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

1. REQUISITION NUMBER	PAGE	OF
REQ-2400-17-0049	1	29

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
GS35F274DA	05/16/2017	CPSC-F-17-0042	CPSC-Q-17-0027	03/23/2017

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	Cassandra Sterba	301-504-7837	

9. ISSUED BY CODE FMPS

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

10. THIS ACQUISITION IS ☒ UNRESTRICTED OR ☐ SET ASIDE: % 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: 541618
SIZE STANDARD: $6.0

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	Net 30	☐	☐RFQ ☐IFB ☐RFP

15. DELIVER TO CODE EXIT

CONSUMER PRODUCT SAFETY COMMISSION
OFFICE OF INFORMATION SERVICES
4330 EAST WEST HWY
ROOM 839-23
BETHESDA MD 20814

16. ADMINISTERED BY CODE FMPS

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

17a. CONTRACTOR/ OFFEROR CODE [redacted] FACILITY CODE

RICHARD S CARSON ASSOCIATES INC
4720 MONTGOMERY LN STE 800
BETHESDA MD 20814-5320

TELEPHONE NO.

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

18a. PAYMENT WILL BE MADE BY CODE FMFS

CPSC Accounts Payable Branch
AMZ 160
P. O. Box 25710
Oklahoma City OK 73125

☐ 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] COR: Mary Meier Phone: (301) 504-7040 Email: MMeier@cpsc.gov The contractor shall provide FISMA evaluation services in accordance with their GSA Schedule GS-35F-274DA, the attached SOW, and the attached terms and conditions. Continued ... *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA
0100A17DSE-2017-5457500000-EXIT002400-251A0

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*
$116,295.65

☐ 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)*
	[signature]

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	5/16/17

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
0001	BASE PERIOD - May 16, 2017 through May 15, 2018 Independent evaluation of the CPSC's compliance with FISMA for Fiscal Year (FY) 2017.				116,295.65
0002	OPTION PERIOD 1 - May 16, 2018 through May 15, 2019 Independent evaluation of the CPSC's compliance with FISMA for Fiscal Year (FY) 2018. Amount: $118,823.82(Option Line Item)				0.00
0003	OPTION PERIOD 2 - May 16, 2019 through May 15, 2020 Independent evaluation of the CPSC's compliance with FISMA for Fiscal Year (FY) 2019. Amount: $102,029.11(Option Line Item)				0.00
0004	OPTION PERIOD 3 - May 16, 2020 through May 15, 2021 Independent evaluation of the CPSC's compliance with FISMA for Fiscal Year (FY) 2020. Amount: $104,154.71(Option Line Item)				0.00
0005	OPTION PERIOD 4 - May 16, 2021 through May 15, Continued ...				0.00

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

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	2022 Independent evaluation of the CPSC's compliance with FISMA for Fiscal Year (FY) 2021. Amount: $106,280.32(Option Line Item) The total amount of award: $547,583.61. The obligation for this award is shown in box 26.				

Statement of Work,
Annual Federal Information Security Management Act of 2002 (FISMA)
Independent Evaluation Services for the Office of the Inspector General (OIG)
Consumer Product Safety Commission (CPSC)

1.0 Objective

The objective of this requirement is to obtain independent evaluations of the CPSC's compliance with FISMA for Fiscal Year (FY) 2017. If options are exercised by the government this Statement of Work (SOW) will include four successive annual FISMA independent evaluations in FY 2018 through FY 2021.

2.0 Scope of Work

The Contractor shall provide all staff resources necessary to accomplish the tasks and deliverables described in this SOW to complete annual independent evaluations of FISMA compliance.

3.0 Background

3.1 Agency

The CPSC is an independent federal regulatory agency created by Congress in 1972 charged with protecting the public against unreasonable risks of injury associated with consumer products. The CPSC's work to help ensure the safety of consumer products such as toys, cribs, power tools, and household chemicals contributed significantly to the decline in the rate of deaths and injuries associated with consumer products over the past 40 years.

3.2 FISMA

The basis for this independent evaluation is the law amended on December 18, 2014, named "Federal Information Security Modernization Act of 2014" (Public Law 113–283). The purpose of the amendments were to, among other objectives; reestablish the oversight authority of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and to establish the authority of the Secretary of the Department of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

