
- Database performance optimization
- Database backup and recovery
- Provision and management of a Disaster Recovery program, including: development and maintenance of an Information System Contingency Plan that covers the T&A system production environment; provision and management of an off-site storage; provision and management of a hot site facility; performing disaster recovery backups; and scheduling, coordination, and support of a disaster recovery testing process.
- Provision of and management of a "health and well-being" monitoring system for the webTA system environment.
- Management of a monitoring and reporting system webTA activity and performance levels
- Provision of and management of a physically secure hosting facility, meeting federal government policies and standards for both physical and logical security
- Host and maintain the required infrastructure for the time and attendance system.
- Communicate system unavailability in a timely manner

Time and Attendance Processing

- webTA provides for collection of leave and work hours, information on shift, overtime, and other premiums, Telework, exceptions to bi-weekly and hourly limits, project numbers, comprehensive editing at time of input, on-line help, and table look-ups. Timesheet processing includes on-line storage of timesheet data, and an on-line audit trail of changes.

- Continuous T&A editing once T&As have been submitted to FPPS, and proactive interactions with timekeepers, personnel offices, and supervisors to resolve T&A errors before payroll calculation. An on-line error correction process used by the Payroll Office allows for cleaner T&A data to be sent to FPPS pay calculation.
- Automated leave processing of all regulatory leave types, including annual, sick, restored, military, leave under the Family and Medical Leave Act (FMLA), bone marrow/organ donations, administrative, and numerous agency-unique leave types. The webTA system also supports credit hours, compensatory time, time-off awards, home leave, and shore leave. Leave processing includes applying accruals, maintaining balances, applying regulatory maximums, and reporting.
- Automated leave share and leave bank programs, including donations and receipts, accrual of special leave accounts per regulations, automated return of unused donations upon case closure.
- Automated support for worker's compensation and continuation of pay cases with quarterly reporting.
- Provide ongoing updates to employee profiles, T&A profiles, location information, leave balances, etc. via daily and bi-weekly feeds.
- Review Vendor test plans and scripts and utilize formal change management process, installation and testing changes to the system
- Biweekly transfer of timecard data the FPPS system
- Initial population of the database, including master accounting data table and employee information
- Ongoing updates to the database of employee profile, T&A profile, and locator information via daily interface feeds, and leave balances via a bi-weekly interface feed
- Update leave balances after calculate
- Update employee status
- Process changes in work schedule and organization code
- Provide link to vendor created User Manuals
- Provide Release Description Documents and website help with each software release

Payroll Processing

Payroll processing is part of the FPPS base level service, found in section IV A, and is the same regardless of T&A system used.

Miscellaneous

- Supports necessary interface files with government and vendor entities
- Imaging of documents to eliminate the need for stored paper documents and allow for imaged document retrieval.

C. OPTIONAL HUMAN RESOURCES CROSS-SERVICING SUPPORT AND SERVICES

Human Resources Cross-Servicing Support and Human Capital Services can be customized per customer needs. Following is a specific listing of the services offered.

	Organization and Position Management	
		Position Classification – Supports the creation or revision of position descriptions, the evaluation of job requirements against classification standards, and administration of the classification appeal process.
		Position Management – Supports the assignment of work and establishment of positions to carry out the organization's mission or program and maintenance of the agency's inventory of positions.
	Staff Acquisition	
		Recruiting – Executes the Staff Acquisition Plan by engaging in marketing, advertising, personal contact, and other outreach activity aimed at building a pool of quality candidates that have potential for meeting the human capital needs of the agency.
		Assessment Model – Identifies or develops assessment tools and criteria to be used to determine the best-qualified candidates for a particular job or job group.
		Staffing – Fulfills government wide and agency-specific regulatory requirements to effect a hiring action for specific position(s). Applies assessment tools and methods to evaluate candidates against requirements of the job for which they are being considered.
		Application Management – Accepts employment applications and captures application information in a manner that makes it available to those who need it. Manages and communicates application status. Analyzes and assesses application information to determine applicant eligibility for employment. Issues selection certificates to hiring managers.
	Performance Management – Provides consultative support on the implementation and evaluation of performance management programs. Provides support to managers and supervisors on individual performance management processes and issues.	
	Compensation Management	
		Pay Administration – Determines eligibility and calculates values for pay and leave and other compensation.
	Benefits Management – design, develop and implement benefit programs that attract, retain, and support current and former agency employees.	
		Benefits Counseling – Advises individuals on a wide range of benefit options, eligibility and impacts. Provides information, counseling, assistance, and advocacy to employees regarding their benefits and entitlements.
		Benefits Processing – Captures, validates, and processes benefits elections and actions.
		Benefits Reporting – Provides the capability to report employee participation in benefits programs.
		Retirement Counseling – Advises individuals on retirement benefits and steps required to prepare for retirement. Calculates annuity estimates.
		Workers Compensation – Provides comprehensive workers

