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)
0019	01/28/2011	REQ-2400-11-0078	

6. ISSUED BY	CODE	7. ADMINISTERED BY (If other than Item 6)	CODE
CONSUMER PRODUCT SAFETY COMMISSION DIV OF PROCUREMENT SERVICES 4330 EAST WEST HWY ROOM 517 BETHESDA MD 20814	FMPS		

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)		9A. AMENDMENT OF SOLICITATION NO.
INTERIOR UNITED STATES DEPT OF ATTN MS LONA PICARDO NATIONAL BUSINESS CENTER 7301 WEST MANSFIELD AVENUE D2920 DENVER CO 80235-2230	(X)	9B. DATED (SEE ITEM 11)
	X	10A. MODIFICATION OF CONTRACT/ORDER NO CPSC-I-02-1369
		10B. DATED (SEE ITEM 13) 09/24/2002
CODE [redacted]	FACILITY CODE	

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)

0100A11DCC 2011 9994800000 EXITIT2400 253P0 Net Increase: $94,163.30

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:
X	D. OTHER (Specify type of modification and authority) 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]

Modification No. 0019 is a continuation of agreement CPSC-I-02-1369 for FY-2011 and provides funding through March 31, 2011.

This agreement is being incrementally funded in the amount of $94,163.30 for the period October 1, 2010 through March 31, 2011. Additional funding will be provided, by modification, when funds become available.

Total amount of agreement: $188,326.60

Add Items 0051 through 0062 as follows: (see pages 2 and 3).

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 Enadish, Program Manager	Donna Hutton
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED: 01/27/11
16B. UNITED STATES OF AMERICA (Signature of Contracting Officer)	16C. DATE SIGNED: 01/28/2011

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)
	Add Item 0051 as follows:				
0051	Basic FPPS and Payroll Operations Support based on 535 W2s at $195.00 per year.	1	LO	52,162.50	52,162.50
	Add Item 0052 as follows:				
0052	HRMS Integration (formerly W2 surcharge) based on 535 W2s @ $8.25 per year.	1	LO	2,206.88	2,206.88
	Add Item 0053 as follows:				
0053	Datamart Maintenance for Hyperion software based on past usage	1	LO	190.50	190.50
	Add Item 0054 as follows:				
0054	Leave and Earning Printing/Mailing based on 6% of 535 W2s mailed @ $9.50 per year.	1	LO	152.47	152.47
	Add Item 0055 as follows:				
0055	OPM Employee Express based on 535 W2s at $5.35 per year.	1	LO	1,431.12	1,431.12
	Add Item 0056 as follows:				
0056	Quicktime T&A based on 535 W2s at $39 per year.	1	LO	10,432.50	10,432.50
	Add Item 0057 as follows:				
0057	Workforce Tracking and Transformation System/Enter On Duty System (WTTS/EODS) based on 535 W2s @ $8.50 per year.	1	LO	2,273.75	2,273.75
	Add Item 0058 as follows:				
0058	Monster Hiring Management Enterprise covers Continued ...	1	LO	10,290.00	10,290.00

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)
	10/1/10 - 10/31/11 (13 months) based on 600 W2s @ $17.77 per year at $11,549. Includes MGS System Certification and Accreditation of $756 and NBC Administration Fee of $8,275.00 .				
	Add Item 0059 as follows:				
0059	Talent Management System includes LMM licensing for 600 users at $2.03/user ($1,218) O&M charges for 600 employee users @ $14.20/user ($8,520) Skillsoft Full Courseware with Legal Compliance Subscription based on 600 users at $23.78/subscription ($14,269.15) Skillsoft Environment, Safety and Health Subscription based on 120 users @ $46.25/user ($5,550)	1	LO	14,778.58	14,778.58
	Add Item 0060 as follows:				
0060	Training Database	1	EA	45.00	45.00
	Add Item 0061 as follows:				
0061	Training Class for 1 participant	1	EA	200.00	200.00
	ALL OTHER TERMS AND CONDITIONS REMAIN UNCHANGED AND IN FULL FORCE AND EFFECT.				