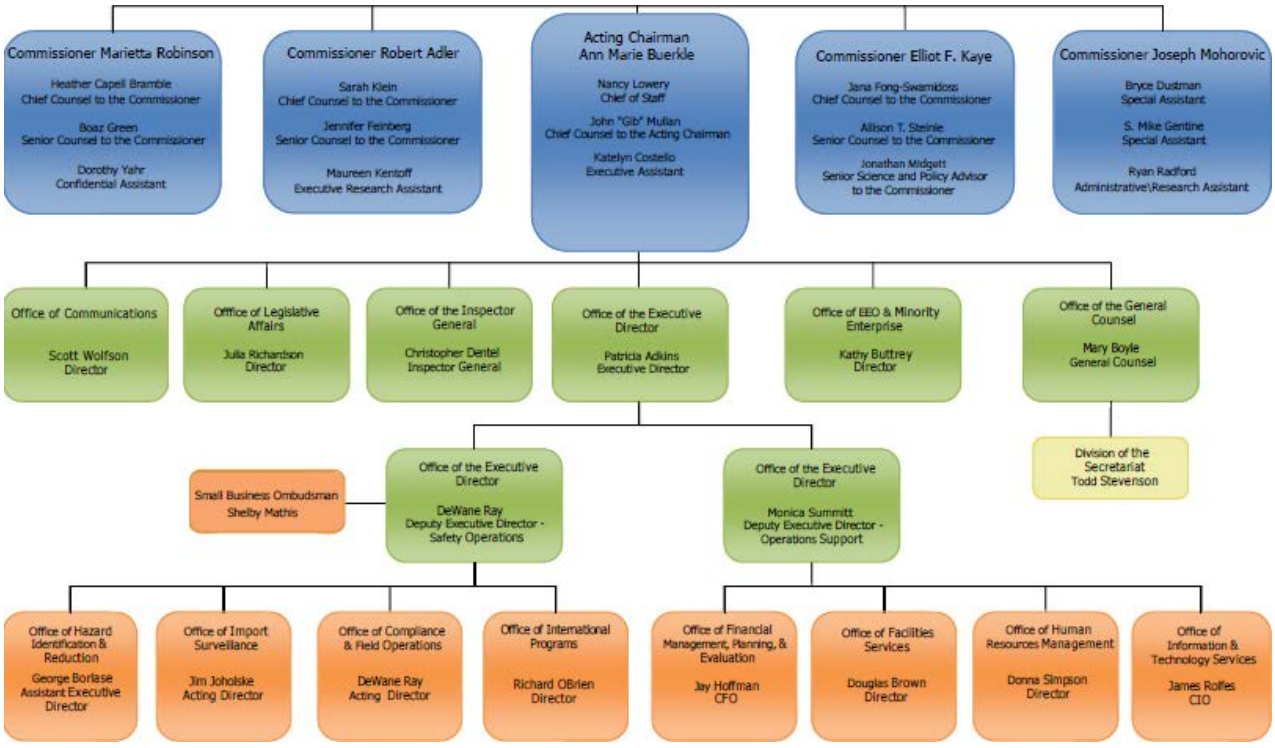
This act compels agency management to perform independent evaluations of information security programs on an annual basis, in an effort to keep risks at or below defined acceptable levels in a cost-effective, timely and efficient manner. Further, the act requires Inspectors General (IGs) to perform an annual independent evaluation of the agency's FISMA implementation.

3.3 Agency Implementation

Since the introduction of FISMA in 2002, the CPSC has been unable to comply with some of the stipulations set forth by the legislation. As a result of the FY 2016 FISMA evaluation, the OIG identified 35 weaknesses across the 8 Department of Homeland Security (DHS) security domains defined in FY 2016. Historically, the CPSC's compliance issues were primarily due to management expending too few resources to comply with the provisions of FISMA. However, over the past two year's management has established a security team led by a Chief Information Security Officer and invested in several new security solutions to address some of the most pressing security weaknesses. The CPSC also hired a new Chief Information Officer (CIO) in 2016 with a security background, and the tone within the CPSC Office of Information Technology (EXIT) toward security is improving.

EXIT is responsible for much of the CPSC's FISMA administration and implementation. FISMA has a high level of visibility within the agency as the CPSC CIO (and Assistant Executive Director of EXIT), reports to the Deputy Executive Director, who then reports to the Executive Director who in turn reports to the CPSC Chairman.

CPSC Organizational Chart



3.4 OIG Authority

The first IG for the CPSC took office on April 9, 1989 as a result of the Inspector General Act Amendments of 1988. The IG's authority flows from the Inspector General Act of 1978 (as amended). This law authorizes the IG to have access to all records, reports, audits, reviews,

documents, papers, recommendations, or other material available to the applicable agency which relate to programs and operations with respect to which the IG has responsibilities under the IG Act.

3.5 Contract Type

This is a fixed-price contract for non-personal services for one base year and four option periods of one year each.

3.6 Contractor Qualifications and Requirements

1) The company performing this service shall have a minimum of five years of experience performing the same or similar services.
2) Key personnel performing the work shall have a minimum of five years of experience performing similar work. All personnel must meet Personal Identification (PIV) requirements, ref Contract Clause LC 30.
3) The contractor shall appoint a lead project manager with overall responsibility for performance. The lead project manager, or key contract personnel, shall be the single point of interface with the government for all matters concerning technical progress and problems, project performance, schedule, resources, and other project-related matters. The contractor shall maintain an organizational chart identifying key and non-key personnel and their assigned duties and responsibilities.
4) The Contractor's lead project manager shall have a demonstrable understanding of current security best practices, NIST, OMB, DHS guidance, and an information security certification from an accredited professional organization (ex. CISA, CISSP, or equivalent).
5) Any proposed changes to personnel after submission of the contractor quote must be equally or more qualified than the personnel they are replacing.
6) Individuals working on these projects must have completed a minimum of 40 hours in the most recent biannual period and are encouraged to have completed at least 80 hours within this timeframe. The Contractor should also describe how the key personnel selected will offer the best possible approach to meeting the requirements of this contract.