		compensation services including adjudication, case management, and counseling.
	Employee Relations – Provides support to management for a variety of employee relations matters including disciplinary action, adverse action, administrative action, action related to unacceptable performance, alternative dispute resolution, grievance, third-party decisions and appeals, suitability, reasonable accommodation, and termination.	
	Labor Relations – Provides support to management and/or agency on a variety of labor relations matters including term, mid-term and ad-hoc negotiations; mediation; arbitration; alternative dispute resolution; filings; and compliance with statutory labor-management relations obligations.	
	Personnel Action Processing – Initiates, validates, approves, updates, and documents personnel actions and data.	
	FPPS Security – Serves as Security Administrator and Security Point of Contact for FPPS. Establishes and maintains offices and organizations; oversees user-related authorities; and establishes personnel action workflow/routing paths.	
	Personnel Security and Homeland Security Presidential Security 12 – (HSPD-12 Processing)	
		Fingerprint and Background Investigation (BI) Processing – Coordinates and processes fingerprints and BIs for employees, applicants, and contractors for non-sensitive low risk positions, Public Trust positions and for National Security Clearances through the Electronic Questionnaire for Investigation Processing (e-QIP) system. Adjudicates BI results for suitability determination and issuance of National Security Clearances per agency and OPM regulations and policies. Advises agency on application of OPM or agency Personnel Security regulations, policies and procedures.
		Homeland Security Presidential Directive (HSPD-12) Processing – Serves as Initiator, Sponsor, and Adjudicator for issuance of HSPD-12 credentials in USA Access on behalf of the agency. Serves as agency Liaison with General Services Administration (GSA) on all card or system issues.
	Other Human Resources work/project as described:	

The services purchased by the client under the IA and supporting SLA are indicated by a checkmark

V. RESPONSIBILITIES

A. GENERAL NBC RESPONSIBILITIES

- Protect client agency data in accordance with the NBC's and the client's security requirements, as well as other laws, regulations and guidelines. The NBC will only disclose client data to authorized personnel.
- Accomplish Payroll and personnel processing following the end of the pay period in sufficient time to meet the established payday. In the event processing is

delayed, it will be rescheduled as soon as practical, consistent with the client agency's payday and appropriate client personnel will be notified.

- Provide support to client agency staff in their use of the NBC services and systems.
- In the event that network/telecommunications is or becomes a service provided by the NBC, the NBC responsibilities are:
    - Plan, analyze, and implement network connectivity and Windows server environment solutions.
    - Provide direct computer services to the client in support of specific applications, if requested.
    - Install, configure, and administer telecommunications hardware/software in support of the client.
    - Monitor and manage the security of NBC's network resources.
    - Administer network servers supporting application, database, E-mail and Web services.
    - Provide user support, problem determination and problem resolution through the NBC's Network Operations Center.
- Provide for business recovery and continuity of operations of NBC business units in the event of a disaster or long-term service interruption to clients. Specifically the NBC will.
    - Prepare and maintain the following three plans:
        - Business Recovery Plan that identifies how NBC business units will resume operations of critical business functions in the event of a disaster.
        - Data Center Continuity of Operations Plan (COOP) that specifically addresses how the Data Center environment, i.e. General Support Systems, will resume operations.
        - Application Continuity of Operations (COO) that specifically addresses how each critical business application will recover.
    - Furnish copies of the Business Recovery Plan, Data Center COOP and Application COO upon request. NBC-sensitive information will be excluded from these copies. Requests made by contractors or auditors representing the client will not be honored.
    - Perform periodic testing of these plans. Clients shall be afforded the opportunity to test their application(s) on an annual basis.
    - Provide for a business recovery work site facility for NBC personnel to conduct business resumption operations and provide for one or more Data Center hot site facilities for NBC to restore its General Support Systems. These facilities shall be available within 24 hours following a disaster or long-term service interruption.
- Provide support to the client agency in response to audit findings related to NBC provided services
- Liaison between the client agency and any vendor(s) with which NBC maintains a contract and the client agency has purchased products or services through the NBC. Please note: NBC does not own COTS product code.