Form NBC-IA-01
(August 2002)

National Business Center
Inter/Intra Agency Agreement

1. Agreement Number: ***11-6420-PPS-CPS-40***	2. Action Type: ***New***
3. Period of Performance: Start Date: ***10/01/2010*** End Date: ***09/30/2011*** 4. FY: ***2011***	
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*** dkessler@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: 6110100	6e. NBC Appropriation Code: ***14X4523***
5f. Customer Account Number:	6f. Agreement Type: ***Fixed Price***
5g. Customer Obligating Doc Number: 0100A1DCC 2011 9994500000 EXTIT12400 253P0	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	$129,228.20		$129,228.20
B. HR Application Services. E-Gov Initiatives	$59,098.40		$59,098.40
Total Price	**$188,326.60**		**$188,326.60**

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).

Form NBC-IA-01
(August 2002)

Agreement Number: ***11-6420-PPS-CPS-40***

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

Economy Act, 31 USC 1535
Working Capital Fund 43 USC 1467, 1468 ✔
Other

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

This agreement may be terminated before the end performance date by ***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: ***Deborah Hamm***
Telephone Number: ***303-969-5437***

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.

13. Approvals

13a. Customer Approval	13b. NBC Approval
Signature: Donna Simpson Date: 1/27/11	Signature: Mishell R. English Date: 01/27/11
Name: Donna Simpson	Name: Mishell R. English
Title: Director, Office of Human Resources	Title: Program Manager
Signature: Donna Hutton Date: 1/28/11	Signature: LC Williams Date: 1/28/11
Name: Donna Hutton	Name: LC Williams
Title: CPSC Contracting Officer	Title: Associate Director

13c. For NBC Internal Use Only

	Signature: Date:
	Name: Aziza Djoumanov
	Title: Budget Office

Description of Services

11-6420-PPS-CPS-40

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	$104,325.00
• Base-level FPPS and Payroll operations support as stated n the SLA. Based on 535 W-2s at $195.00 per W-2 per year.		
QUICKTIME OPERATIONS & MAINTENANCE	Fixed	$20,865.00
• Time and Attendance support. Based on 535 W-2s at $39.00 per W-2 per year.		
EMPLOYEE EXPRESS	Fixed	$2,862.25
• Services provided through the OPM Employee Express program. Based on 535 W-2s at $5.35 per W-2 per year.		
DATAMART LICENSING MAINTENANCE	Fixed	$381.00
• Maintenance for Hyperion software licenses based on past usage.		
LEAVE AND EARNINGS STATEMENT (LES)	Fixed	$304.95
• LES printing and mailing costs. Based on 6% of 535 W-2s mailed at $9.50 per W-2 per year.		
TRAINING DATABASE	Fixed	$90.00
• Training database for clients to use for client-specific training needs.		
TRAINING	Fixed	$400.00
• Provide one training class		
Service A - Total		$129,228.20

Description of Services

11-6420-PPS-CPS-40

Service B - HR Application Services. E-Gov Initiatives

- HR Application Services. E-Gov Initiatives

Activity	Hours/Units	Amount
HRMS INTEGRATION (FORMERLY W2 SURCHARGE)	Fixed	$4,413.75
• Human Resources Management System (HRMS) integration. Based on 535 W2-s at $8.25 per W-2 per year.		
WORKFORCE TRACKING AND TRANSFORMATION SYSTEMS/ENTRANCE ON DUTY SYSTEM (WTTS/EODS)	Fixed	$4,547.50
• Operations and Maintenance based on 535 W-2s at $8.50 per W-2 per year.		
MGS HIRING MANAGEMENT ENTERPRISE	Fixed	$20,580.00
• MGS Hiring Management Enterprise subscriptions, covers 10/01/10 - 10/31/11 (13 months) at current discounted rate of $17.77/W2 based on 600 W-2s ($11,549) • MGS system Certification and Accreditation on behalf of customers charged each year ($756) • NBC administration fee charged each year ($8,275)		
TALENT MANAGEMENT SYSTEM	Fixed	$29,557.15
• LMM licensing for 600 users at $2.03/user ($1,218) • O&M charges for 600 employee users @ $14.20/user ($8,520) • Skillsoft Full Courseware with Legal Compliance Subcription based on 600 users at $23.78/subscription ($14,269.15) • Skillsoft Environment, Safety and Health Subscription based on 120 users @ $46.25/user ($5,550)		
Service B - Total		$59,098.40