3.7 Experience Requirements

In addition to demonstrating general knowledge of internal information security, internal controls and auditing the offeror will be evaluated on relevant and demonstrable experience/ability in the following areas:

1) Performing independent evaluations of federal agency compliance with FISMA on behalf of the Offices of the Inspectors General of Federal agencies of comparable size and resources. Specifically the offeror must demonstrate:
    a. at minimum five years of experience performing independent evaluations of FISMA on behalf of the Offices of the Inspectors General of Federal agencies by the lead auditor.

b. at minimum two years of experience performing independent evaluations of FISMA on behalf of the Offices of the Inspectors General of Federal agencies by any supporting auditor/technical expert.
c. familiarity with the criteria described in Exhibit 1 of the Statement of Work.
d. experience in auditing Windows environments within the past two years
e. experience in auditing Linux (SuSE) environments within the past two years.
f. experience in auditing Virtual Desktop Infrastructure (VDI) environments within the past two years.

2) Developing effective, clear, and concise reports that include an accurate, understandable, and complete view of all of the issues identified and recommendations made.

3) Compliance with National Institute of Standards and Technology Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

3.8 Place of Performance

All documentation related to this effort is located at the CPSC HQ building in Bethesda, MD. Much of said documentation is available from various CPSC personnel. It is anticipated that the place of performance of this contract will be primarily at the contractor's place of business with interviews and walkthroughs taking place at the CPSC HQ building in Bethesda, MD.

4.0 Criteria

These independent evaluations will be performed in accordance with the current versions of criteria listed in Exhibit 1. It is the Contractor's responsibility to remain up-to-date on changing criteria.

Should there be any deviations from the methodology set forth in the Council of Inspectors General on Integrity and Efficiency (CIGIE), *Quality Standards for Inspection and Evaluation*, or the requirements set forth by DHS and OMB, the Contractor shall provide documentation (preferably via email) to the Contracting Officer's Representative (COR) immediately, demonstrating how the Contractor's methodology satisfies the established for criteria.

5.0 Deliverables

5.1 Schedule of Deliverables

In fulfilment of this effort, the Contractor shall provide the deliverables as described in Exhibit 2. All deliverables shall be submitted to the COR and one other OIG staff member, unless otherwise agreed upon.

These schedules will be developed collaboratively between OIG, Contractor, and Agency within two weeks of the entrance conference at the start of each year. As OMB and DHS reporting dates are released during the independent evaluation, the three parties, OIG, Contractor, and Agency, will

work together to update these schedules with the understanding that all parties will work to meet statutory deadlines. The schedule of deliverables for this independent evaluation can be found in Exhibit 2.

All written documents are due either at the time specified or by 4 pm of the date named. All documents will be reviewed by OIG within two business days. The Contractor will have two business days to respond to the Government's comments. Lack of response by this deadline will be construed as acceptance of the Government's edits. Additional iterations will have a 24-hour turnaround requirement until the due date at which time the editing/review window will be 2 hours for each party.

Exit/Entrance Conference and Meeting agenda are due for review by 8 AM the second government working day before meeting, e.g., Monday morning for a Wednesday meeting, Friday morning for a Tuesday meeting. The editing/review timeframe for all parties is two hours for each iteration. Lack of timely response by either party will be construed as acceptance.

All deliverables will be provided in the following formats: MS Office, or Adobe (please note, other formats may be deemed acceptable on a case by case basis by the COR) and disseminated via a secure method [Federal Information Processing Standards (FIPS) 140-2 compliant] of file transfer to the COR and at least one other OIG staff member as at the designated by the COR time of the entrance conferences.

5.2 Specific Tasks

The Contractor is responsible for completing the work described in this contract according to the schedule proscribed by OMB/DHS in Exhibit 2. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this SOW. When hiring personnel, the Contractor shall keep in mind that stability and continuity of the workforce are essential. Please note all deliverables shall conform to applicable OMB/DHS and CIGIE guidance. The contractor shall be responsible for providing all personnel and resources (except as identified in 11.4 Government-furnished Property) to complete the following task areas:

5.2.1 Initial Meeting

The Contractor shall host an initial meeting with the COR which shall discuss the logistics of the scheduled tasks. The contractor key personnel shall meet with the COR for a kick off meeting within fifteen (15) calendar days after contract award. The contractor key personnel agrees to attend the meeting on site or via conference call and shall be available to discuss and finalize the Project Management Plan, deliverables, progress, exchange information and resolve emergent technical problems and issues. If this meeting takes place on-site, the location shall be the Consumer Product Safety Commission facility located at:

4340 East West Highway

Bethesda, MD 20814

5.2.2 Independence Statement/Quality Control Assurance Statement
Within 5 days after the Initial Meeting, the Contractor shall provide an Independence Statement and Quality Control Assurance Statement to the COR. The Independence Statement must disclose any and all disclosures which could impact the impartiality of the Auditors assigned to this requirement. Additionally, the Contractor shall provide CPSC a Quality Control Assurance statement which demonstrates the Contractor's capability to meet or exceed the Council of Inspectors General on Integrity and Efficiency (CIGIE), Quality Standards for Inspection and Evaluation as well as the performance standards outlined in SOW sections 8.0 and 9.0.

