

<b>SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEM</b> <i>OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, &amp; 30</i>				1. REQUISITION NUMBER REQ-2400-09-0058		PAGE OF 1 36			
2. CONTRACT NO CPSC-D-10-0003		3. AWARD/ EFFECTIVE DATE <i>4/29/2010</i>		4. ORDER NUMBER		5. SOLICITATION NUMBER CPSC-Q-09-0016		6. SOLICITATION ISSUE DATE 01/21/2010	
7. <b>FOR SOLICITATION INFORMATION CALL:</b>		a. NAME Robert Frost			b. TELEPHONE NUMBER (301) 504-7116		8. OFFER DUE DATE/LOCAL TIME ET		
9. ISSUED BY  CONSUMER PRODUCT SAFETY COMMISSION DIV OF PROCUREMENT SERVICES 4330 EAST WEST HWY ROOM 517 BETHESDA MD 20814				CODE FMPS	10. THIS ACQUISITION IS <input checked="" type="checkbox"/> UNRESTRICTED OR <input type="checkbox"/> SET ASIDE. % FOR.  <input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> EMERGING SMALL BUSINESS <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> SOLE SOURCE <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> 8(A)  NAICS: 541519 SIZE STANDARD: \$23.00				
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input type="checkbox"/> SEE SCHEDULE		12. DISCOUNT TERMS Net 30			13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700) <input type="checkbox"/>		13b. RATING		14. METHOD OF SOLICITATION <input checked="" type="checkbox"/> RFQ <input type="checkbox"/> IFB <input type="checkbox"/> RFP
15. DELIVER TO  CONSUMER PRODUCT SAFETY COMMISSION OFFICE OF INFORMATION SERVICES 4330 EASTWEST HIGHWAY ROOM 504 BETHESDA MD 20814				CODE EXIT	16. ADMINISTERED BY  CONSUMER PRODUCT SAFETY COMMISSION DIV OF PROCUREMENT SERVICES 4330 EAST WEST HWY ROOM 517 BETHESDA MD 20814				
17a. CONTRACTOR/ OFFEROR  SECURE IT ATTN JIM GRAHAM 1902 CAMPUS COMMONS DR STE 100 RESTON VA 20191-1581				CODE 	FACILITY CODE	18a. PAYMENT WILL BE MADE BY  CONSUMER PRODUCT SAFETY COMMISSION DIVISION OF FINANCIAL SERVICES 4330 EAST WEST HWY ROOM 522 BETHESDA MD 20814			CODE FMFS
TELEPHONE NO 703 230-0734				17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER <input type="checkbox"/>					18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED <input type="checkbox"/> SEE ADDENDUM
19. ITEM NO	20. SCHEDULE OF SUPPLIES/SERVICES				21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT	
	Delivery Order Contract-Information Technology Security Consulting Services (ITSCS)  This requirement is awarded in accordance with the contractor's applicable GSA Federal Supply Schedule Contract GS-35F-0644N.  This contract includes Firm Fixed Prices for Annual support to assist CPSC in its certification and accreditation program for the Basic and each Option Period if exercised. <i>(Use Reverse and/or Attach Additional Sheets as Necessary)</i>								
25. ACCOUNTING AND APPROPRIATION DATA						26. TOTAL AWARD AMOUNT (For Govt. Use Only) \$0.00			
27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4, FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED.									
27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4 FAR 52.212-5 IS ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> 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 HEREIN					29. AWARD OF CONTRACT REF. <input checked="" type="checkbox"/> OFFER DATED <u>02/04/2010</u> 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) 				
30b. NAME AND TITLE OF SIGNER (Type or print)			30c. DATE SIGNED		31b. NAME OF CONTRACTING OFFICER (Type or print) Donna Hutton		31c. DATE SIGNED <i>4/29/10</i>		