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

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

I. BACKGROUND

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

II. PURPOSE

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

III. RESPONSIBILITIES

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

A: NBC RESPONSIBILITIES AND EXPECTATIONS RELATING TO CUSTOMERS

1. **The NBC:**
   - Publishes policies, standards, and procedures relating to all aspects of computer and information security.
   - Conducts continuity of operations planning to ensure the recoverability and continuity of services for all NBC customers in the event of a disaster or other unplanned outage.
   - Establishes and maintains policies and procedures for performing and storing backups, and for securing sensitive or restricted information contained in backups from unauthorized access.
   - Maintains systems security certification and accreditation (C&A) documentation for all GSSes and MAs for which the NBC is responsible. Copies of signed authority to operate (ATO) documents will be provided to customers on request.
   - Conducts regular security assessments and tests as prescribed in the Federal Information Security Management Act (FISMA) of 2002 and the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 2, "Recommended Security Controls for Federal Information Systems".
   - Ensures that appropriate background investigations are conducted for NBC employees and contractors.
   - Ensures that all NBC employees and contractors receive initial security awareness training before being given access to NBC-managed computer systems, and annual follow-up security awareness training as required by OMB Circular A-130, Appendix III, Department of the Interior Departmental Manual 375, Chapter 19, and the NBC Computer and Information Security Policy (NBCM-CIO-6300-001).
   - Endeavors to ensure through the use of policies and awareness training, that all NBC employees and contractors know how to identify sensitive or restricted information, and that they comply with requirements for marking, handling, disclosing, releasing, storing, retaining, copying or backing up, disposing of, sanitizing, or destroying such information.
   - Provides customers with reasonable assurance that IT resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. Such controls include physical controls, (e.g., keeping computers in locked rooms to limit physical access), logical controls (e.g., security software programs designed to prevent or detect unauthorized access to sensitive files), and personnel controls (e.g., background checks, security clearances, etc.) as required by Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors.
   - Follows stringent requirements of the Department of the Interior, and bureau-wide policies and guidelines requiring the use of firewalls, intrusion detection systems (IDS), and computer security incident response capabilities.
   - Applies appropriate communications security, in accordance with OMB, FIPS, NIST and

Departmental policies and standards.

- Uses antivirus software and ensures that current versions are used on all equipment, to include procedures for ensuring that portable devices such as laptops are updated as often as possible.
- Maintains a security management process designed to provide auditable records of request activity for access to customer data.
- Enforces the use of individually assigned User IDs and complex secret passwords that must be changed on a standardized cycle of password aging.
- Employs security procedures that apply when employees terminate employment or change jobs.
- Routinely monitors activity against sensitive application and system files to detect indicators of misuse or abuse and notifies customers whenever evidence of misuse or abuse of customer data has been detected.
- Provides ad hoc reporting to auditors and customers relating to various aspects of computer and information security.
- Acts as Subject Matter Experts for computer and information security matters for the NBC and its customers.
- Provides a Computer Security Incident Response Capability in the event of a successful penetration attack against an NBC system and notifies customers whenever a computer security incident occurs that involves or threatens the customer's application or data.

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

     Customers may elect to have one Data Custodian for the entire organization or may choose to designate separate individuals for each MA. Similarly, depending on the size of the organization, a Data Custodian may also perform the function of SPOC.
   - Ensuring that appropriate background investigations are conducted for all customer employees and contractors who will access an NBC-managed computer system or application, in accordance with HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors.
   - Ensuring that all customer employees and contractors, who have a business requirement to connect to and log on to an NBC-managed computer system or application, AND who are subject to the requirements of OMB Circular A-130, Appendix III, receive initial security awareness training before being given access to NBC-managed systems, and annually thereafter.
   - Acknowledging that the security of customer data is ultimately the responsibility of the customer organization. Except for the actions of customer end-users, the NBC is responsible for the security of customer data while it is housed and processed in the NBC data center. Customers are responsible for having an auditable internal process for documenting requests for access to customer data. According to the Federal Information System Controls Audit Manual (FISCAM) the process should include such things as:
     - Standard forms to document access requests. Request documentation should be retained in active archives for as long as the user remains with the organization.
     - A procedure to document the approval of access requests by senior managers or by designated access approval authorities within the organization.
     - A process to ensure secure transfer of access request documentation to customer security representatives.
     - Periodic reviews of access authorizations to determine if they remain appropriate.
   - Informing the NBC, as part of the Interagency Agreement (IAA) process of:
     - Information sensitivity classification(s) associated with customer data, that **exceed** the information sensitivity classifications currently processed and managed by the NBC, (e.g., anything more restrictive than Controlled Unclassified Information (CUI)). Also include any special handling requirements that **exceed** those currently being enforced by the NBC for its customers.