5.2.3 Staffing List and Competency Evidence
Within 5 days after the Initial Meeting, the Contractor shall provide the COR with a detailed staffing list and sufficient information for compliance with agency personal identity verification (PIV) procedures. The Contractor must provide evidence that all assigned staff meet the requirements of this SOW. In addition, prior to reassigning any of the specified individuals to other efforts, the offeror shall notify the Contracting Officer and the Contracting Officer's Representative reasonably in advance and shall submit justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on the independent evaluation. No diversion shall be made by the offeror without the written consent of the Contracting Officer; provided, that the Contracting Officer may ratify in writing such diversion, and such ratification shall constitute the consent of the Contracting Officer required by this clause. The contract may be amended from time to time during the course of the contract to either add or delete personnel, as appropriate.

5.2.4 Entrance and Exit Conference
The Contractor shall conduct an entrance conference and an exit conference with key CPSC and OIG officials. The entrance conference shall occur prior to the commencement of the evaluation and the exit conference shall occur upon completion of the evaluation. The Contractor shall coordinate and schedule these meetings in advance and shall provide the COR with the draft agenda and meeting materials at least two business days prior to the meeting. The final agenda and meeting materials shall be distributed at least 24 hours prior to the meeting.

5.2.5 Planning/Field Work
The Contractor shall conduct all planning and field work necessary to develop an independent evaluation of the CPSC's compliance with FISMA. The planning documents shall conform to applicable OMB/DHS and CIGIE guidance and include the following elements:

a. Objective
b. Scope
c. Methodology
d. Research
e. Identification of criteria & evidence

f. Work Plan

Once the COR has approved the plan, the contractor shall conduct all necessary field work to collect and analyze the data.

5.2.6 Monthly Progress Meetings

The Contractor shall participate in a monthly status meeting to discuss the status of the independent evaluation. One status meeting shall include CPSC Agency staff, and one will be just OIG and Contractor staff who will discuss the status of the independent evaluation. All status and other meetings described below will be attended by key contractor personnel either in person or via teleconferencing technology. Each routine meeting will be scheduled for one-half hour. If any party has additional items to cover, the meeting duration may be extended based on prior discussions between COR and Contractor.

Status meetings among the Contractor, Agency staff, and OIG representatives, including the COR, will be held, at a minimum, on a monthly basis for each month between the entrance and exit conference for each year of the contract, or as mutually agreed to by the aforementioned individuals.

The agenda for all monthly status meetings shall include the following topics:

- ✓ The time, date, and location of the meeting.
- ✓ Overall status of the independent evaluation.
- ✓ Work completed.
- ✓ Work in progress (including a mention of timeliness of deliverables from Agency if appropriate).
- ✓ Potential issues/results of work uncovered since the last meeting.
- ✓ Opportunity for questions, general discussion.
- ✓ The time, date, and location of the next status meeting.

Potential issues such as access to records and documents, scheduled field office visits, and any other areas where the Contractor, Agency, and OIG representatives may need clarification or assistance shall be discussed with the COR prior to the monthly status meeting.

5.2.7 Draft Report and Responses to the annual FISMA checklist in Cyberscope/Draft FISMA Report

The Contractor shall be responsible for completing the annual DHS FISMA checklist for OIGs available on Cyberscope. The Contractor shall complete the annual DHS FISMA checklist in accordance with the guidance provided by OMB/DHS for the current year. The Contractor shall provide these responses to the COR upon completion of the fieldwork and in conjunction with the Draft FISMA Evaluation Report. The OIG will be responsible for entering the responses into the Cyberscope portal.

5.2.8 Final FISMA Report

The contractor shall include management comments in the Final FISMA Evaluation Report and provide this report to the COR prior to the annual FISMA submission deadline. The final FISMA Evaluation Report shall be presented at the Exit Conference and issued in accordance with CIGIE, Quality Standards for Inspection and Evaluation.

6.0 Performance Requirements

1) All services shall comply with applicable laws and regulations listed in Exhibit 1.
2) All delivery dates shall be met. Deliverables shall be on time and complete.
3) All written reports, procedures and/or programs are clear, concise and easily interpreted by the applicable users.

7.0 Delivery, Inspection, and Acceptance

The Government will review all deliverables to ensure accuracy, functionality, completeness, professional quality, and overall compliance with government policies, regulations, laws and directives. Written documents shall be concise and clearly written. The government will have two (2) business days to accept or reject deliverables. If a deliverable is rejected and returned to the Contractor for revision, the Contractor shall provide the corrected deliverable within two (2) business days of notification of the request for revision. All deliverables shall be submitted to the COR via a secure method (FIPS 140-2 compliant) of file transfer.

The Contractor shall allow for a minimum of two revisions of the written deliverables.