*Todd Stevenson*

19 ITEM NO.	20 SCHEDULE OF SUPPLIES/SERVICES	21 QUANTITY	22 UNIT	23 UNIT PRICE	24 AMOUNT
	<p>This contract includes Firm Fixed Price fully loaded hourly rates for the Base and all option periods for the categories set forth below. The hourly rates will be used to negotiate Task Orders over and above the annual support issued against the contract if required. The rates shall be in accordance with the contractor's applicable GSA Federal Supply Schedule Contract.</p> <p>0001 Base Period Effective date of the award - 09/30/2010.</p>				
0001 AA	<p>Annual support to assist CPSC in its certification and accreditation program. Negotiated Amount \$74,000.00 DELIVERY-DURING THE BASE PERIOD AS SET FORTH IN TASK ORDER IF ISSUED In accordance with the attached statement of work.</p> <p>Obligated Amount: \$0.00</p>	1	LO	0.00	
0001 AB	Information Security Engineer - Level 2		HR	68.00	0.00
0001 AC	Information Security Engineer - Level 3		HR	85.00	0.00
0001 AD	Information Security Engineer - Level 4		HR	115.00	0.00
	Continued ...				

32a QUANTITY IN COLUMN 21 HAS BEEN  RECEIVED  INSPECTED  NOTED ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS

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 \_\_\_\_\_ 34 VOUCHER NUMBER \_\_\_\_\_ 35 AMOUNT VERIFIED CORRECT FOR \_\_\_\_\_ 36 PAYMENT  COMPLETE  PARTIAL  FINAL \_\_\_\_\_ 37 CHECK NUMBER \_\_\_\_\_

PARTIAL  FINAL

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 \_\_\_\_\_

**CONTINUATION SHEET**

REFERENCE NO OF DOCUMENT BEING CONTINUED  
 CPSC-D-10-0003

PAGE OF  
 3 36

NAME OF OFFEROR OR CONTRACTOR  
 SECURE IT

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0001 AE	Information Security Engineer - Level 5		HR	125.00	0.00
	0002 Option Period One 10/01/2010 - 09/30/2011				
0002 AA	Annual support to assist CPSC in its certification and accreditation program. Negotiated Amount \$40,468.50 DELIVERY-DURING OPTION PERIOD ONE AS SET FORTH IN TASK ORDER IF ISSUED In accordance with the attached statement of work.	1	LO	0.00	
	Obligated Amount: \$0.00				
0002 AB	Information Security Engineer - Level 2		HR	69.36	0.00
0002 AC	Information Security Engineer - Level 3		HR	86.70	0.00
0002 AD	Information Security Engineer - Level 4		HR	117.30	0.00
0002 AE	Information Security Engineer - Level 5		HR	127.50	0.00
	0003 Option Period Two 10/01/2011 - 09/30/2012				
0003 AA	Annual support to assist CPSC in its certification and accreditation program. Negotiated Amount \$41,884.90 DELIVERY-DURING OPTION PERIOD TWO AS SET FORTH IN TASK ORDER IF ISSUED In accordance with the attached statement of work.	1	LO	0.00	
	Obligated Amount: \$0.00				
0003 AB	Information Security Engineer - Level 2		HR	70.75	0.00
0003 AC	Information Security Engineer - Level 3		HR	88.43	0.00
	Continued ...				