- o Any special data backup requirements that would **exceed** the nightly and weekly data backup standard currently being provided for NBC customer data.

  Also see Section B. relating to this subject.

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

3. **The customer Data Custodian, for organizations whose employees and contractors have a business need to connect to and log on to an NBC-managed computer system or application, is responsible to:**
   - Coordinate with NBC IT Security to establish and maintain security of data belonging to the customer organization.
   - Identify appointments to NBC IT Security, in writing, for individuals to serve as Security Points of Contact (SPOCs) for the customer organization. (This requirement is satisfied through the completion of NBC forms (DEN-NBC-IT-02 and 03).
   - Ensure that customer employees and contractors behave in a manner that is appropriate to the use and protection of NBC-managed computer systems and applications, based on applicable government security guidelines and recommendations.

     NOTE: Section VI of this SSA contains application-specific rules of behavior (ROB) for NBC-managed systems. These ROB are provided in compliance with OMB Circular A-130, Appendix III, paragraph 3., a., 2), a). The ROB portion of this SSA should be removed by the customer and provided to the customer data custodian(s). The ROB may be used at the customer's discretion to ensure application users behave in a manner appropriate for the security and protection of federal computer systems.
   - Authorize the NBC, in writing, to access customer data to the extent necessary to perform normal data center operational functions (e.g., system performance, system backup and recovery, resource utilization analysis), and normal database maintenance and support functions (e.g., database performance, database backup and recovery, database utilization analysis) as required.
4. **The SPOC, for organizations whose employees and contractors have a business need to connect to and log on to an NBC-managed computer system or application, is responsible to:–**
   - Coordinate local security administration activities between NBC IT Security and the assigned area of responsibility.
   - Administer security on NBC-owned and managed systems, in accordance with all requirements of the NBC Rules of Behavior for SPOCs, which are completed during the SPOC assignment process.
   - Submit customer requests for access to NBC IT systems or applications via NBC-approved methods (e.g., electronic or hardcopy forms, etc.) that are current at the time of the submission.
   - Notify NBC IT Security when any customer employee or contractor who has access to an NBC-managed computer system terminates employment or for any other reason no longer requires access to an NBC-managed computer system.
   - Participate in periodic security audits with NBC IT Security representatives to ensure that all User IDs have been assigned proper privileges (e.g., minimum access required to perform the user's duties), and that the User IDs are deleted when the users are separated, transferred, or for any other reason no longer require access to the NBC system.
5. **Whenever customer employees and contractors have a business need to access (e.g., connect to, and log on to) an NBC-managed computer system or application, customer agrees to be responsible for implementing and overseeing end-user compliance with appropriate security-related activities. For example, the customer agrees to endeavor to ensure that end-users:–**
   - Use NBC-managed computer hardware, programs, and data for work-related purposes only.
   - Do not share User ID or logon password with anyone at any time.
   - Choose complex passwords that are difficult to guess, to minimize the risk of having the system compromised as a result of poor password selection.
   - Change exposed or compromised passwords immediately.

- Contact the customer Security Point of Contact (SPOC) if problems are encountered with his/her User ID, password, or other access.
- Are personally accountable for all actions associated with the use of his/her assigned User ID.
- Lock the workstation keyboard or log off when leaving the workstation area to prevent unauthorized use of the User ID.
- Are responsible for the appropriate use and protection of sensitive information to which he/she has authorized access.
- Immediately report all computer security incidents (viruses, intrusion attempts, system compromises, etc.) to his/her SPOC.

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

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

1. NBC PRODUCTS AND SERVICES

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

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

2. INFORMATION SENSITIVITY

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

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

- Special network or data isolation **beyond that which currently exists**.
- Special markings affixed to printed media **beyond those already in use**.
- Special employee security clearances **above those already in place** for NBC employees and contractors.

IV. NBC IT SECURITY POINTS OF CONTACT

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

V. NBC RULES OF BEHAVIOR (ATTACHED)

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

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

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

These rules are based on Office of Management and Budget (OMB) Circular A-130, Appendix III, Department of the Interior (DOI) Departmental Manual 375, Chapter 19 (375 DM 19), and the NBC Computer and Information Security Policy (NBCM-CIO-6300-001). These rules apply to all users of NBC computer systems.