- Provide notification of the separation or long-term absence of their respective points of contact. In addition, NBC will provide notification of any changes in points of contact information or changes in job responsibilities.
- Assure that the security for systems hosted by the NBC are 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 redacted C&A documentation available to clients for review at a designated NBC location.
- Provide a copy of the C&A letters for systems hosted at the NBC from the NBC Designated Approving Authority.
- Report any incident involving personally identifiable information (PII) as outlined in Section VII A below.
- The C&A can be reviewed by authorized client representatives in Denver Colorado at 7301 Mansfield Avenue, Lakewood Colorado or at the Main Interior Building in Washington DC.

B. GENERAL CUSTOMER RESPONSIBILITIES

- Ownership and control of your agency's data
- The Privacy Act requires the owner of information in a system of records to publish a System of Records Notice (SORN) in the Federal Register to cover their own data in FPPS and DataMart.
- Designate a representative(s) to participate in FPPS Users Group meetings.
- Designate principal contacts in the finance, human resources, security, and information technology areas.
- Acquire remote (peripheral) hardware and communications. This would like any routers necessary to maintain dedicated connection with the National Business Center Denver Data Center or specific printer equipment that may be required for FPPS.
- Provide for the transmission of input data to the NBC computer facility according to the Personnel/Payroll System Biweekly Processing Schedule. Both parties must agree to any changes to this schedule.
- Prepare and maintain a Business Recovery Plan that identifies how the client will resume operations of its business functions should a disaster at the client facility occur. The Plan should specifically address where the client will be relocated and replacement of client-provisioned network circuits to NBC and the NBC hot site.
- Participate, as mutually agreed upon, in annual testing of the Business Recovery Plan at the NBC hot site.
- Provide notification of the separation or long-term absence of their respective points of contact. In addition, client will provide notification of any changes in points of contact information or changes in job responsibilities.
- Report any incident involving personally identifiable information (PII) as outlined in Section VII A below.
- For all time and attendance system customers:

- Monitor the time and attendance system each pay period to ensure all timecards are validated and certified in the system and transmitted to FPPS in a timely manner.
- Monitor all timecard corrections in the system to ensure they are transmitted to FPPS in a timely manner.
- Reset time and attendance system passwords and unlock user accounts
- Release timecards in time to meet NBC biweekly pay calculation deadlines
- Assign and maintain roles within time and attendance solution.
- Respond to employee time and attendance policy questions.

C. NBC REPSONSIBLITIES FOR OPTIONAL HUMAN RESOURCES CROSS SERVICING/HUMAN CAPITAL SERVICES

- Protect client agency data in accordance with applicable laws, regulations, guidelines, and Department of the Interior security requirements.
- Disclose the client's human resources data only to authorized personnel as instructed in writing by the client.
- Provide competent, trained, and certified staff and management for services to be provided.
- Be readily available for scheduled and, as schedule permits, for unscheduled on-site meetings.
- Provide support to the client 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 clients by telephone and/or email within 4 hours in the event of a disaster or other contingency that disrupts the normal operation of any service.
- Provide operations point of contact and escalation point of contact.
- Ensure all actions are in accordance with Merit System Principles (MSPs), Federal Laws, Federal regulations, and agency policy and standard operating policies (SOPs).
- Perform services identified in a timely and efficient manner.
- Utilize automated systems in accordance with applicable polices, regulations, and laws to ensure proper safeguarding of data, system security, and internal controls.