All materials provided hereunder are for the exclusive use in performance of this contract. The Contractor shall not release any materials for public dissemination without prior written approval from the CPSC COR.

During the performance of this contract, all technical questions and concerns shall be coordinated with the designated COR.

When changes are required as a result of the COR review of deliverables submitted, the COR will submit approvals and change requests via a secure method (FIPS 140-2 compliant) of file transfer to the Contractor's representative.

The OIG will accept/reject deliverables based on conformance with the Statement of Work

7.1 General Deliverable Acceptance Criteria

The general quality measures as set forth below will be applied to each work product received from the Contractor under this contract/order.

Timely submission of deliverables is essential to successfully completing this requirement. Schedules for deliverables are specified herein. All deliverables shall be prepared and submitted according to format, content, and schedule described in the SOW. All "hard copy" deliverables will be submitted on at least 30 percent recycled-content paper, and printed double-sided in compliance with environmental regulations.

- ✓ Accuracy – Work products shall be accurate in presentation, technical content, and adherence to accepted elements of style. The Contractor will follow the OIG Style Manual which will be provided upon contract award.

- ✓ Clarity – Work products shall be clear and concise. All exhibits or diagrams shall be easy to understand and relevant to the supporting narrative.

- ✓ Specifications Validity – All work products must satisfy the requirements of the Government as specified herein.

- ✓ File Editing – All text and files shall be editable by the Government

- ✓ Format – Work products shall be submitted electronically.

- ✓ Timeliness – Work products shall be submitted on or before the due date specified in the contract/order, or submitted in accordance with a later, scheduled date determined by the COR, as applicable.

8.0 Period of Performance

The performance period will be from date of award through one year, with four option periods of one year each.

The contractor must complete all prior deliverables and the final report no later than 10 business days before the Cyberscope reporting deadline as defined by OMB guidance for the year under evaluation. Specific interim deadlines will be negotiated between OIG, Contractor, and Agency.

10.0 Access to Documentation/Data Security Requirements

It is imperative that the Contractor shall protect all documentation from unauthorized access and applies the appropriate physical safeguarding measures at all times. As part of these requirements, the contractor must be in full compliance with FISMA, including compliance with NIST SP 800-171. Only Contractor staff with a justified need to know shall have access to documentation.

The OIG shall have ongoing access to the Contractor personnel and documentation during regular business hours as described in the contract. The evaluation documentation shall not be disclosed

outside of the CPSC OIG unless directed by statutory or other regulatory requirements. Any disclosure shall require the approval of the COR. In addition, the Contractor will work collaboratively with Agency to comply with data security requirements. The requirements can include method of transfer of sensitive and personally identifiable information (PII), between Agency and Contractor information systems, security requirements for Contractor hard- and software limits of Contractor access to Agency systems. COR will be included in all discussions related to access to and security of Agency information.

11.0 General Information

11.1 Communications with Agency

Opinions are not to be discussed with any Agency personnel without prior approval and in the presence of the COR. This includes discussing proposed finding recommendations and general information regarding finding elements.

11.2 Contractor Travel

The Contractor shall be required to attend the following meetings:

- Initial Meeting, as required, at 4340 East West Highway Bethesda, MD at a date and time to be determined after contract award.
- Monthly meetings at Agency headquarters located in Bethesda MD during the performance of the work for each year.

The Contractor's firm fixed price quote shall be inclusive of travel costs necessary to perform the work required under this SOW.

11.3 Government-furnished property:

1) With the exception of the personnel to be interviewed and the documentation to be reviewed (primarily electronically available), the Contractor will provide all services, personnel, facilities, equipment, and materials necessary to perform the work described in this contract.
2) Records, files, and documents provided by CPSC or generated in support of this contract shall be maintained by the contractor in accordance with CIGIE Standards. After work is completed, the contractor shall store all independent evaluation documentation (work papers etc.) in accordance with CIGIE standards. One copy of these records is to be made available to the OIG, upon request, at no cost to the Government.

11.4 Contractor and Contractor Personnel Requirements

For the purposes of this SOW and the ensuing contract, the term Contractor and Contractor personnel shall include any Subcontractors and Subcontractor personnel.

The Government reserves the right to judge the qualifications and acceptability of any individual proposed by the Contractor for any position, and may require the Contractor to replace an individual whose qualifications and suitability are judged deficient with written notification.

For each option year that is exercised, the Contractor shall provide evidence that key personnel meet the requirements of the SOW.

Contractor personnel shall present a neat appearance and be easily recognized as Contractor employees. All Contractor personnel shall wear a government-issued badge while on-site at any Agency location. Contractor personnel attending meetings, answering phones, and working in other situations where their status is not obvious are required to identify themselves as such to avoid creating the impression that they are Government officials.

All proposed personnel must currently hold the same or higher position in the firm with regard to the position for which they are being proposed under this SOW.

The Contractor shall not employ any person who is an employee of the U.S. Government if employing that person would create a conflict of interest. Additionally, the Contractor shall not employ any person who is an employee of the CPSC, unless such person seeks and receives approval according to CPSC regulations.