## CONTINUATION SHEET

REFERENCE NO OF DOCUMENT BEING CONTINUED  
CPSC-D-10-0003PAGE OF  
4 36NAME OF OFFEROR OR CONTRACTOR  
SECURE IT

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0003 AD	Information Security Engineer - Level 4		HR	119.65	0.00
0003 AE	Information Security Engineer - Level 5		HR	130.05	0.00
	0004 Option Period Three 10/01/2012 - 09/30/2013				
0004 AA	Annual support to assist CPSC in its certification and accreditation program. Negotiated Amount \$43,350.87 DELIVERY-DURING OPTION PERIOD THREE AS SET FORTH IN TASK ORDER IF ISSUED In accordance with the attached statement of work.  Obligated Amount: \$0.00	1	LO	0.00	
0004 AB	Information Security Engineer - Level 2		HR	72.16	0.00
0004 AC	Information Security Engineer - Level 3		HR	90.20	0.00
0004 AD	Information Security Engineer - Level 4		HR	122.04	0.00
0004 AE	Information Security Engineer - Level 5		HR	132.65	0.00
	0005 Option Period Four 10/01/2013 - 09/30/2014				
0005 AA	Annual support to assist CPSC in its certification and accreditation program. Negotiated Amount \$44,868.15 DELIVERY-DURING OPTION PERIOD FOUR AS SET FORTH IN TASK ORDER IF ISSUED In accordance with the attached statement of work.  Obligated Amount: \$0.00	1	LO	0.00	
0005 AB	Information Security Engineer - Level 2		HR	73.61	0.00
0005 AC	Information Security Engineer - Level 3		HR	92.01	0.00
0005 AD	Information Security Engineer - Level 4		HR	124.48	0.00
0005 AE	Information Security Engineer - Level 5		HR	135.30	0.00
	The total amount of award: \$0.00. The obligation Continued ...				

**CONTINUATION SHEET**

REFERENCE NO. OF DOCUMENT BEING CONTINUED  
CPSC-D-10-0003

PAGE OF  
5 36

NAME OF OFFEROR OR CONTRACTOR  
SECURE IT

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	for this award is shown in box 26.				

## 1. CONTRACT TYPE

This contract is for Information Technology Security Consulting Services (ITSCS) including that which will assist CPSC in complying with Office of Management and Budget/ National Institute of Standards and Technology (OMB/NIST) security regulations for federal information systems. It is a firm-fixed price, Indefinite Quantity, Indefinite Delivery, Performance Based, Delivery Order contract with Options. Task Orders will be issued for work as required. The guaranteed minimum for the entire contract is \$10,000.00. If exercised, the guaranteed minimum for each option year is \$10,000.00. The maximum for the entire contract (Basic Period and all option years inclusive) is not to exceed \$2,000,000.00. If travel costs are required under tasks, the travel costs will be negotiated as Firm Fixed Price amounts in accordance with the Federal Travel Regulation. This contract includes a Base Period and four one year option periods.

## 2. SERVICES AND PRICES

- a. Obtain contractor annual support to assist CPSC in its certification and accreditation program. The support will be for the Basic Period and each option period if exercised.
- b. Fixed Price Hourly rates in support of other task orders as required.
- c. Each hourly rate is a fully loaded labor rate (including, but not limited to, applicable direct and indirect costs such as compensation, fringe benefits, insurance, social security, overhead, general and administrative expenses, and profit.)
- d. Travel will be negotiated at Firm Fixed Price amounts in accordance with the Federal Travel Regulation for each task order.
- e. Services provided by this contract shall be accomplished through the issuance of task orders. All task orders over and above the annual support will be negotiated based on the hourly rates specified in the schedule of services for the applicable period of performance indicated. If unanticipated additional

labor categories are required, these labor categories will be added to the contract and the rates for those categories will be negotiated prior to the issuance of a task order.

### **3. BACKGROUND INFORMATION**

The United States (U.S.) Congress and the Office of Management and Budget (OMB) have instituted a number of laws, regulations, and directives that govern establishment and implementation of federal information security practices. These laws, regulations, and directives establish agency-level responsibilities for information security, define key information security roles and responsibilities, identify minimum information security controls, specify compliance reporting rules and procedures, and provide other essential requirements and guidance.

### **4. OBJECTIVES**

The objective of this statement of work is to obtain annual contractor support to assist CPSC in its certification and accreditation program. The contractor shall provide information assurance expertise to support the development of documentation required for the certification and accreditation (C&A) of CPSC's General Support System (GSS) and one (1) Major Application (CPSRMS). The C&A documentation must be written to satisfy standards set forth by CPSC, OMB and NIST. These activities are described below in the descriptions of required deliverables. All work done under this contract must be coordinated with the CPSC Information Systems Security Officer (ISSO) or his designee.