D. CUSTOMER RESPONSIBILITIES FOR OPTIONAL HUMAN RESOURCES CROSS SERVICING SERVICES

- Provide knowledgeable contacts to respond to questions related to services provided by the NBC.
- Follow NBC guidance to ensure compliance with the aforementioned MSPs, Federal laws, Federal regulations, agency policy and SOPs. Failure by client to maintain compliance with aforementioned laws, regulations and policies may constitute grounds for immediate termination of services by NBC.
- Provide agency documentation necessary to allow NBC to execute its responsibilities under this agreement, e.g. Strategic Plan, Documentation of

Delegated Authorities from the Office of Personnel Management, position descriptions, human resources policy, etc.

- Provide access to agency data in the Federal Personnel and Payroll System (FPPS).
- Provide management assistance and involvement when necessary to coordinate and resolve human resources-related issues.
- Provide an escalation point of contact.
- Initiate personnel actions using FPPS in a timely and accurate manner if applicable.
- Initiate human resources requirements in a timely and accurate manner.
- Utilize automated systems in accordance with applicable polices, regulations, and laws to ensure proper safeguarding of data, system security, and internal controls.

VI. PERFORMANCE MEASUREMENT

Measures of performance have been identified for customer service, personnel systems, payroll operations, and human resources services. These metrics are identified in this SLA. They have been identified as the NBC's planned service levels to ensure high quality services to customers. See Attachment A for the performance measures and service levels applicable for personnel systems and payroll operations and Attachment B for optional human resources cross servicing. Metrics will be reported to customers on a quarterly basis.

VII. SECURITY

Security roles, responsibilities, and procedures related to this document are defined in the Security Services Advisory (SSA) that is embedded within the accompanying Interagency Agreement.

An Interconnect Security Agreement (ISA) is established between the NBC Information Technology Services Line of Business and non-DOI clients 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 client 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.

A. PERSONALLY IDENTIFIABLE INFORMATION (PII)

Incident Reporting and notification of PII Breech

The NBC or Client, upon discovering an incident involving personally identifiable information (PII) in electronic or physical form shall report it to the U.S. Computer Emergency Readiness Team (CERT) within one hour of discovery. The reportable incidents shall not distinguish between suspected and confirmed breaches.

Additionally, the NBC or Client, upon discovering a system-related security incident, shall report it in accordance with its agency-specific incident reporting procedures and shall notify the NBC Help Desk (888) 367-1622 within two hours. NBC will follow incident response procedures, currently based on the *NBC Computer Security Incident Response Team Handbook,* Version 2.2.6a, dated December 23, 2008, which follows DOI Computer Incident Reporting Capability (CIRC) procedures.

NBC staff shall immediately notify the designated Client counterpart by telephone or e-mail upon discovering an incident involving personally identifiable information (PII) in electronic or physical form or when a system-related security incident(s) is detected, so their counterpart may take steps to determine whether a system has been compromised and to take appropriate action. The designated client counterpart shall investigate as necessary and coordinate remediation activities for their agency.

If the origin of the incident is with the NBC, NBC staff shall keep the designated Client counterpart informed of workarounds, corrective actions, and final resolution.

VIII. FUTURE SYSTEMS PLANNING

NBC will work with the OPM, THE Shared Service Center Advisory Council (SSCAC), and the HRD clients to determine the future direction of payroll/personnel systems and the Federal Enterprise Architecture (FEA) at the NBC. This includes schedule, funding and migration planning.

IX. FUNDING

Under the provisions of the Working Capital Fund, 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. NBC will notify the customer of their annual budget within the customer's budget cycle. Customer budgets are established by distributing total NBC cost to all clients on the basis of number of W2s. Any optional services provided to the customer will be billed on an actual cost basis. 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 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.

X. 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 advance written notice as outlined in the IAA 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 transition is completed. 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.

XI. 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, this can be in the form of an email or hard copy letter. 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.