11.5 Government Closure and Recognized Holidays

In the event of Government or facility closures for holidays or any other reason, the Contractor may perform work at an approved alternate location provided funding is available to support the work effort. The Contractor may work on the recognized Federal holidays:

New Year's Day	Labor Day
Martin Luther King Jr's Birthday	Columbus Day
President's Dday	Veteran's Day
Memorial Day	Thanksgiving
Independence Day	Christmas Day

11.6 Agency Security Requirements

Contractor personnel will abide by the facility access and information technology security requirements of the Agency for the life of the contract. The minimum clearance for staff is the suitability check or Tier 1 with a credit check (formerly known as a National Agency Check with Inquiries (NACI)).

11.7 Timeliness of Communication Response

The Contractor, will strive for an email response standard of 1 business day and a telephone call

response within two (2) hours.

11.8 Training

All Contractor employees under this task order who require building access or access to any agency information technology system shall complete all agency-required information security awareness course(s), information privacy awareness(s), and any other agency-required courses as designated by the COR prior to commencement of work, and then annually thereafter.

Contractors must complete all training requirements by the assigned due dates. Failure to complete training by the assigned due dates may result in dismissal from the contract. Contractors must provide copies of the certifications of completion to the COR during each year of the task order, and must maintain copies of the completion certificates for the life of this task order. This requirement is in addition to any other training that may be required of the Contractor(s) to maintain professional certification(s).

11.9 Disclosure of Information

Information made available to the contractor by the Government for the performance or administration of this effort shall be used only for those purposes and shall not be used in any other way without the written agreement of the CO.

The contractor agrees to assume responsibility for protecting the confidentiality of Government records, which are not public information. Each contractor or employee of the contractor to whom information may be made available or disclosed shall be notified in writing by the contractor that such information may be disclosed only for a purpose and to the extent authorized herein.

Contractor team members will not disclose, share, or otherwise make public the results of the assessments beyond the requirements of the written results for inclusion as a deliverable report. Contractor team members will not discuss their activities or findings with family members, co-workers, colleagues, or other contractor or Government personnel outside of a controlled venue requiring the presence of the COR.

11.10 Limited Use of Data

Performance of this effort may require the contractor to access and use data and information proprietary to a Government agency or Government contractor which is of such a nature that its dissemination or use, other than in performance of this effort, would be adverse to the interests of the Government and/or others.

Contractor and/or contractor personnel shall not divulge or release data or information developed or obtained in performance of this effort, until made public by the Government, except to authorize Government personnel or upon written approval of the CO. The contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as required in the

performance of this effort. Nothing herein shall preclude the use of any data independently acquired by the contractor without such limitations or prohibit an agreement at no cost to the Government between the contractor and the data owner which provides for greater rights to the contractor.

11.11 Security and Privacy

(a) Agency rules of conduct that the Contractor and the Contractor's employees shall be required to follow:

In performing its duties related to management, operation, and/or access of systems containing sensitive PII under this contract, the Contractor, its employees and subcontractors shall comply with all applicable security requirements and rules of conduct as specified by the following:

1. Contractor employees must comply with agency personal identity verification (PIV) requirements in order to logically access Government systems.
2. System access granted under this contract is only for work required to perform official duties specified in the contract. The performance of any unrelated and/or unauthorized activity is prohibited.
3. Access to Government information systems (where applicable) will only be for the period stated in the contract. Thereafter, all accounts, passwords, and access associated with the contract will be terminated.
4. Disclosure of any system account information or system passwords to any unauthorized third-party is prohibited.
5. Exhibiting or divulging the content of any record or report to any person except in the performance of official duties specified in the contract is prohibited.
6. Using any data accessed with a Government system account for unauthorized purposes is prohibited.
7. No official record, report, database, or copy thereof, may be removed from Government premises or Government systems without prior written permission.
8. Contractor employees are prohibited from modifying, altering, or otherwise changing any Government system component or configuration except in the performance of official duties specified in the contract. Contractor employees are prohibited from issuing any system command or running any software, scripts, or programs on Government systems without prior authorization.
9. Contractor employees must not disclose sensitive or personal privacy-related information to any unauthorized third-party.
10. Contractor must notify the Government Contracting Officer immediately upon the termination of any Contractor or subcontractor employee so that system accounts, remote access, or other forms of system access can be terminated.
11. The use of Contractor-owned laptops or other portable media storage devices to process, transmit, or store sensitive PII is prohibited under this contract [unless the Contractor is authorized to access Government systems through the agency's virtual desktop infrastructure environment].
12. The Contractor must notify the Government Contracting Officer and the agency's Information Systems Security Officer (ISSO) immediately upon the discovery—or suspected discovery—of any type of security incident, malicious activity, or data breach affecting or that

might potentially affect the Government's network or specific systems.
13. Contractor employees with access to Government systems must agree to agency Rules of Behavior and shall complete annual security awareness training.