### **5. STATEMENT OF WORK**

Independently, and not as an agent of the Government, the contractor shall furnish all necessary personnel, materials, services, and facilities to support the agency in its efforts to comply with Federal Information Security Management Act (FISMA) requirements and each Task Order as

issued; except as provided in Section 16 "Government Furnished Materials."

a. The Contractor shall provide annual Certification and Accreditation support services. This shall include:

1. The Contractor shall perform an asset inventory of hardware and software for both the CPSC General Support System (GSS) and the CPSRMS application. The Contractor shall provide written *Hardware and Software Inventory* reports consisting of all key assets that make up both the CPSC GSS and the CPSRMS application. The information for the asset inventory may be obtained through a combination of automated inventory tools as well as through on-site inspection of systems and staff interviews.
2. The Contractor shall provide a CPSC *Security Test and Evaluation Plan* for both the CPSC General Support System and the CPSRMS application. The plan must include a detailed description of the testing methodology. Additionally, the following requirements pertaining to the ST&E plan must be met:
  - a. The ST&E plan must clearly state the roles and responsibilities of those involved in the ST&E and must specify CPSC personnel to be involved in the exercise. This includes individuals to be interviewed, those required to demonstrate system controls, and those required to provide documentation.
  - b. The ST&E plan must specify required access to the system or its components; this must be specified in the plan so that it can be coordinated by CPSC in advance.
  - c. The ST&E plan must define the scope of testing (i.e., all "moderate" controls in NIST SP 800-53, CPSC GSS LAN, etc.).
  - d. The ST&E plan must include a list of CPSC-owned system documentation, lists, policies, plans, guides that will be reviewed.
3. The Contractor shall perform a *Security Test and Evaluation* (compliant with NIST Special Publication 800-53 and 800-53A) of the CPSC General Support System and the CPSRMS application. The assessment of CPSC's

security controls shall use established assessment procedures to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the respective system. The Contractor shall provide written *Security Test and Evaluation reports* (for both the GSS and CPSRMS application). Additionally, the following requirements pertaining to the ST&E must be met:

- a. The Contractor shall provide specific recommendations on how to correct deficiencies in system/application security controls.
- b. A minimum of two analysts must conduct testing.
- c. Analysts conducting tests must be fully knowledgeable of the technologies that comprise the CPSC GSS and CPSRMS application, to include operating systems, database software, web server software, application software, and other platforms as necessary.
- d. Analysts must be able to appropriately assess the output of any automated testing tools, used to conduct testing, and be able to identify false positives, inconsistent results, and inaccuracies.
- e. Analysts must possess at least three (3) years experience conducting similar ST&E tasks on federal information systems and possess at least one professional security/IT auditing certification.
- f. Analysts conducting technical control tests must have an authorized system user run any test scripts or system commands. The analyst must not initiate any direct system testing or enter any system commands on any production system.
- g. Analysts conducting tests must get prior CPSC approval before initiating tests involving social engineering, vulnerability scanning tools, penetration techniques, or data extraction.
- h. Analysts conducting tests must document in the ST&E report, if a control is not in place or does not meet a predetermined standard, why that particular control failed.
- i. Analysts conducting tests must rank findings by risk: *low, moderate, or high*.

