SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE	OF
REQ-2400-16-0071	1	29

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
GS-35F-348DA	09/29/2016	CPSC-F-16-0090	CPSC-Q-16-0067	07/07/2016

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	Greg Grayson	301-504-7725	

9. ISSUED BY	CODE	10. THIS ACQUISITION IS
CONSUMER PRODUCT SAFETY COMMISSION DIV OF PROCUREMENT SERVICES 4330 EAST WEST HWY ROOM 523 BETHESDA MD 20814	FMPS	☐ UNRESTRICTED OR ☒ SET ASIDE: 100.00 % FOR: ☒ SMALL BUSINESS ☐ HUBZONE SMALL BUSINESS ☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS ☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM ☐ EDWOSB ☐ 8(A) NAICS: 541519 SIZE STANDARD: $27.5

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING	14. METHOD OF SOLICITATION
☐ SEE SCHEDULE	SB/Net 30	☐		☐ RFQ ☐ IFB ☐ RFP

15. DELIVER TO	CODE	16. ADMINISTERED BY	CODE
CONSUMER PRODUCT SAFETY COMMISSION OFFICE OF INFORMATION SERVICES 4330 EAST WEST HWY ROOM 839-23 BETHESDA MD 20814	EXIT	CONSUMER PRODUCT SAFETY COMMISSION DIV OF PROCUREMENT SERVICES 4330 EAST WEST HWY ROOM 523 BETHESDA MD 20814	FMPS

17a. CONTRACTOR/ OFFEROR	CODE	FACILITY CODE	18a. PAYMENT WILL BE MADE BY	CODE
KONIAG SERVICES INC 4100 LAFAYETTE CENTER DRIVE SUITE 303 CHANTILLY VA 20151-1234 TELEPHONE NO	[redacted]		CPSC Accounts Payable Branch AMZ 160 P.O. Box 25710 Oklahoma City OK 73125	FMFS

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19 ITEM NO	20. SCHEDULE OF SUPPLIES/SERVICES	21 QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	DUNS Number: [redacted] Contracting Officer Representative: Name: Amelia (Amy) Shifflett Tel: 301-504-7172 Email: ashifflett@cpsc.gov The Contractor shall provide all necessary personnel and services in the preparation of documents on plans, policies, and procedures as it relates to information security in accordance with Statement of Work, GSA contract number *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA	26. TOTAL AWARD AMOUNT (For Govt. Use Only)
0100A16DSE-2016-5457500000-EXIT002400-251A0	$921,636.64

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☐ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

☐ 29. AWARD OF CONTRACT: _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)
	Eddie Ahmad

30b. NAME AND TITLE OF SIGNER (Type or print)	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER (Type or print)	31c. DATE SIGNED
		Eddie Ahmad	9/29/16

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 2/2012)
Prescribed by GSA - FAR (48 CFR) 53.212

19 ITEM NO	20 SCHEDULE OF SUPPLIES/SERVICES	21 QUANTITY	22 UNIT	23 UNIT PRICE	24 AMOUNT
	GS-35F-348DA, the Contractor's quote dated July 29, 2016 and the attached terms and conditions. The Contractor shall invoice in accordance with the payment schedule noted in their price proposal. Period of Performance: 09/29/2016 to 09/28/2017				
0001	Contingency Planning Support, Configuration Management and Risk Management Support Services for the U.S. Consumer Product Safety Commission, Office of Information & Technology Services in accordance with attached Statement of Work The total amount of award: $921,636.64. The obligation for this award is shown in box 26.				921,636.64

32a QUANTITY IN COLUMN 21 HAS BEEN

[ ] RECEIVED [ ] INSPECTED [ ] ACCEPTED AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED _____

32b SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c DATE	32d PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE
32e MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32f TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32g E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33 SHIP NUMBER [ ] PARTIAL [ ] FINAL	34 VOUCHER NUMBER	35 AMOUNT VERIFIED CORRECT FOR	36 PAYMENT [ ] COMPLETE [ ] PARTIAL [ ] FINAL	37 CHECK NUMBER
38 S/R ACCOUNT NUMBER	39 S/R VOUCHER NUMBER	40 PAID BY		

41a I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a RECEIVED BY *(Print)*	
41b SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c DATE	42b RECEIVED AT *(Location)*	
		42c DATE REC'D *(YY/MM/DD)*	42d TOTAL CONTAINERS

Performance Work Statement
Contingency Planning Support

1 Description of Services

The Contractor shall provide all necessary personnel and services to develop plans, policies, and procedures as it relates to Information Security at the U.S Consumer Product Safety Commission.

2 Background

The E-Government Act (P.L. 107-347) passed by the one hundred and seventh Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for agencies to develop, document, and implement an agency-wide program to provide information security for the information systems that support its operations and assets. The ultimate goal of FISMA is to conduct the day-to-day operations of the agency and to accomplish the agency's stated missions with what the Office of Management and Budget (OMB) Circular A-130 defines as adequate security, or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

3 Contract Type

This procurement shall be a firm-fixed-price, performance-based contract.

4 Description of Work

The requirements in this Statement of Work (SOW) are to support the documentation and related activities that FISMA requires as specified in the National Institute of Standards and Technology (NIST) Special Publications series and Federal Information Processing Standards. The basis for all security work is that CPSC information has value and that the mission of the agency to provide services authorized by Congress is fully supported by the information and systems it owns without disruption, alteration or unauthorized disclosure.

5 Task 1: Contingency Planning Support

The contractor shall provide contingency planning support services to support the operation of the CPSC General Support System Local Area Network (GSS LAN) and the CPSC Major Applications (CPSRMS, DCM, CPSC.GOV, and ITDS-RAM). The work may involve interviewing agency staff, facilities security and management staff, application system support contractors, infrastructure support staff, application systems owners and users, business process managers, and IT security staff. This work will involve developing contingency planning (CP) documentation in accordance with NIST, OMB, Federal guidelines, and commercial best practices. The contractor shall review existing documents, such as security plans, application

system input and output documents, C&A packages, user guides, operational procedures, security policies, risk assessments, security assessments, audits, and POAMs.

Contingency Planning (CP) applies to information systems, and provides the steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency.