(b) A list of the anticipated threats and hazards that the Contractor must guard against.
The Contractor must use reasonable measures to guard against the following threats and hazards:
1. Unauthorized disclosure or use of sensitive system information—including system architecture, system configuration, system accounts, and system passwords.
2. Unauthorized disclosure or use of the contents of any information obtained from Government systems—including system records, system reports, or databases.
3. Unauthorized modification or alteration of any Government system component or configuration
4. Unauthorized circumvention, avoidance, or deception of any Government security system, measure, or control.
5. Unauthorized installation and/or use of hardware, software, firmware, portable media storage, or mobile devices on Government systems.
6. Unauthorized use of Government systems—including hardware, software, system accounts, Internet access, and email accounts—for activity which is not required to perform official duties under this contract.

(c) A description of the safeguards that the Contractor must specifically provide.
1. The Contractor shall limit access to any information related to this contract to those employees and subcontractors who require the information in order to perform their official duties under this contract.
2. The Contractor, Contractor employees, and subcontractors must physically secure PII when not in use and/or under the control of an authorized individual, and when in transit to prevent unauthorized access or loss.
3. When PII is no longer needed or required to be retained under applicable Government records retention policies, it must be destroyed through means that will make the PII irretrievable.
4. The Contractor shall only use PII obtained under the contract for purposes of the contract, and shall not collect or use such information for any other purpose without the prior written approval of the Contracting Officer.
5. At expiration or termination of this contract, the Contractor shall turn over to the Government, all PII obtained under the contract that is in its possession.
6. In the event of any actual or suspected breach of PII, the Contractor shall immediately report the breach to the Contracting Officer, the Contracting Officer's Representative (COR), and the agency's Information Systems Security Officer (ISSO).
7. In the event that a PII breach occurs as a result of the violation of a term of this contract by the Contractor or its employees, the Contractor shall, as directed by the Contracting Officer and at no cost to the Government, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected persons for a

period of at least 18 months from discovery of the breach. If the Government elects to provide and/or procure notification or identity protection services in response to a breach, the Contractor shall be responsible for reimbursing the Government for those expenses. The Contractor shall incorporate the substance of this clause, its terms and requirements in all subcontracts under this contract, and require written subcontractor acknowledgement of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.

(d) Requirements for a program of Government inspection during performance of the contract that will ensure the continued efficacy and efficiency of safeguards and the discovery and countering of new threats and hazards.

Work to be performed under this contract requires the design, development, operation, or disposal of a Federally-controlled information system containing sensitive personally identifiable information or handling sensitive personally identifiable information. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of personally identifiable information, the Contractor shall permit the Government access to, and information regarding, the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases, when requested by the Government, as part of its responsibility to ensure compliance with privacy and security requirements. The Contractor shall otherwise cooperate with the Government in assuring compliance with such requirements. Government access shall include independent validation testing of controls, system penetration testing by the Government, Federal Information Security Management Act data reviews, and access by agency Inspectors General for its reviews.

Definitions.

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace a person's identity, such as his or her name, social security number, or biometric records, that alone, or when combined with other personal or identifying information which is linked or linkable to a specific person, such as date and place of birth, or mother's maiden name.

"Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar situation where persons other than authorized users, and for other than authorized purpose, have access or potential access to Personally Identifiable Information, whether physical or electronic.

EXHIBIT 1: Criteria

Criteria	Author/ Issuing Body	Current version March 8, 2017
Council of Inspectors General on Integrity and Efficiency (CIGIE), Quality Standards for Inspection and Evaluation	CIGIE	January, 2012
A-130 Appendix III	OMB	July 2016
A-123 – Management's Responsibility for Enterprise Risk Management and Internal Control (Revised)	OMB	July 2016
The "Privacy Act of 1974," as amended	Legislation	2015
OMB Memoranda	OMB	Various
National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publications and Special Publications (SPs)	NIST	Various
NIST Cybersecurity Framework	NIST	February, 2014
Chief Financial Officers Council's (CFO Council) Enterprise Risk Management (ERM) Playbook	CFO Council	July, 2016
Chief Information Officers Council's (CIO Council) Federal Enterprise Architecture Security and Privacy Profile	CIO Council	July, 2004
Federal Emergency Management Agency's (FEMA) Federal Continuity Directives	FEMA	Various
Department of Homeland Security's Presidential Directives and Binding Directives	DHS	Various
United States Computer Emergency Preparedness Team (US-CERT) Incident Reporting Guidelines	US-CERT	Various
CPSC policies and procedures	CPSC	Various

EXHIBIT 2: CPSC Independent Evaluation Deliverables

a. Schedule of Deliverables (please note, these dates will be adjusted each year):

Item	SOW Reference	Deliverable:	Due to COR:
1	**5.2.1**	**Initial Meeting**	Within 5 business days following the award
2	**5.2.2**	**Independence Statement/Quality Control Assurance Statement**	Within 5 business days following the initial meeting
3	**5.2.3**	**Staffing List and Competency evidence**	Within 5 business days following the initial meeting
4	**5.2.4**	**Entrance Conference**	Within 10 business days following the initial meeting
5	**5.2.5**	**Planning Document(s):** **Objective** **Scope** **Methodology** **Research** **Identification of criteria & evidence** **Work Plan**	Within 20 business days following the entrance conference
6	**5.2.5**	**Field Work**	To be completed by October 20, 2017 or 10 business days before the due date established by the most recent OMB guidance, whichever is earlier.
7	**5.2.6**	**Status Briefings with COR**	Monthly, by the 15th calendar day of each month (5/15/2017 – 10/15/2017)