4. The Contractor shall perform an independent *System Risk Assessment* for the CPSC General Support System and the CPSRMS application (compliant with NIST Special Publication 800-30) and provide written System Risk Assessment reports for both systems. The System Risk Assessment shall verify the adequacy of minimum baseline security controls and recommend appropriate changes: either additional or alternative security controls. Additionally, the following requirements pertaining to the System Risk Assessment must be met:
  - a. The System Risk Assessment must focus on asset, threat, and vulnerability identification.
  - b. Analysts must provide a calculation of risk for each threat/vulnerability pair in the form of a *risk matrix*.
  - c. Recommended security controls must be specific, detailed enough to allow for representation as a technical solution, and practical enough to be cost-effective. When adequate security controls do not exist or are not practical, analyst must recommend the consideration of risk acceptance.
  - d. Analysts must review current user practices, system operations, system security features, and security control weaknesses to help form risk determinations.
  - e. Analysts must be able to successfully interact with CPSC technical and management staff during the information acquisition process.
  - f. Analysts must possess at least three (3) years experience conducting similar system risk assessment tasks for federal information systems and possess at least one professional security/IT auditing certification.
  
5. The Contractor shall provide a written *System Security Plan* (compliant with NIST Special Publication 800-18) for both the CPSC General Support System and the CPSRMS application. The System Security Plan shall accurately describe the security posture of the CPSC GSS and the CPSRMS application relative to NIST 800-53, 800-26, 800-18 and other industry "best practice" security controls. Additionally, the System Security Plan must address the following:

- a. The SSP must accurately describe the system/application, its components, and its operating environment.
  - b. The SSP must document the system/application security category.
6. Under Task Orders if issued, the Contractor shall provide a system Contingency Plan (compliant with NIST Special Publication 800-34) for both the CPSC General Support System and the CPSRMS application. As an appendix or supplemental document, the Contingency Plan must include a relevant Business Impact Assessment for the associated system/application.
7. Under Task Orders if issued, the Contractor shall provide a written Configuration Management Plan (compliant with NIST Special Publications 800-18 and 800-12) for all CPSC information systems.
8. Under Task Orders if issued, the Contractor shall provide a written *Privacy Impact Assessment* of CPSC's GSS, CPSRMS application, public web site, or other sensitive information system to determine if restricted information is appropriately protected. Additionally, the Privacy Impact Assessment must address the following:
  - a. Describe privacy controls
  - b. Describe privacy threats
  - c. Describe privacy vulnerabilities
  - d. Document the locations of PII in CPSC systems and applications
9. Under Task Orders if issued, the Contractor shall provide a written *Security Awareness and Training Plan*. The Security Awareness and Training Plan must document CPSC's security awareness training program and be compliant with NIST Special Publication 800-50. Additionally, the Security Awareness and Training Plan must address the following:
  - a. Describe the appropriate type and frequency of training for CPSC personnel
  - b. Describe the appropriate type and frequency of training for security/technical staff
  - c. Describe how training should be tracked and documented

- d. Describe the process for evaluating training effectiveness
- e. Describe the roles and responsibilities associated with the security awareness training program

## 6. PROFESSIONAL SKILLS REQUIRED:

- a. The Government's minimum requirements for each labor category are identified in the paragraphs below. The Contractor may propose to the Government, at their discretion, additional labor categories and job descriptions within the scope of the contract.

The Contractor must provide pricing by hourly rate for the following potential labor categories for task orders to be negotiated under this contract. Individuals proposed must meet minimum qualifications. Prior to submitting their proposal, these qualifications may be negotiated. All references to "education" and "experience" below refer to minimum education and experience requirements. If the Contractor proposes revisions to the qualifications, they must do so at the time the proposal is submitted, in writing, otherwise minimums will be enforced. The Contractor may propose additional labor categories to be listed on the contract if they anticipate a possible need for additional categories. All individuals performing under these labor categories must pass any required personal identity verification and security clearance.

### - Information Security Engineer - Level 2

Education: B.A. or B.S. degree and 3 years minimum equivalent experience in a related field.  
General Experience: Must possess professional training or equivalent experience in one of the following types of disciplines: computer science, information systems management, information security, engineering, math, physics, or a closely related field. These staff have demonstrated specific experience in one or more of the

technical information security functional engineering areas: Computer Security, Communications Security, TEMPEST, or Operations Security. Engineers demonstrate experience in analytical problem solving involving systems design and integration, system analysis and testing, independent verification and validation (IV&V), or risk analysis and have demonstrated experience with information security products and systems.