5.1 Task 1.1: Develop Business Impact Analysis (BIA)

The BIA is a key step in implementing the CP controls in NIST SP 800-53 and in the contingency planning process overall. The BIA is used to determine contingency planning requirements and priorities. The Contractor shall:

1. Conduct a Business Impact Analysis which correlates CPSC information systems with the agency's critical mission/business processes and services, and based on that information, characterizes the consequences of a disruption.

The Contractor must complete the following three steps in accomplishing the BIA:

1. **Identify critical information system assets supporting essential missions/business functions.**

2. **Determine mission/business processes and recovery criticality.** Mission/Business processes supported by the system are identified and the impact of a system disruption to those processes is determined **along with outage impacts and estimated downtime.** The downtime should reflect the maximum time that an agency mission/business unit can tolerate while still maintaining the mission.

3. **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.

4. **Identify recovery priorities for system resources.** Based upon the results from the previous activities, system resources should be linked more clearly to critical mission/business processes and functions. Priority levels should be established for sequencing recovery activities and resources.

5.2 Task 1.2: Develop Information System Contingency Plans (ISCP)

The Information System Contingency Plan (ISCP) establishes comprehensive procedures to recover critical agency information systems quickly and effectively following a service

disruption. The Contractor shall develop ISCPs for the GSS LAN, CPSRMS, DCM and CPSC.GOV. Each ISCP shall meet the following requirements:

1. Plans shall contain detailed roles, responsibilities, teams, and procedures associated with restoring an information system following a disruption.
2. Plans shall document technical capabilities designed to support contingency operations and should be tailored to the organization and its requirements.
3. Plans shall be formatted to provide quick and clear directions in the event that personnel unfamiliar with the plan or the systems are called on to perform recovery operations.
4. Plans shall be clear, concise, and easy to implement in an emergency. Where possible, checklists and step-by-step procedures shall be used.
5. Plans shall include the following subsections:

    a. **Background.** This subsection establishes the reason for developing the ISCP and defines the plan objectives.

    b. **Scope.** The scope identifies the FIPS 199 impact level and associated RTOs as well as the alternate site and data storage capabilities (as applicable).

    c. **Assumptions.** This section includes the list of assumptions that were used in developing the ISCP as well as a list of situations that are not applicable. See Appendix A Sample Information System Contingency Plan Templates, for a sample of assumptions and situations.

    d. **System description**. It is necessary to include a general description of the information system addressed by the contingency plan. The description should include the information system architecture, location(s), and any other important technical considerations. An input/output (I/O) diagram and system architecture diagram, including security devices (e.g., firewalls, internal and external connections) are useful. The content for the system description can usually be taken from the System Security Plan.

    e. **Overview of three phases**. The ISCP recovery is implemented in three phases: (1) Activation and Notification, (2) Recovery, and (3) Reconstitution.

    f. **Roles and responsibilities**. The roles and responsibilities section presents the overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams. The section also provides an overview of team member roles and responsibilities in a contingency situation. Teams and team members should be designated for specific response and recovery roles during contingency plan activation.

g. **Activation and Notification Phase.** The Activation and Notification Phase defines initial actions taken once a system disruption or outage has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the plan. At the completion of the Activation and Notification Phase, ISCP staff will be prepared to perform recovery measures to restore system functions.

h. **Notification Procedures.** Notification procedures should be documented in the plan for outages or disruptions that may or may not have advanced notice. The procedures should describe the methods used to notify recovery personnel during business and non-business hours. Personnel to be notified should be clearly identified in contact lists appended to the plan.

i. **Outage Assessment.** To determine how the ISCP will be implemented following a system disruption or outage, it is essential to assess the nature and extent of the disruption. The outage assessment should be completed as quickly as the given conditions permit, with personnel safety remaining the highest priority. When possible, the Outage Assessment Team is the first team notified of the disruption. Outage assessment procedures may be unique for the particular system, but the following minimum areas should be addressed:

    i. Cause of the outage or disruption;
    ii. Potential for additional disruptions or damage;
    iii. Status of physical infrastructure (e.g., structural integrity of computer room, condition of electric power, telecommunications, and heating, ventilation and air-conditioning [HVAC]);
    iv. Inventory and functional status of system equipment (e.g., fully functional, partially functional, nonfunctional);
    v. Type of damage to system equipment or data (e.g., water, fire and heat, physical impact, electrical surge);
    vi. Items to be replaced (e.g., hardware, software, firmware, supporting materials); and
    vii. Estimated time to restore normal services.

j. **Recovery Phase.** Formal recovery operations begin after the ISCP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location. At the completion of the Recovery Phase, the information system will be functional and capable of performing the functions identified in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual

processing, recovery and operation at an alternate system, or relocation and recovery at an alternate site. It is feasible that only system resources identified as high priority in the BIA will be recovered at this stage.

k. **Sequence of Recovery Activities.** When recovering a complex system, such as a wide area network (WAN) or virtual local area network (VLAN) involving multiple independent components, recovery procedures should reflect system priorities identified in the BIA. The sequence of activities should reflect the system's MTD to avoid significant impacts to related systems. Procedures should be written in a stepwise, sequential format so system components may be restored in a logical manner.

l. **Recovery Procedures.** To facilitate Recovery Phase operations, the ISCP should provide detailed procedures to restore the information system or components to a known state. Procedures should be assigned to the appropriate recovery team and typically address the following actions:

    i. Obtaining authorization to access damaged facilities and/or geographic area;
    ii. Notifying internal and external business partners associated with the system;
    iii. Obtaining necessary office supplies and work space;
    iv. Obtaining and installing necessary hardware components;
    v. Obtaining and loading backup media;
    vi. Restoring critical operating system and application software;
    vii. Restoring system data to a known state;
    viii. Testing system functionality including security controls;
    ix. Connecting system to network or other external systems; and
    x. Operating alternate equipment successfully.

m. **Reconstitution Phase.** The Reconstitution Phase is the third and final phase of ISCP implementation and defines the actions taken to test and validate system capability and functionality. During Reconstitution, recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. This phase consists of two major activities: validating successful recovery and deactivation of the plan. Validation of recovery typically includes these steps:

    i. **Concurrent Processing.** Concurrent processing is the process of running a system at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly and securely.

ii. **Validation Data Testing**. Data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely and are current to the last available backup.

iii. **Validation Functionality Testing**. Functionality testing is a process for verifying that all system functionality has been tested, and the system is ready to return to normal operations.