XII. POINTS OF CONTACT

NBC maintains a communication process that is used for day-to-day operating issues and questions using established contacts. In the case where an issue or concern needs to be escalated, the following contacts should be used. At that time, it can be determined what appropriate course of action needs to be taken for problem resolution.

NAME	TITLE	ADDRESS	EMAIL	PHONE
Karen Roper	Client Liaison, Client Liaison and Product Development Division	Atrium Bldg Reston, VA	Karen_roper@nbc.gov	703-964-3581
Mishell English	Deputy Chief, Client Liaison and Product Development Division	7301 W. Mansfield Ave. Denver, CO 80235	mishell_english@nbc.gov	303-969-5193
Leisa Schievelbein	Chief, Client Liaison and Product	7301 W. Mansfield Ave. Denver, CO	leisa_schievelbein@nbc.gov	303-969-7200

	Development Division	80235		
LC Williams	Associate Director, Federal Personnel Payroll Systems and Services	7301 W. Mansfield Ave. Denver, CO 80235	lc_williams@nbc.gov	303-969-7200

Attachment A

PERSONNEL SYSTEMS AND PAYROLL OPERATIONS SERVICES PERFORMANCE MEASUREMENT

The measures below apply to FPPS, T&A, WTTS, and TMS customers

MEASURE	PERFORMANCE METRIC
Implementing New Federal Pay and Personnel Regulatory Requirements	
▪ Requirements received with sufficient lead time	▪ 100% implementation of all changes within timeframe mandated or work-around solutions mutually agreed to as an interim
▪ Requirements with a retroactive effective date or when sufficient lead time not provided	▪ 100% implementation of all changes scheduled for an upcoming FPPS Release with work-around solutions mutually agreed to as an interim
Payroll Accuracy	
▪ Pay and leave processed accurately	▪ 99.8% accuracy based on information received and in NBC's control
Disbursements	
▪ Disbursements are made on or before the scheduled process date	▪ 99.9% timely payroll disbursements
Reports	
▪ External reports/interfaces completed by scheduled due dates	▪ 99% timely reports/interfaces ▪ 99% accuracy based on information provided

MEASURE	PERFORMANCE METRIC
Benefits Updates ▪ Transmission of employee update files to external benefit providers within established timeframes. Includes: Long Term Care, Flexible Spending Account, Dental/Vision Benefit, Federal Employee Health Benefit files.	▪ 98% timely file submissions
Hours of Operation ▪ Payroll staff available Monday through Friday, 7:30am – 4:00pm Mountain Time (MT); excluding Federal holidays. ▪ Employee and end-user help desks available Monday through Friday, 6:00am – 5:30pm MT; excluding Federal holidays. Interactive Voice Response available 24x7.	▪ 99% available ▪ 99% available
Help Desks ▪ Employee calls returned within 2 hours. ▪ Employee issues resolved within 24 hours ▪ End-user calls returned within 4 hours ▪ End-user issues resolved within 48 hour	▪ 95% returned within 2 hours or less ▪ 95% issues resolved within 24 hours or less ▪ 95% returned within 4 hours or less ▪ 95% issues resolved within 48 hours or less
System Availability-FPPS ▪ Production system available Monday through Friday, 5:00am – 6:00pm MT; Saturday 5:00am – 3:00pm MT; excluding Federal holidays, and during payroll processing or other regularly scheduled outages. Additional hours available upon request for special circumstances	▪ 97% available