Specialized Experience: Engineers provide the expertise to conduct information security systems analysis, certification and accreditation, integration of secure products, security test and evaluation (ST&E), or development of complex information systems that will meet the assigned information security requirements. Engineers demonstrate a broad knowledge of the technical information security discipline and apply extensive expertise as an information engineering professional.

**- Information Security Engineer - Level 3**

Education: B.A. or B.S. degree and 5 years minimum equivalent experience in a related field.

General Experience: Must possess professional training or equivalent experience in one of the following types of disciplines: computer science, information systems management, information security, engineering, math, physics, or a closely related field. These staff have demonstrated specific experience in one or more of the technical information security functional engineering areas: Computer Security, Communications Security, TEMPEST, or Operations Security. Engineers demonstrate experience in analytical problem solving involving systems design and integration, system analysis and testing, independent verification and validation (IV&V), or risk analysis and have demonstrated experience with information security products and systems.

Specialized Experience: Engineers provide the expertise to conduct information security systems analysis, certification and accreditation, integration of secure products, security test and evaluation (ST&E), or development of complex information systems that will meet the assigned information security requirements. Engineers demonstrate a broad knowledge of the technical information

security discipline and apply extensive expertise as an information engineering professional.

**- Information Security Engineer - Level 4**

Education: B.A. or B.S. degree and 8 years minimum equivalent experience in a related field.

General Experience: Must possess professional training or equivalent experience in one of the following types of disciplines: computer science, information systems management, information security, engineering, math, physics, or a closely related field. These staff have demonstrated specific experience in one or more of the technical information security functional engineering areas: Computer Security, Communications Security, TEMPEST, or Operations Security. Engineers demonstrate experience in analytical problem solving involving systems design and integration, system analysis and testing, independent verification and validation (IV&V), or risk analysis and have demonstrated experience with information security products and systems.

Specialized Experience: Engineers provide the expertise to conduct information security systems analysis, certification and accreditation, integration of secure products, security test and evaluation (ST&E), or development of complex information systems that will meet the assigned information security requirements. Engineers demonstrate a broad knowledge of the technical information security discipline and apply extensive expertise as an information engineering professional.

**-Information Security Engineer - Level 5**

Education: B.A. or B.S. degree and 10 years minimum equivalent experience in a related field.

General Experience: Must possess professional training or equivalent experience in one of the following types of disciplines: computer science, information systems management, information security, engineering, math, physics, or a closely related field. These staff have demonstrated specific experience in one or more of the technical information security functional engineering areas: Computer Security, Communications Security, TEMPEST, or Operations Security. Engineers demonstrate experience in analytical problem solving involving systems design and

integration, system analysis and testing, independent verification and validation (IV&V), or risk analysis and have demonstrated experience with information security products and systems.

Specialized Experience: Engineers provide the expertise to conduct information security systems analysis, certification and accreditation, integration of secure products, security test and evaluation (ST&E), or development of complex information systems that will meet the assigned information security requirements. Engineers demonstrate a broad knowledge of the technical information security discipline and apply extensive expertise as an information engineering professional. Engineers generally have a security clearance at the level of Secret or higher and perform in an environment involving special security requirements, as task orders may dictate.

b.. Any persons employed by the Contractor and assigned to perform work specified in this contract shall at all times be under the control and full responsibility of the Contractor. The Contractor shall be responsible for standards of professional employee competency, conduct, and integrity.

c.. The Contractor shall comply with all Federal, State, and local laws applicable to work performed hereunder. The Contractor shall be responsible for taking such disciplinary action with respect to its employees as may be necessary.

d.. It is the Contractor's responsibility to ensure that personnel are adequately trained and technically qualified to perform services under this contract.

e.. *List any special requirements for contractor personnel since this is a security contract.*