n. **Deactivation.** Deactivation of the plan is the process of returning the system to normal operations and finalizing reconstitution activities to prepare the system against another outage or disruption. These activities include:

i. **Notifications**. Upon return to normal operations, users should be notified by the ISCP Coordinator (or designee) using predefined notification procedures.

ii. **Cleanup**. Cleanup is the process of cleaning up work space or dismantling any temporary recovery locations, restocking supplies, returning manuals or other documentation to their original locations, and readying the system for another contingency event.

iii. **Offsite Data Storage**. If offsite data storage is used, procedures should be documented for returning retrieved backup or installation media to its offsite data storage location.

iv. **Data Backup**. As soon as reasonable following reconstitution, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup should be stored with other system backups and comply with applicable security controls.

v. **Event Documentation**. All recovery and reconstitution events should be well documented, including actions taken and problems encountered during the recovery and reconstitution efforts. An after-action report with lessons learned should be documented and included for updating the ISCP.

o. **Plan Appendices.** Contingency plan appendices provide key details not contained in the main body of the plan. Common contingency plan appendices include the following:

i. Contact information for contingency planning team personnel;

ii. Vendor contact information, including offsite storage and alternate site POCs;

iii. BIA;

iv. Detailed recovery procedures and checklists;
v. Detailed validation testing procedures and checklists;
vi. Equipment and system requirements lists of the hardware, software, firmware, and other resources required to support system operations. Details should be provided for each entry, including model or version number, specifications, and quantity;
vii. Alternate mission/business processing procedures that may occur while recovery efforts are being done to the system;
viii. ISCP testing and maintenance procedures;
ix. System interconnections (systems that directly interconnect or exchange information); and
x. Vendor SLAs, reciprocal agreements with other organizations, and other vital records.

5.3 Task 1.3: Conduct Contingency Plan Testing

The Contractor shall develop contingency plan test procedures and then coordinate a **tabletop** exercise designed to determine the effectiveness of each contingency plan and the organizational readiness to execute each plan.

5.4 Task 1: Deliverables

Deliverable due dates are reflected in actual dates where warranted. Otherwise due dates are specified in weeks or months after contract award (ACA).

Deliverable	Due Date, Format (NLT-No Later Than)
Business Impact Analysis	• 180 calendar days prior to the end of the period of performance
Information System Contingency Plan – GSS LAN	• 60 calendar days prior to the end of the period of performance
Information System Contingency Plan – CPSRMS	• 60 calendar days prior to the end of the period of performance
Information System Contingency Plan – DCM	• 60 calendar days prior to the end of the period of performance
Information System Contingency Plan – CPSC.GOV	• 60 calendar days prior to the end of the period of performance

Information System Contingency Plan – GSS LAN	• 60 calendar days prior to the end of the period of performance
Information System Contingency Plan Test – GSS LAN	• 30 calendar days prior to the end of the period of performance
Information System Contingency Plan Test – CPSRMS	• 30 calendar days prior to the end of the period of performance
Information System Contingency Plan Test – DCM	• 30 calendar days prior to the end of the period of performance
Information System Contingency Plan Test – CPSC.GOV	• 30 calendar days prior to the end of the period of performance
Information System Contingency Plan – ITDS-RAM	• 30 calendar days prior to the end of the period of performance
Information System Contingency Plan Test – ITDS-RAM	• 30 calendar days prior to the end of the period of performance

All deliverables are to be provided in MS Word and PDF format to the COR for review and comment. Comments shall be provided by the CPSC COR within 5 business days of each deliverable receipt from the contractor. Comments from CPSC shall be addressed by the contractor and revised deliverables provided within 5 business days of receiving comments from the CPSC COR.

6 Task 2: Configuration Management Support

The contractor shall provide system configuration management support services to support the operation of the CPSC General Support System Local Area Network (GSS LAN) and the CPSC Major Applications (CPSRMS, DCM, CPSC.GOV, and ITDS-RAM). The work may involve interviewing agency staff, facilities security and management staff, application system support contractors, infrastructure support staff, application systems owners and users, business process managers, and IT security staff. This work will involve developing configuration management (CM) documentation in accordance with NIST, OMB, Federal guidelines, and commercial best practices. The contractor shall review existing documents, such as security plans, application system input and output documents, C&A packages, user guides, operational procedures, security policies, risk assessments, security assessments, audits, and POAMs.

Configuration Management (CM) comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.

6.1 Task 2.1: Develop Configuration Management Plans

The agency must develop procedures to facilitate the implementation of the agency's configuration management policy and associated configuration management controls. The Contractor shall:

a) Develop a configuration management plan for each in-scope system (in accordance with guidance provided by NIST Special Publication 800-128)—which includes: the GSS LAN, CPSRMS, DCM, CPSC.GOV, and ITDS-RAM. The CM plan is a comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems. Each individual CM plan must:

1) Briefly describe the subject information system;
2) Document a component inventory for the system;
3) Document information system configuration items;
4) Document the rigor to be applied to managing changes to configuration items (e.g., based on the impact level of the information system);
5) Document the CM roles and responsibilities;
6) Provide identification and composition of the group or individual(s) that consider change requests;
7) Document configuration change control procedures to be followed (including references to organization-wide procedures);
8) Document the location where CM artifacts (change requests, approvals, etc.) are maintained (e.g., media libraries);
9) Document access controls employed to control changes to configurations;
10) Document access controls to protect CM artifacts, records, reports, etc. (e.g., commensurate with system impact level);
11) Document CM tools that are used;
12) Document common secure configurations (e.g., FDCC/USGCB, DISA STIGs, National Checklist Program, etc.) to be used as a basis for establishing approved baseline configurations for the information system;
13) Document deviations from common secure configurations for configuration items including justifications;
14) Identify criteria for approving baseline configurations for the information system;
15) Identify procedures for handling of exceptions to the CM plan (e.g., location of CM artifacts, configuration change control procedures, etc.).

b) Additionally, CM plans must include the following components:

1) *Templates* - Establish templates related to CM that integrate the organization-wide CM policy and procedures and allow individual system owners to fill in information specific to their information system.
2) *IS Component Inventory* – Describe how components are to be managed within the inventory (e.g., how new components are added to the inventory, what information

about each component is tracked, and how updates are made including removal of retired components). If automated tools are to be used, factors such as how often they will run, who will administer them, who will have access, and how they will be audited are described.