MEASURE	PERFORMANCE METRIC
System Availability-Quicktime ▪ Production system available Monday through Friday, 4:00am – 12:00am MT; Saturday 4:00am – 9:00pm MT; Sunday 12:00pm – 8:00pm Bureau of Land Management and DOI Office of the Secretary only. Excluding Federal holidays and other regularly scheduled outages. Scheduled maintenance may be performed after 6:00 pm MT as necessary with prior notification.	▪ 97% available
System Availability-webTA ▪ Production system available Monday through Friday, 4:00am – 12:00am MT; Saturday 4:00am – 9:00pm MT; Excluding Federal holidays and other regularly scheduled outages. Scheduled maintenance may be performed after 6:00 pm MT as necessary with prior notification.	▪ 97% available
System Availability-Workforce Transformation Tracking System ▪ Production system available Monday through Friday, 5:00am – 6:00pm MT; Saturday 5:00am – 3:00pm MT. Excluding Federal holidays and other regularly scheduled outages.	▪ 97% available
System Availability-Talent Management System ▪ Production system available 24x7 excluding regularly scheduled outages, including each Sunday from 2 AM to 1:30 PM.	▪ 97% available
System Performance ▪ Internal system response time within established parameters.	▪ 95% available

MEASURE	PERFORMANCE METRIC
System Operations ▪ User access granted within 72 hours of request.	▪ 98% access granted within 72 hours or less

Attachment B

PERFORMANCE MEASURES
OPTIONAL HUMAN RESOURCES SERVICES
PERFORMANCE MEASUREMENT

The items checked below are the specific measures and metrics that are related to the services provided to the customer under this service level agreement (SLA). Performance metrics are based on a normal human resources operating environment and unusual situations, e.g. Reduction in Force, staffing of newly funded organization, may result in deviations from established metrics that will be discussed and agreed to with agency management.

	Measure	Performance Metric
	Organization and Position Management Positions are classified in accordance with OPM published classification standards.	95% of all positions are classified in accordance with OPM published classification standards within 14 calendar days of receiving all appropriate materials from client management * *If major classification activity is taking place, e.g. reorganization, management will prioritize work with the understanding that metric will be impacted by the special project
	Staff Acquisition Posting of vacancy announcement, reviewing applicants, issuing certificates and making tentative job offer. **External metric missed due to client request for higher priority over job offer	90% of vacancy announcements will be posted within 7 calendar days of receipt of completed recruitment package, including approved SF 52, Request for Eligible, and final job analyses 92% of the time upon receipt of properly documented selection certificate, Human Resources Representative will make tentative job offer within 4 calendar days.
	Benefits Management Retirement annuity estimates will be provided.	Retirement annuity estimates will be provided within 14 calendar days of request from employee 90% of the time.* *Metric may be impacted if NBC does not have complete employee record, e.g. waiting for OPF from National Records Center or former agency.

	Measure	Performance Metric
	Employee Relations Draft corrective action documents (Letters of Counseling/Warning, Letters of Reprimand) will be provided to management.	Draft corrective action documents (Letters of Counseling/Warning, Letters of Reprimand) will be provided to management within 7 calendar days of agreement on course of action 95% of the time.
	Employee Relations Draft disciplinary, adverse and performance action documents (proposal and decision documents for suspensions, demotions, and removals) will be provided to management. NBC will coordinate with general/legal counsel, union, and or employee representative as necessary, which may impact metric time. Special attention will be given to critical employee relations issues.	Draft disciplinary, adverse and performance action documents (proposal and decision documents for suspensions, demotions, and removals) will be provided to management within 14 calendar days of agreement on course of action 95% of the time.
	Personnel Action Processing SF-50 personnel actions and other actions, such as benefit processing, will be processed for proposed allowable effective date	SF-50 personnel actions and other actions, such as benefit processing, will be processed for proposed allowable effective date 95% of the time.
	FPPS Security User profiles will be established or changed	User profiles will be established or changed within 7 calendar days of receiving completed user access request 90% of the time.

PERSONNEL SECURITY

	Measurement	Metrics
	Background Investigation Processing Initiation and processing of Fingerprints and Background Investigations (BI) for Internal and External Clients	Fingerprints initiated and submitted to OPM within 3 (work) days of receipt of security package 80% of the time
		Background Investigations initiated and submitted to OPM within 14 (Calendar) days of receipt of fingerprint results 80% of the time
	HSPD-12 Card Processing	HSPD-12 Card Initiation, Sponsorship and

	Measurement	Metrics
	Completion of HSPD-12 Card Initiation, Sponsorship and Enrollment	Enrollment completed within 14 (Calendar) days of receipt of initiation in DOI Access 80% of the time