8	**5.2.6**	**Technical Status meetings with CPSC management and COR**	Monthly, as agreed upon by the individuals involved
9	**5.2.7**	**Draft Report and responses to the annual FISMA checklist in Cyberscope**	By October 20, 2017
10	**5.2.4**	**Exit Conference with management**	By November 1, 2017
11	**5.2.8**	**Final Report**	By November 7, 2017 or the due date established by the most recent OMB guidance, whichever is earlier

This requirement includes all of the terms and conditions of the Contractor's GSA Schedule.

52.217-8 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 10 days.

(End of clause)

52.217-9 Option to Extend the Term of the Contract (Mar 2000)
(a) The Government may extend the term of this contract by written notice to the Contractor within 10 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 15 days before the contract expires. The preliminary notice does not commit the Government to an extension.
(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 5 years.

(End of clause)

LOCAL CLAUSES:

LC1A CONTRACTOR'S NOTE

Deliveries and/or shipments shall not be left at the Loading Dock. **All deliveries shall be considered "inside deliveries"** to the appropriate room at the Consumer Product Safety Commission (CPSC) and in accordance with the instructions below. When scheduling deliveries the purchase order number shall always be referenced and all packages shall clearly display the Purchase Order Number on the outside of the cartons and/or packages, to include the packing slip.

ATTENTION GOVERNMENT VENDOR

A. DELIVERY INSTRUCTIONS:

1. DELIVERY INSTRUCTIONS FOR LARGE OR HEAVY ITEMS:

If the shipment or item being delivered requires use of a loading dock, advance notification is required. The contractor shall contact the Shipping and Receiving Coordinator at 301-892-0586 or Constantia Demas (301) 504-7544 forty-eight (48) hours in advance of the date the items are to arrive to schedule use of the loading dock.

LOADING DOCK HOURS OF OPERATION:

9:00 am to 11:00 am or 1:30 pm to 4:00 pm
Monday through Friday (except holidays)

Please notify contact person if there is a change in the delivery date. For changes, delays, or assistance please contact CPSC as follows:

Facilities Management Support Services (301) 504-7091 and

The COR – See page 1 of award.

Upon arrival, the driver should contact the CPSC Guard, 301-504-7721, at the loading dock to obtain assistance in using freight elevators and to gain access to CPSC security areas.

2. DELIVERY INSTRUCTION FOR SMALL ITEMS

When delivering or shipping small items, the contractor and/or carrier service shall report to the 4th floor lobby, North Tower, 4330 East West Highway, to sign in with the CPSC guard. Upon completion of signing in, the contractor shall deliver all shipments to the COR in the OIG Suite, Room 702-C. After delivery, delivery personnel shall promptly depart the building.

MAIL ROOM HOURS OF OPERATION:

Monday through Friday (except holidays) – 7:30 am to 5:00 pm

B. 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. For Contracts on Form OF347 - The contract or purchase order number on the Form OF347 shall include the purchase order number indicated in blocks #2 and #3.

6. For Contract on Form SF1449 - The contract or purchase order number on the Form SF1449 shall include the purchase order number and /or Task number indicated in blocks #2 and #4. For Example: CPSC-D-17-0012/0003

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

8. Shipping cost terms (if applicable).

9. Payment terms.

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

11. 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.

C. 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.

D. INSPECTION & ACCEPTANCE PERIOD

Unless otherwise stated in the Statement of Work or Description, the Commission will ordinarily inspect all materials/services within two (2) 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.

E. ALL OTHER INFORMATION RELATING TO THE PURCHASE ORDER

Contact: Contract specialist Cassandra Sterba at 301-504-7838.

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.

LC 5 Contracting Officer's Representative (COR) Designation

a. The following individual has been designated at the Government's COR for this contract:

Mary Meier / MMeier@cpsc.gov / (301) 504-7040

b. The CPSC COR is responsible for performing specific technical and administrative functions, including:

(1) performing technical evaluation as required;

(2) assisting the Contractor in the resolution of technical problems encountered during performance; 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; and

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

c. The COR, who may be personally liable for unauthorized acts, is not authorized to and shall not:

(1) make changes in scope of work, contract schedules, and/or specifications, or to make changes that affect price, quality, quantity or delivery,

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

(3) make commitments or changes that affect price, or take any action that commits the Government or could lead to a claim against the Government.

d. This delegation is not redelegable and remains in effect during the period of performance of the contract.

e. 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.

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.

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. Contracted 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 contracted personnel, including full name, social security number, and place (city and state) and date of birth to the designated Contracting Officer's 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 contracted employees at the Consumer Product Safety Commission. The COR shall ensure that each contractor employee completes CPSC's official out processing procedures. The contracted 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.

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 protected 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.

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 quote 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.