3) *Baseline Configuration* – Identify the steps for creation of a baseline configuration, content of the baseline configuration, approval of the initial baseline configuration, maintenance of the baseline configuration (i.e., when it should be updated and by whom), and control of the baseline configuration.
4) *Common Secure Configurations* – Identify commonly recognized and standardized secure configurations to be applied to configuration items. The common secure configurations specified in the procedure are derived from established federal, organizational, or industry specifications (the National Checklist Program contains references to common secure configurations such as the United States Government Configuration Baseline (USGCB), Federal Desktop Core Configuration (FDCC), Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs), Center for Internet Security (CIS) Benchmarks, etc.). Where possible, common secure configurations use SCAP-expressed content. Deviations from the common secure configurations are also addressed (e.g., identification of acceptable methods for assessing, approving, documenting, and justifying deviations to common secure configurations, along with identification of controls implemented to mitigate risk from the deviations), in the event that the configuration for a given system must diverge from the defined configuration due to mission requirements or other constraints.
5) *Patch Management* – Define the organizational patch management process and how it is integrated into CM, how patches are prioritized and approved through the configuration change control process, and how patches are tested for their impact on existing secure configurations. Also defines how patches are integrated into updates to approved baseline configurations and how patch implementation is controlled (access controls, etc.).
6) *Configuration Change Control* – Identify the steps to move a configuration change from its initial request to eventual release into the operational environment.
7) *Help Desk Procedures* – Describe how change requests originating through the help desk are recorded, submitted, tracked, and integrated into the configuration change control process.
8) *Monitoring* – Describe how monitoring activities and related reports are applied to assess the secure state of the information system, and how to identify when the actual configuration becomes different in some way from the approved baseline configuration (i.e., unauthorized change) within an information system through analysis of monitoring and reporting activities.

6.2 Task 2.2: Develop Baseline Configuration Documents

The baseline configuration of an information system includes the sum total of the secure configurations of its constituent CIs and represents the system-specific configuration against which all changes are controlled.

The agency must document baseline configurations for each major component of the GSS LAN, CPSRMS, DCM, CPSC.GOV, and ITDS-RAM. The baseline configuration is a set of specifications for a system that have been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes. The Contractor shall:

a) Develop a baseline configuration document for each identified configuration item (CI) of the GSS LAN, CPSRMS, DCM, CPSC.GOV, and ITDS-RAM. In-scope CIs include a combination of operating systems, hardware, and software. Each individual baseline configuration document must:

    1) Document the types of information that are associated with a CI and may include:
        i. The information system of which the CI is a part;
        ii. Logical and/or physical placement within the system;
        iii. Ownership and management information;
        iv. Inventory of IS components that makes up the CI;
        v. Version numbers for components and non-component objects;
        vi. Relationship to/dependencies on other CIs within the system;
        vii. Information related to custom software used within the CI;
        viii. IT products or components common secure configurations; and
        ix. Any other information needed to rebuild or reconstitute the CI.

    2) Document secure baseline settings for each configuration item including, but not limited to:

        i. OS and application features (enabling or disabling depending on the specific feature, setting specific parameters, etc.);
        ii. Services (e.g., automatic updates) and ports (e.g., DNS over port 53);
        iii. Network protocols (e.g., NetBIOS, IPv6) and network interfaces (e.g., Bluetooth, IEEE 802.11, infrared);
        iv. Methods of remote access (e.g., SSL, VPN, SSH, IPSEC);
        v. Access controls (e.g., controlling permissions to files, directories, registry keys, and restricting user activities such as modifying system logs or installing applications);
        vi. Management of identifiers/accounts (e.g., changing default account names, determining length of time until inactive accounts are disabled, using unique user names, establishing user groups);
        vii. Authentication controls (e.g., password length, use of special characters, minimum password age, multifactor authentication/use of tokens);

viii. Audit settings (e.g., capturing key events such as failures, logons, permission changes, unsuccessful file access, creation of users and objects, deletion and modification of system files, registry key and kernel changes);
ix. System settings (e.g., session timeouts, number of remote connections, session lock); and
x. Cryptography (e.g., using FIPS 140-2-validated cryptographic protocols and algorithms to protect data in transit and in storage);
xi. Applying vendor-released patches in response to identified vulnerabilities, including software updates;
xii. Using approved, signed software, if supported;
xiii. Implementing safeguards through software to protect end-user machines against attack (e.g., antivirus, antispyware, anti-adware, personal firewalls, host-based intrusion detection systems [HIDS]);
xiv. Applying network protections (e.g., TLS, IPSEC);
xv. Establishing the location where a component physically and logically resides (e.g., behind a firewall, within a DMZ, on a specific subnet, etc.);

6.3 Task 2: Deliverables

Deliverable due dates are reflected in actual dates where warranted. Otherwise due dates are specified in weeks or months after contract award (ACA).

Deliverable	Due Date, Format (NLT-No Later Than) (POP–Period of Performance)
Configuration Management Plan – GSS LAN	• NLT 180 calendar days prior to the end of the period of performance (POP)
Configuration Management Plan – CPSRMS	• NLT 180 calendar days prior to the end of the POP
Configuration Management Plan – ITDS-RAM	• NLT 180 calendar days prior to the end of the POP
Configuration Management Plan – CPSC.GOV	• NLT 180 calendar days prior to the end of the POP
Configuration Management Plan – DCM	• NLT 180 calendar days prior to the end of the POP
Baseline Configuration Document – GSS LAN	• NLT 180 calendar days prior to the end of the POP
Baseline Configuration Document – CPSRMS	• NLT 180 calendar days prior to the end of the POP
Baseline Configuration Document – ITDS-RAM	• NLT 180 calendar days prior to the end of the POP

Deliverable	Due Date, Format (NLT-No Later Than) (POP–Period of Performance)
Baseline Configuration Document – CPSC.GOV	• NLT 180 calendar days prior to the end of the POP
Baseline Configuration Document – DCM	• NLT 180 calendar days prior to the end of the POP

All deliverables are to be provided in MS Word and PDF format to the COR for review and comment. Comments shall be provided by the CPSC COR within 5 business days of each deliverable receipt from the contractor. Comments from CPSC shall be addressed by the contractor and revised deliverables provided within 5 business days of receiving comments from the CPSC COR.