## 7. MEETINGS, REPORTS, DELIVERABLE ITEMS AND SCHEDULE

Description	Quantity/Frequency	Schedule
Project Kickoff Meeting	1 ea	To be negotiated at the time of issuance of the Task Order
Annual support to	Up to 5 ea	To be negotiated at

assist CPSC in its certification and accreditation program.		the time of issuance of the Task Order
Task Order deliverables	ea	To be negotiated at the time of issuance of the Task Order

**8. REPORTS AND PLANS**

All reports, plans and deliverables shall be submitted to CPSC in electronic format either in Word or PDF format. The required elements of the report and its format shall follow standard industry practice. The government will require 5 days to review a draft of any report or document before it is finalized. The government will accept the report based on the report being technically acceptable.

**9. ACCEPTANCE OF DELIVERABLES**

a. Acceptance/rejection/ comments/corrections and changes will be transmitted to the Contractor by the CPSC Project Officer, in writing. The CPSC will require 30 calendar days to evaluate each deliverable for acceptance by the Government.

b. Acceptance/rejection will be based on the report meeting the specified objectives and the functional requirements for each task.

**10. PERFORMANCE ACCEPTANCE PLAN/PERFORMANCE MEASURES**

Objectives

Thresholds

Deliverables

Defined and consistent document formats. All documents developed under this contract must have a well defined and consistent format. Documents must use a logical, predetermined, and easy to follow format that makes it easy to determine document

completeness. Basic information requirements for each C&A document must be easily identified and maintained through the use of document templates.

Consistency across documents. All documents developed under this contract must be complementary of each other and present a consistent picture of the security posture of the CPSC GSS and CPSRMS application. The *Hardware and Software Inventory, Security Test and Evaluation Plan, Security Test and Evaluation report, Risk Assessment, and System Security Plan* must all be interconnected, mutually supporting and uniform in their evaluation of the security posture of the CPSC GSS and CPSRMS application.

Clearly written. All documents developed under this contract must be written in clear, easy to understand English. When technical or esoteric terms are used, these expressions must be clearly defined in the document in a glossary of terms.

#### Reporting Requirements:

Reports are accurate, complete, and properly formatted in accordance with the delivery schedule

Reports are submitted timely 95% of the time. Information provided is 100% accurate.

provided in Paragraph 7,  
Meetings, Reports,  
Deliverable Items and  
Schedule

Acceptable performance is indicated by meeting the thresholds above.

#### **11. PERIOD OF PERFORMANCE**

a. The period of performance is from the effective date of the contract through 09/30/2010 with four one year option periods.

b. Task Orders issued during the base, any option, or award term period are effective through completion of the Period of Performance set forth in each Task Order.

#### **12. PLACE OF PERFORMANCE**

Work shall be performed at CPSC headquarters in Bethesda, MD or at the CPSC Lab currently located in Gaithersburg MD. Note that the lab may be relocated during the period of performance. The contractor will be required to continue performance at the new CPSC Lab location. Some performance may be done remotely at the discretion of the Project Officer.

#### **13. WITHHOLDING OF CONTRACT PAYMENT**

Notwithstanding any other payment provision of this contract, failure of the Contractor to submit required reports when due, or failure to perform or deliver required work, supplies, or services, will result in the withholding of payments under this contract unless such failure arises out of causes beyond the control, and without the fault or negligence of the Contractor. The Government will promptly notify the Contractor of its intention to withhold payment of any invoice or voucher submitted.

#### **14. PROJECT OFFICER DESIGNATION**

a. Patrick Manley of the Commission's Division of

Information Technology Policy and Planning has been designated as the Government's Project Officer for this contract. This individual may be reached on (301) 504-6946.

b. THE PROJECT OFFICER 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 on schedule in accordance with Section 6, Meetings, Reports, Deliverable Items and 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 PROJECT OFFICER 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.