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

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

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

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

Because network-based systems are inherently insecure, users should take appropriate measures to protect sensitive information. CLICK HERE for the NBC Information Classification and Handling Policy, NBCM-CIO-6300-003.

COMPUTER USE

- National Security Information (NSI Classified Data) may NOT be entered into any NBC

computer system. **In the event that National Security Information is accidentally transmitted to an NBC system, the local IT Security Manager must be contacted immediately.**

- **NBC and other DOI computer hardware, programs, and data are considered to be the property of the U.S. Government.** Except as allowed by the DOI Policy on Limited Personal Use of Government Office Equipment (available on the DOI Web site at http://www.doi.gov/ethics/docs/personaluse.pdf), Government-owned or Government-leased computers, software, and telecommunications systems are to be used for work-related purposes only. Resources are not to be used to conduct or support a personal business; and no personally owned data or software shall be entered into an NBC system, LAN, or personal computer.

- **Unofficial (personal) use of Government-owned IT resources** – As noted above, the DOI Policy on Limited Personal Use of Government Office Equipment spells out the rules and conditions governing personal use of IT resources (e.g., computers, printers, E-mail, Internet, etc). This policy is available on the DOI Web site at http://www.doi.gov/ethics/docs/personaluse.pdf. Whenever there is a question or a doubt about the propriety of personal use of any Government-owned IT resource, refer to the DOI Policy on Limited Personal Use of Government Office Equipment or to the local IT Security Manager.

PASSWORDS AND USER IDS

- **Passwords** for all NBC computer systems:
  - Are considered private and confidential. Users are prohibited from sharing any of their system passwords with anyone.
  - To minimize the risk of having the system compromised because of poor password selection, users are responsible for selecting passwords that are difficult to guess. Wherever technically supported, as many as possible of the following password selection criteria should be employed:
    - Passwords must be at least eight or more characters in length.
    - Passwords should contain a mix of both upper and lower case letters.
    - There must be at least one numeric character (0, 1, 2, 3...9).
    - New (changed) passwords must not be revisions of an old password. Reuse of the same password with a different prefix or suffix (A, B, C, etc.) is not permitted.
    - Dictionary words, derivatives of User IDs, and common character sequences such as "123456" may not be used.
    - Personal details such as a spouse's name, license plates, social security numbers, and birthdays should not be used unless accompanied by additional unrelated characters.
    - Proper names, geographical locations, common acronyms, and slang should **not** be used.
- If exposed or compromised, passwords must be changed immediately.
- **User Identifiers (User IDs)** are required for all users for access to NBC computer systems. Each user must be uniquely identified. **The User ID possesses privileges that are tailored to the duties of the individual user's job and to the individual user's level of "need-to-know".** Each change in access must be approved.

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

- When employment terminates, each NBC system to which a user has access must be identified and the access terminated. This is accomplished on the checkout form completed by the user and supervisor on the last day of employment during the exit/clearance process. When employment termination is involuntary, is a result of natural or accidental death, or is caused by any other circumstance that precludes the user from performing the exit/clearance process, then it is the responsibility of the employee's immediate supervisor to expediently provide the notification(s).

NOTE: The terms "Security Point of Contact" and "SPOC" refer to any individual who has been delegated security responsibilities for administering user accounts (User IDs, passwords, access authorities, etc.), regardless of platform. When the user is a contractor, the Government responsible manager or Contracting Officer's Representative is the supervisor for the purposes of these Rules of Behavior.

- If problems are encountered with a User ID, the supervisor or SPOC must be contacted. CLICK HERE for the NBC Computer and Information Security Policy, NBCM-CIO-6300-001.

USER ACCOUNTABILITY

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

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

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

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

AUTHORIZED ACCESS

- **Users are responsible for the appropriate use and protection of sensitive information to which they have authorized access.** The use of such information for anything other than "official Government business" is expressly prohibited. Users are responsible for adequately protecting any sensitive or Privacy Act data entrusted to them. Users are prohibited from disclosing, without proper authorization, sensitive or Privacy Act information to individuals who have not been authorized to access the information.

- **Due to the high sensitivity of Individual Indian Trust Data (IITD) and Tribal Trust Data (TTD)**, users must take extra care and precautions to protect any files or data entrusted to them related to IITD/TTD from unauthorized access.

- Casual browsing of sensitive or Privacy Act information, such as personnel data, is not appropriate and is prohibited. Users should only access this data when there is an official business reason.