7 Task 3: Risk Management Support

The contractor shall provide risk management support services to support the operation of the CPSC General Support System Local Area Network (GSS LAN) and the CPSC Major Applications (CPSRMS, DCM, CPSC.GOV, and ITDS-RAM). The work may involve interviewing agency staff, facilities security and management staff, application system support contractors, infrastructure support staff, application systems owners and users, business process managers, and IT security staff. This work will involve developing risk management (RM) documentation in accordance with NIST, OMB, Federal guidelines, and commercial best practices. The contractor shall review existing documents, such as security plans, application system input and output documents, C&A packages, user guides, operational procedures, security policies, risk assessments, security assessments, audits, and POAMs.

Risk Management (RM) comprises a collection of activities focused on the management of information system-related security risks, through the development and implementation of comprehensive governance processes and organization-wide risk management strategies.

7.1 Task 1: Develop Agency-Wide Risk Management Strategy

The contractor shall develop an agency-wide risk management strategy which includes processes for framing risk, assessing risk, responding to risk, and monitoring risk. The Contractor shall:

a) Develop and document an organizational risk framework that helps to inform and drive each component of the risk management process assessment, monitoring, and response.

    1) Develop and document processes that the agency uses to assess risk (i.e., risk assessment) within the context of the organizational risk framework. This step must define how the agency identifies: (i) threats to the agency; (ii) vulnerabilities internal and external to the agency; (iii) the harm (i.e., adverse impact) that may occur given

the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur.

2) Define and document the tools, techniques, and methodologies that the agency will use to develop risk assessments.
3) Define and document how risk and threat information is collected.
4) Develop processes that the agency uses to respond to risk once risk is determined based on the results of a risk assessment. This component should provide a consistent, organization-wide response to risk in accordance with the organizational risk framework by: (i) developing alternative courses of action for responding to risk; (ii) evaluating the alternative courses of action; (iii) determining appropriate courses of action consistent with organizational risk tolerance; and (iv) implementing risk responses based on selected courses of action.
5) Develop processes that the agency uses to monitor risk over time. This step must define how the agency: (i) determines the ongoing effectiveness of risk responses (consistent with the organizational risk frame); (ii) identify risk-impacting changes to organizational information systems and the environments in which the systems operate; and (iii) verify that planned risk responses are implemented and information security requirements derived from and traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, standards, and guidelines are satisfied.

b) Develop and document an organizational risk management strategy.
   1) Develop and document an organizational risk management strategy that establishes the organization risk foundation and defines risk boundaries.
   2) The risk management strategy must comply with federal legislation, directives, and policies.
   3) Document how information system common controls are selected by organization officials.
   4) Define and document the order of recovery for critical agency information systems.
   5) Define and document an agency risk executive function that supports risk management at all levels.
   6) Document risk management roles and responsibilities.
   7) Document risk management processes at the mission/business level (e.g., determining and defining what technologies are acceptable for information systems, etc.).
   8) Document risk management processes at the information system level (e.g., categorizing information systems, allocating security controls, managing the selection of allocated security controls, etc.).

7.2 Task 2: Develop An Information System Inventory/Boundary

The agency must appropriately define the information system boundary for the GSS LAN and each Major Application—to include CPSRMS, ITDS-RAM, DCM, and CPSC.GOV. The Contractor shall:

a) Develop and document an inventory of information system components that includes all components within the authorization boundary for each in-scope system.

7.3 Deliverables

Deliverable due dates are reflected in actual dates where warranted. Otherwise due dates are specified in weeks or months after contract award (ACA).

Deliverable	Due Date, Format (NLT-No Later Than) (POP – Period of Performance)
Risk Management Strategy	• NLT 90 calendar days prior to the end of the period of performance (POP)
Information System Inventory/Boundary – GSS LAN	• No Later than 90 calendar days prior to the end of the POP
Information System Inventory/Boundary – CPSRMS	• No Later than 90 calendar days prior to the end of the POP
Information System Inventory/Boundary – ITDS-RAM	• No Later than 90 calendar days prior to the end of the POP
Information System Inventory/Boundary – DCM	• No Later than 90 calendar days prior to the end of the POP
Information System Inventory/Boundary – CPSC.GOV	• No Later than 90 calendar days prior to the end of the POP

All deliverables are to be provided in MS Word and PDF format to the COR for review and comment. Comments shall be provided by the CPSC COR within 5 business days of each deliverable receipt from the contractor. Comments from CPSC shall be addressed by the contractor and revised deliverables provided within 5 business days of receiving comments from the CPSC COR.

8 Project Management Deliverables:

Deliverable	Due Date, Format (NLT-No Later Than)
Kick-Off Meeting to present High-Level Schedule and Draft Project Management Plan to be held at the CPSC HQ	• NLT 5 calendar days after contract award
Weekly Status Reports for each task	• Weekly, NLT end of day Monday, to begin two weeks after contract award
Monthly Status Reports for each task	• Monthly, NLT the 5th day of the month, to begin 30 calendar days after contract award
Final Project Management Plan for each task	• NLT 30 calendar days from contract award

All deliverables are to be provided in MS Word and PDF format to the COR for review and comment. Comments shall be provided by the CPSC COR within 5 business days of each deliverable receipt from the contractor. Comments from CPSC shall be addressed by the contractor and revised deliverables provided within 5 business days of receiving comments from the CPSC COR.

9 PERFORMANCE ASSESSMENT PLAN

Successful performance will be measured by:

Performance Objective	Performance Thresholds
Reporting Requirements: Accuracy of completed work in comparison to requested requirements	100% accuracy
Timely submission of deliverables	95% submitted on time
Defined and consistent document formats. All documents developed under this contract shall have a well-defined and consistent format. Documents shall have a logical, predetermined, and easy to follow format that makes it easy to determine document completeness.	99% consistency

Performance Objective	Performance Thresholds
Basic information requirements for each C&A document must be easily identified and maintained through the use of document templates.	
Clearly written. All documents developed under this contract shall be written in clear, easy to understand English. When technical or esoteric terms are used, these expressions shall be clearly defined in the document in a glossary of terms.	100% accuracy

10 PERIOD OF PERFORMANCE

September 29, 2016 – September 28, 2017

11 PLACE OF PERFORMANCE

Work shall be primarily performed at CPSC Headquarters in Bethesda, MD and at the CPSC Lab Facility, in Rockville, MD. Off-site work at Contractor's designated locations shall be coordinated through the CPSC COR for written approval prior to work being performed off-site.

