AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1 CONTRACT ID CODE	PAGE OF PAGES
	1 | 3

2 AMENDMENT/MODIFICATION NO	3 EFFECTIVE DATE	4 REQUISITION/PURCHASE REQ NO	5 PROJECT NO (If applicable)
0027	12/26/2012	REQ-2400-13-0040	

6 ISSUED BY CODE FMPS

CONSUMER PRODUCT SAFETY COMMISSION
DIV OF PROCUREMENT SERVICES
4330 EAST WEST HWY
ROOM 523
BETHESDA MD 20814

7 ADMINISTERED BY (If other than Item 6) CODE FMPS

CONSUMER PRODUCT SAFETY COMMISSION
DIV OF PROCUREMENT SERVICES
4330 EAST WEST HWY
ROOM 517
BETHESDA MD 20814

8 NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)

INTERIOR UNITED STATES DEPT OF
NATIONAL BUSINESS CENTER
7301 WEST MANSFIELD AVENUE
D2920
DENVER CO 80235-2230

CODE [redacted] FACILITY CODE

(x) 9A AMENDMENT OF SOLICITATION NO

9B DATED (SEE ITEM 11)

X 10A MODIFICATION OF CONTRACT/ORDER NO. CPSC-I-02-1369

10B. DATED (SEE ITEM 13) 09/24/2002

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended ☐ is not extended

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required) Net Increase: $49,839.60

0100A13DSE-2013-9994800000-EXIT002400-253P0

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	
	A THIS CHANGE ORDER IS ISSUED PURSUANT TO (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO IN ITEM 10A
	B THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D OTHER (Specify type of modification and authority)
X	BILATERAL MODIFICATION, FAR 43.103(b)

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return 1 copies to the issuing office

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

DUNS Number: [redacted]
COR: Donna Simpson
PHONE: (301) 504-7218
EMAIL: dsimpson@cpsc.gov

Modification No. 0027 is a continuation of agreement CPSC-1-02-1369 for FY-2013.

Add Items 0118 through 0128 (see pages 2 and 3).

Modification 0027 is being incrementally funded in the amount of $49,839.60 for the period January 1, 2013 through March 31, 2013. Additional funding will be provided, by

Continued ...

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A NAME AND TITLE OF SIGNER (Type or print)	16A NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
Mitchell Gaulish Program Manager	Donna Rutton
15B CONTRACTOR/OFFEROR	15C DATE SIGNED: 4/15/13
16B UNITED STATES OF AMERICA (Signature of Contracting Officer)	16C DATE SIGNED: 12/26/12

NSN 7540-01-152-8070
Previous edition unusable

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA
FAR (48 CFR) 53.243

NAME OF OFFEROR OR CONTRACTOR
INTERIOR UNITED STATES DEPT OF

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	modification, when funds become available. FULLY FUNDED AMOUNT FOR FY-2013: $199,358.35 Add Item 0118 as follows:				
0118	Basic FPPS and Payroll Operations Support based on 630 W2s at 198.00 per year	1	LO	31,185.00	31,185.00
	Add Item 0119 as follows:				
0119	Quicktime T&A based on 630 W2s at $41 per year.	1	LO	6,457.50	6,457.50
	Add Item 0120 as follows:				
0120	OPM Employee Express based on 630 W2s at $5.80 per year	1	EA	913.50	913.50
	Add Item 0121 as follows:				
0121	Datamart Maintenance for Hyperion software based on past usage	1	LO	99.50	99.50
	Add Item 0122 as follows:				
0122	Leave and earning printing/mailing based on 0% of 630 W2s mailed @ $10.50 per year	1	LO	0.00	0.00
	Add Item 0123 as follows:				
0123	Training database	1	EA	28.67	28.67
	Add Item 0124 as follows:				
0124	Training class for 1 participant	1	EA	103.00	103.00
	Add Item 0125 as follows:				
0125	HRMS Integration (formerly W2 surcharge) based on 630 W2s @ $8.75 per year.	1	LO	1,378.13	1,378.13
	Continued ...				

CONTINUATION SHEET	REFERENCE NO OF DOCUMENT BEING CONTINUED CPSC-I-02-1369/0027	PAGE 3 OF 3

NAME OF OFFEROR OR CONTRACTOR
INTERIOR UNITED STATES DEPT OF

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Add Item 0126 as follows:				
0126	Workforce tracking and transformation System/Enter on duty system (WTTS/EODS) based on 630 W2s @ $9.50 per year	1	LO	1,496.25	1,496.25
	Add Item 0127 as follows:				
0127	Monster Hiring Management Enterprise Subscriptions, covers 11/1/12-10/31/13 (12 months) at current discounted rate of $22.53/FTE based on 556 Fedscope FTEs ($12,526.68) MGS System Certification and Accreditation ($844.20) NBC Administration FEE ($8,523)	1	LO	5,473.55	5,473.55
	Add Item 0128 as follows:				
0128	Talent Management System includes LMM licensing for 600 users at $2.03/user ($1,218) O&M chargers for 699 employee users @ $16/users (9,600)	1	LO	2,704.50	2,704.50
	ALL OTHER TERMS AND CONDITIONS REMAIN UNCHANGED AND IN FULL FORCE AND EFFECT.				

CPSC-I-02-1369; MOD #27

Form NBC-IA-01
(August 2002)

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:	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 #27	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 #27 to CPSC-I-02-1369 is being incrementally funded in the amount of 49,839.60 for the period 1/1/13 through 3/31/13. Additional funding will be provided, by modification, when funds become available.
Appro. Data: 0100A13DSE 2013 9994800000 EXIT002400 253PO

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: 12/20/12	Lonalee Picardo Signature: Date: 08/02/2012
Name: Donna Hutton Title: Contracting Officer	Name: Lonalee Picardo Title: HRD Business Mgmt Ofc
Signature: Date:	M 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

CPSC-I-02-1369; MOD #27

Form NBC-IA-01
(August 2002)

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:	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 #27	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 #27 to CPSC-I-02-1369 is being incrementally funded in the amount of 49,839.60 for the period 1/1/13 through 3/31/13. 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 appropiration 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:** 12/20/12	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.
  - 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.
  - Safeguards for automated records subject to the Privacy Act must follow National Institute of Standards and Technology (NIST) requirements.
  - 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.
  - 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: _____