For details:
CLICK HERE for the NBC Computer and Information Security Policy, NBCM-CIO-6300-001.
and
CLICK HERE for the NBC Information Classification and Handling Policy, NBCM-CIO-6300-003.

UNAUTHORIZED ACCESS

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

DATA PROTECTION

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

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

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

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

DENIAL OF SERVICE

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

MALICIOUS (HOSTILE) SOFTWARE

- **Users must not intentionally write, compile, copy, propagate, execute, or attempt to introduce** any computer code designed to self-replicate, damage, or otherwise hinder the performance of any DOI or NBC computer system. Examples of these would be computer viruses, worms, and Trojan horses. -

For details: CLICK HERE for the NBC Computer and Information Security Policy, NBCM-CIO-6300-001.

-

BYPASSING SYSTEM SECURITY CONTROLS

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

- **Workers must not test or probe security mechanisms** at either the NBC or external installations unless they have first obtained permission from the NBC IT Security Manager.

COPYRIGHT LAWS AND LICENSE REQUIREMENTS

- **Commercially developed software.** Commercially developed software must be treated as the proprietary property of its developer. Title 17 of the U.S. Code states that it is illegal to make or distribute copies of copyrighted material without authorization. The only exception is the user's right to make a backup for archival purposes assuming the manufacturer does not provide one. It is illegal to make copies of software for any other purposes without the written permission of the copyright owner. Making or using unauthorized copies of copyrighted products from a DOI or NBC computer system is illegal and is expressly prohibited.

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

- **Personally owned software.** Users may not install personally owned software on DOI or NBC-owned computer systems. This includes but is not limited to personally owned screensaver software. An employee who has any doubt as to the appropriateness of installing personally owned software on a DOI or NBC-owned computer system should check with his or her supervisor for guidance.

CONNECTING TO THE INTERNET

NBC personnel are provided with the equipment and Internet connection to accomplish the work of the NBC. Limited personal use of the Internet is governed

by the DOI Policy on Limited Personal Use of Government Office Equipment (available on the DOI Web site at http://www.doi.gov/ethics/docs/personaluse.pdf). Workers on **non-duty** time are allowed to use the Internet for personal use in accordance with the DOI Internet Acceptable Use Policy (available on the DOI Web site at http://www.doi.gov/ethics/docs/internet.html). Except as prohibited by the DOI Internet Acceptable Use Policy, workers are allowed minimal personal purchases through the Internet, but only during non-duty time. Non-duty time is determined by DOI and NBC management and is limited to official breaks, lunch, and before and after duty hours. When making such purchases, however, employees must arrange for the purchases sent to a non-Government address. Employees are prohibited from using Government office equipment at any time to make purchases for personal commercial gain activity. The prohibited activities listed in the DOI Internet Acceptable Use Policy include but are not limited to:

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

RECORD RETENTION REQUIREMENTS

- **Users must follow DOI and NBC records management policies** (available on the DOI Web site at http://www.doi.gov/ocio/records). Any documents or E-mail created may be considered Federal records that must be preserved by being printed and filed and may not be deleted from the system before being saved in the system's backup process.
- **Record Retention Requirements for Cobell v. Norton litigation.** Users must print and file, in accordance with applicable Court and Departmental directives, any documents they have or create and any E-mail messages they send or receive, including attachments, that relate to the three functional areas of:
  - American Indian Trust Reform, including the High-Level Implementation Plan or any of its subprojects;
  - The Cobell v. Norton litigation; or
  - Administration of Individual Indian Money (IIM) accounts.

COMPUTER SECURITY INCIDENTS

- **Users and management are required to report all computer security incidents** (viruses, intrusion attempts, system compromises, offensive E-mail, inadequate protection of sensitive data, etc.) to the NBC Cyber Security Operations Team Desk at (303)-969-5434.
  - For additional assistance, users may contact the NBC Customer Service Center (CSC) at 1-888-367-1622.
  - **Users are responsible for cooperating with NBC IT System Administration and IT Security staff and the local IT Security Manager** during the investigation of a computer security incident.

USER RESPONSIBILITY

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

- **Individual accountability.** Users will be held accountable for their actions on DOI and NBC IT systems. If a user adversely impacts the operation of a DOI or NBC IT system, the employee's access may be removed without notice to ensure the operation and availability for the rest of the system users.

End.