12 GOVERNMENT-FURNISHED EQUIPMENT AND MATERIALS

CPSC shall furnish the following materials to The Contractor in connection with this contract:

a. All necessary reports, documentation, policies, Standard Operating Procedures, etc., required to perform the work

b. All items provided hereunder are for exclusive use in performance of this contract. Any such items not expended in performance of this contract shall be returned to CPSC upon completion of the contract.

c. All other materials/equipment required in performance by this contract shall be furnished by The Contractor.

d. Results from scanning tools operated by CPSC to include Asset Reporting, Vulnerability Reporting and Configuration Compliance Reporting

e. Updated and approved System Security Plans for ITDS-RAM, CPSC.Gov, and DCM

f. CPSC Subject Matter Experts for onsite security control testing demonstration.

Clauses In Addition To GSA Federal Supply Schedule Contract

LC1A CONTRACTOR'S NOTE

A. BILLING INSTRUCTIONS

Pursuant to the Prompt Payment Act (P.L. 97-177) and the Prompt Payment Act Amendments of 1988 (P.L. 100-496) all Federal agencies are required to pay their bills on time, pay interest penalties when payments are made late, and to take discounts only when payments are made within the discount period. To assure compliance with the Act, vouchers and/or invoices shall be submitted on any acceptable invoice form which meets the criteria listed below. Examples of government vouchers that may be used are the Public Vouchers for Purchase and Services Other Than Personal, SF 1034, and Continuation Sheet, SF 1035. At a minimum, each invoice shall include:

1. The name and address of the business concern (and separate remittance address, if applicable).

2. **Do NOT** include Taxpayer Identification Number (TIN) on invoices sent via e-mail.

3. Invoice date.

4. Invoice number.

5. The contract or purchase order number (see block 2 of OF347 and block 4 of SF1449 on page 1 of this order), or other authorization for delivery of goods of services.

6. Description, price and quantity of goods or services actually delivered or rendered.

7. Shipping cost terms (if applicable).

8. Payment terms.

9. Other substantiating documentation or information as specified in the contract or purchase order.

10. Name, title, phone number and mailing address of responsible official to be notified in the event of a deficient invoice.

ORIGINAL VOUCHERS/INVOICES SHALL BE SENT TO:

PREFERED: Via email to:

9-AMC-AMZ-CPSC-Accounts-Payable@faa.gov

OR

U.S. Mail
Enterprise Service Center, c/o CPSC, Accounts Payable Branch, AMZ-160
PO Box 25710
Oklahoma City, Ok. 73125

FEDEX
Enterprise Service Center, c/o CPSC, Accounts Payable Branch, AMZ-160
6500 S. MacArthur Blvd.
Oklahoma City, Ok. 73169

Invoices not submitted in accordance with the above stated minimum requirements will not be processed for payment. Deficient invoices will be returned to the vendor within seven days or sooner. Standard forms 1034 and 1035 will be furnished by CPSC upon request of the contractor.

Inquiries regarding payment should be directed to the Enterprise Service Center (ESC), Office of Financial Operations, Federal Aviation Administration (FAA) in Oklahoma City,9-AMC-AMZ-CPSC-Accounts-Payable@faa.gov.

B. PAYMENT

Payment will be made as close as possible to, but not later than, the 30th day after receipt of a proper invoice as defined in "Billing Instructions," except as follows:

When a time discount is taken, payment will be made as close as possible to, but not later than, the discount date. Discounts will be taken whenever economically justified. Otherwise, late payments will include interest penalty payments. Inquiries regarding payment should be directed to 9-AMC-AMZ-CPSC-Accounts-Payable@faa.gov or at the U.S. Mail and Fedex addresses listed above:

Complaints related to the late payment of an invoice should be directed to Ricky Woods at the same the same address (above) or 405-954-5351.

Customer Service inquiries may be directed to Adriane Clark at AClark@cpsc.gov.

C. INSPECTION & ACCEPTANCE PERIOD

Unless otherwise stated in the Statement of Work or Description, the Commission will ordinarily inspect all materials/services within seven (7) working days after the date of receipt. The CPSC representative responsible for inspecting the materials/services will transmit disapproval, if appropriate, to the contractor and the contract specialist listed below. If other inspection information is provided in the Statement of Work or Description, it is controlling.

D. ALL OTHER INFORMATION RELATING TO THE PURCHASE ORDER
Contact: Contract Specialist Greg Grayson at (301) 504-7725 or ggrayson@cpsc.gov

E. PROCESSING INSTRUCTIONS FOR REQUESTING OFFICES

The Purchase Order/Receiving Report (Optional Form 347 or Standard Form 1449) must be completed at the time the ordered goods or services are received. Upon receipt of the goods or services ordered, each item should be inspected, accepted (partial or final) or rejected. The Purchase Order/Receiving Report must be appropriately completed, signed and dated by the authorized receiving official. In addition, the acceptance block shall be completed (Blocks 32 a, b & c on the SF 1449 and column G and page 2 of the OF 347). The receiving report shall be retained by the requesting office for confirmation when certifying invoices.

F. PROPERTY/EQUIPMENT PURCHASES

In the case of Purchase Orders/Receiving Reports involving the purchase and receipt of property/equipment, a copy of the Purchase Order/Receiving Report must also be immediately forwarded directly to the Property Management Officer (Constantia Demas) in the Facilities Management Support Services Branch (Room 425). The transmittal of Purchase Orders/Receiving Reports to the property management officer is critical to the integrity and operation of CPSC's Property Management System. Receiving officials should also forward copies to their local property officer/property custodian consistent with local office procedures.

(End of clause)

LC 5 Contracting Officer's Representative (COR) Designation

a. The following individual has been designated at the Government's COR for this contract:
Name: Amy Shifflett
Division: IT - Division of Solution and Development
Telephone: 301-504-7172
Email: Ashifflett@cpsc.gov
b. **The CPSC COR is responsible for:**

(1) monitoring the Contractor's technical progress, including surveillance and assessment of performance, and notifying the Contracting Officer within one week when deliverables (including reports) are not received on schedule in accordance with the prescribed delivery schedule.

(2) performing technical evaluation as required, assisting the Contractor in the resolution of technical problems encountered during performance; and

(3) inspection and acceptance of all items required by the contract.

c. **The COR is not authorized to and shall not:**

(1) make changes in scope of work, contract schedules, and/or specifications to meet changes and requirements,

(2) direct or negotiate any change in the terms, conditions, or amounts cited in the contract; and

(3) take any action that commits the Government or could lead to a claim against the Government.

d. A clear distinction is made between Government and Contractor personnel. No employer-employee relationship will occur between government employees and contractor employees. Contractor employees must report directly to their company (employer) and shall not report to Government personnel.

(End of Clause)

LC 6 Contractor Use of CPSC Information Technology (IT) Resources

a. As identified under sections of the statement of work pertaining to Government furnished materials and equipment, the contractor is to be furnished certain CPSC IT resources. Access will be granted to Contractor employees from time to time during contract performance and will be limited to those Contractor employees specified in advance. In addition, the use of CPSC IT facilities, equipment or other resources by Contractor personnel shall be limited to performance of the work described in the contract.

b. Prior to utilizing any CPSC IT resources, the Contractor shall contact the Director of the Information Technology Division and provide an estimate (written if requested) of the amount of resources to be required and shall request that a time be scheduled for use of the resources. In the event of any scheduling conflict between CPSC contract work and in-house CPSC work, the CPSC in-house work shall take precedence unless otherwise specified by the Director of the Information Technology Division.

(End of Clause)

LC 9 Key Personnel

a. The following individuals, listed by name and title, have been identified as key personnel for performance under this contract:
[ ]

b. The personnel specified above and/or in the schedule of the contract are considered to be essential to the work being performed hereunder. If these individuals are unavailable

for assignment for work under the contract, or it is anticipated that their level of involvement will be significantly different from the negotiated level, the Contractor shall immediately notify the Contracting Officer and shall submit justifications (including proposed substitutions) in sufficient detail to permit evaluation of the impact on the program. The Contracting Officer shall review, and may ratify in writing, such substitutions. Prior to substitution of key personnel, the Contractor shall obtain the written consent of the Contracting Officer.

(End of Clause)

LC 13 Insurance

a. In accordance with the Federal Acquisition Regulation (FAR), Subparts 28.301 and 28.307-2, and Clause 52.228-5 of this contract entitled "Insurance-Work on a Government Installation," the Contractor shall at its own expense provide and maintain during the entire performance period of this contract at least the kinds and minimum amounts of insurance set forth below:

(1) Workers' compensation and employer's liability. Contractors are required to comply with applicable Federal and State workers' compensation and occupational disease statutes. If occupational diseases are not compensable under those statutes, they shall be covered under the employer's liability section of the insurance policy, except when contract operations are so commingled with a Contractor's commercial operations that it would not be practical to require this coverage. Employer's liability coverage of at least $100,000 shall be required, except in States with exclusive or monopolistic funds that do not permit workers' compensation to be written by private carriers.

(2) General liability. The Contractor shall have bodily injury liability insurance coverage written on the comprehensive form of policy of at least $500,000 per occurrence.

(3) Insurance Clause. The Contractor shall present evidence of insurance coverage in Compliance with (1) and (2) above within fifteen calendar days of award.

(End of Clause)

LC 21A Disclosure of Information - Limits on Publication

a. The Contractor shall submit to the Commission any report, manuscript or other document containing the results of work performed under this contract, before such document is published or otherwise disclosed to the public, to assure compliance with Section 6(b) of the Consumer Product Safety Act (15 U.S.C. Section 2055(b)), Commission regulations (16 C.F.R. Part 1101), and a Commission directive (Order 1450.2). These provisions restrict disclosure by Commission Contractors of information that (1) permits the public to identify particular consumer products or (2) reflects on the safety of a class of consumer products. Prior submission allows the Commission staff to

review the Contractor's information and comply with the applicable restrictions. CPSC should be advised of the Contractor's desire to submit or publish an abstract or a report as soon as practical.

b. Any publication of, or publicity pertaining to, the Contractor's document shall include the following statement: "This project has been funded with federal funds from the United States Consumer Product Safety Commission under contract number CPSC-F-16-0026. The content of this publication does not necessarily reflect the views of the Commission, nor does mention of trade names, commercial products, or organizations imply endorsement by the Commission

(End of Clause)

LC 24 Nondisclosure of any Data Developed Under this Contract

a. The Contractor agrees that it and its employees will not disclose any data obtained or developed under this contract to third parties without the consent of the U. S. Consumer Product Safety Commission Contracting Officer.

b. The Contractor shall obtain an agreement of non-disclosure (attached) from each employee who will work on this contract or have access to data obtained or developed under this contract.

(End of Clause)

LC 29 In and Out-Processing Requirements

Contractor personnel performing on site must comply with all in- and out-processing requirements at the agency and shall sign a "Confidentiality/Record Agreement" prior to their departure.

(End of Clause)

LC 30 Security and Personal Identity Verification Procedures

a. The performance of this contract requires contractor employees to have access to CPSC facilities and/or systems. In accordance with Homeland Security Presidential Directive-12 (HSPD-12), all such employees must comply with agency personal identity verification (PIV) procedures. Contractor employees who do not already possess a current PIV Card acceptable to the agency shall be required to provide personal background information, undergo a background investigation (NACI or other OPM-required or approved investigation), including an FBI National Criminal History Fingerprint Check prior to being permitted access to any such facility or system. CPSC may accept PIV issued by another Federal Government agency but shall not be required to do so. No contractor employee will be permitted access to a CPSC facility or system without approval under the PIV process.

b. Contractor employees must meet the following citizenship requirements:

1. A United States (U.S.) citizen; or,

2. A national of the United States (see 8. U.S.C. 1408); or,

3. An alien lawfully admitted into the United States for permanent residence as evidenced by an alien Registration Receipt Card form I-151

c. Within five (5) days after contract award, the contractor shall provide a list of contractor personnel, including full name, social security number, and place (city and state) and date of birth to the designated Contracting Officer Representative(COR). This information will be used to determine whether personnel have had a recent Federal background investigation and whether or not further investigation is required.

d. For each contractor employee subject to the requirements of this clause and not in possession of a current PIV Card acceptable to CPSC, the contractor shall submit the following properly-completed forms: Electronic Standard Form (SF) 85 or 85-P, "Questionnaire for Non-sensitive Positions", SF (87) Fingerprint Chart, Optional Form (OF) 306 and a current resume. The SF-85 is available from the Office of Personnel Management's (OPM) secure website. The CPSC Office of Human Resources will provide the COR with the other forms that are not obtainable via the internet.

e. The contractor shall complete the electronic security form and deliver the other completed forms indicated in paragraph d above to the COR within five (5) days of written notification from the COR of those contractor employees requiring background investigations.

f. Upon completion of the investigation, the COR will notify the contractor in writing of all investigation determinations. If any contractor employees are determined to be unsuitable to be given access to CPSC, the contractor shall immediately provide identical information regarding replacement employees. The contractor is responsible for providing suitable candidates and fulfilling staffing requirements under the contract so that there is no break in service. This approval process applies to contract start up and any required replacement personnel. Failure to prequalify potential replacement personnel will not serve as an excuse for failure to provide performance. Non performance due to failure to provide suitable contractor employees may result in a Termination for Cause or Default.

g. CPSC will issue a PIV Card to each on site contractor employee who is to be given access to CPSC facilities and systems. The employee will not be given access prior to issuance of a PIV card. CPSC may revoke a PIV Card at any time if an investigation or subsequent investigation reveals that the personnel are unsuitable.

h. PIV Cards shall identify individuals as contractor employees. Contractor employees shall display their PIV Cards on their persons at all times while working in a CPSC

facility, and shall present cards for inspection upon request by CPSC officials or security personnel. The contractor shall be responsible for all PIV Cards issued to the contractor's employees and shall immediately notify the COR if any PIV card(s) cannot be accounted for.

i. CPSC shall have and exercise full and complete control over granting, denying, withholding, and terminating access of contractor employees to CPSC facilities and systems. The COR will notify the contractor immediately when CPSC has determined that an employee is unsuitable or unfit to be permitted access. The contractor shall immediately notify such employee that he/she no longer has access, shall remove the employee and shall provide a suitable replacement in accordance with contract requirements and the requirements of this clause.

j. By execution of this contract, the contractor certifies that none of the employees working under this contract have been convicted of a felony, a crime of violence, or a misdemeanor involving moral turpitude, such as a conviction of larceny within the last five (5) years. During contract performance the contractor shall immediately notify CPSC if one of its employees working under this contract has been convicted of a felony, a crime of violence, or a misdemeanor involving moral turpitude, such as a conviction of larceny within the last five years.

k. The Government reserves the right to have removed from service any Contractor employee for any of the following:

1. Conviction of a felony, a crime of violence, or a misdemeanor involving moral turpitude, such as a conviction of larceny within the last five (5) years.

2. Falsification of information entered on security screening forms or other documents submitted to the Government.

3. Improper conduct during performance of the contract, including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct prejudicial to the Government regardless of whether the conduct is directly related to the contract.

4. Any behavior judged to be a threat to personnel or property.

l. The COR shall be responsible for proper separation of contractor employees at the Consumer Product Safety Commission. The COR shall ensure that each contractor employee completes CPSC's official out processing procedures. The contractor employee shall report to the CPSC Facilities Security Specialist to obtain a Contractor Employee Accountability and Clearance Record. This record shall be completed as part of the official out-processing procedures and returned along with the PIV card, key fobs, keys and any other previously issued material.

m. Contractor employees shall comply with applicable Federal and CPSC statutes, regulations, policies and procedures governing the security of the facilities and system(s) to which the contractor's employees have access.

n. Failure on the part of the contractor to comply with the terms of this clause may result in termination of this contract for cause or default.

o. The contractor shall incorporate this clause in all subcontracts.

(End of Clause)

LC 31 Restrictions on Use of Information

a. If the Contractor, in the performance of this contract, obtains access to information such as CPSC plans, reports, studies, data projected by the Privacy Act of 1974 (5 U.S.C. 552a), or personal identifying information which has not been released or otherwise made public, the Contractor agrees that without prior written approval of the Contracting Officer it shall not: (a) release or disclose such information, (b) discuss or use such information for any private purpose, (c) share this information with any other party, or (d) submit an unsolicited proposal based on such information. These restrictions will remain in place unless such information is made available to the public by the Government.

b. In addition, the Contractor agrees that to the extent it collects data on behalf of CPSC, or is given access to, proprietary data, data protected by the Privacy Act of 1974, or other confidential or privileged technical, business, financial, or personal identifying information during performance of this contract, that it shall not disclose such data. The Contractor shall keep the information secure, protect such data to prevent loss or dissemination, and treat such information in accordance with any restrictions imposed on such information.

(End of Clause)

LC 32 Standards of Conduct

1. Government contractors must conduct themselves with the highest degree of integrity and honesty. Contractors shall have standards of conduct and internal control systems that:
a. Are suitable to the size of the company and the extent of their involvement in Government contracting,
b. Promote such standards,
c. Facilitate timely discovery and disclosure of improper conduct in connection with Government contracts, and
d. Ensure corrective measures are promptly instituted and carried out.

2. By submitting a proposal in response to this solicitation and under award of any resultant contract, the Contractor agrees to employ standards of conduct and internal control systems, which shall include, but are not necessarily limited to the following.

The contractor shall provide, for all employees:
a. A written code of business ethics and conduct and an ethics training program
b. Periodic reviews of company business practices, procedures, policies, and internal controls for compliance with standards of conduct and the special requirements of Government contracting;
c. A mechanism, such as a hotline, by which employees may report suspected instances of improper conduct, and instructions that encourage employees to make such reports;
d. Internal and/or external audits, as appropriate;
e. Disciplinary action for improper conduct;
f. Timely reporting to appropriate Government officials of any suspected or possible violation of law in connection with Government contracts or any other irregularities in connection with such contracts; and
g. Full cooperation with any Government agencies responsible for either investigation or corrective actions.
h. A copy of the written code of ethics and information regarding the above shall be made available to the Government upon request.

(End of Clause)

LC 33 Contractor Personnel

A clear distinction is made between Government and Contractor personnel. No employer-employee relationship will occur between government employees and contractor employees. Contractor employees must report directly to their company (employer) and shall not report to Government personnel.

(End of Clause)

52.217-8 Option to Extend Services.

Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 15 days prior to completion of the last stated option period.

(End of clause)