**15. KEY PERSONNEL**

a. The Contractor has identified the following individuals as its key personnel who will be most directly involved in performing and/or supervising the services as required under this contract.

NAME	TITLE
Jim Graham	Project Manager
Joe Zadjura	IT Security Engineer Level 5
Bogdan Dragomir	IT Security Engineer Level 4
Jamie Poole	IT Security Engineer Level 4
Antonio Uriarte	IT Security Engineer Level 3

b. The personnel specified above 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. Prior to substitution of key personnel, the Contractor shall obtain the written consent of the Contracting Officer as to the acceptability of the succeeding personnel: Provided that the Contracting Officer may ratify in writing such substitution and such ratification shall constitute the consent of the Contracting Officer required by this clause.

#### **16. GOVERNMENT-FURNISHED MATERIALS**

The Government shall furnish to the Contractor for use in connection with this contract the materials set forth below:

- 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 the performance of this contract shall be furnished by the Contractor.

#### **17. CONTRACT CLAUSES**

The following clauses are incorporated by reference:

## FEDERAL ACQUISITION REGULATION CLAUSES:

52.217-8 Option to Extend Services. (Nov 1999)  
52.228-5 Insurance-Work on a Government Installation  
(Jan 1997)  
52.245-1 Government Property (June 2007) Alternate 1

The following clauses are incorporated in full text:

## FEDERAL ACQUISITION REGULATION CLAUSES:

52.216-18 Ordering (Oct 1995)  
  
52.216-19 Order Limitations. (Oct 1995)  
52.216-22 Indefinite Quantity. (Oct 1995)  
52.217-9 Option to Extend the Term of the Contract.  
(Mar 2000)

## CPSC LOCAL CLAUSES:

520000-4004A CONTRACTOR'S NOTE  
LC 6 Contractor Use of CPSC Information Technology  
(IT) Resources  
LC-21 DISCLOSURE OF INFORMATION  
LC-24 NONDISCLOSURE OF ANY DATA DEVELOPED UNDER THIS  
CONTRACT  
LC 30 Security and Personal Identity Verification  
Procedures  
LC 31 RESTRICTIONS ON USE OF INFORMATION  
LC 32 STANDARDS OF CONDUCT  
LC 34 Technology Additions/Substitutions

the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; *provided*, that the Contractor shall not be required to make any deliveries under this contract after the completion date of Phase 4.

(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 30 days of expiration; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 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 48 months.

(End of clause)

**1. 520000-4004A 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) 366-7018 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) 504-7085  
and  
Project Officer Patrick Manley 301 504-6946.

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 Mail Room, Room 516. 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. Taxpayer Identification Number (TIN).
3. Invoice date (use of invoice number in addition to invoice date is prudent but not required).
4. 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 or services.
5. Description, price and quantity of goods or services actually delivered or rendered.
6. Shipping cost terms (if applicable).
7. Payment terms.

8. ACH Vendor Information which includes: the Financial Institution, routing transit number, and depositor account number. In addition please specify whether account is a checking account or savings account.

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

10. Name (where practicable), 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:

Accounting Officer  
Div. of Financial Services, Room 522  
U.S. Consumer Product Safety  
Commission  
4330 East-West Hwy  
Bethesda, MD 20814

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.

#### C. PAYMENT

Payment will be made as close as possible to, but not later than, the 30<sup>th</sup> 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 the Accounting Officer at (301) 504-7203 or 301-504-7130 or at the following address:

Accounting Officer  
Div. of Financial Services, Room 522  
U.S. Consumer Product Safety Commission  
4330 East-West Hwy  
Bethesda, MD 20814

Complaints related to the late payment of an invoice should be directed to Deborah Peebles Hodge, Director, Division of Financial Services at the same address (above).

**D. INSPECTION & ACCEPTANCE PERIOD**

The Commission at the destination point within thirty (30) calendar days after the date of receipt shall inspect all materials/services. The CPSC contact person will transmit disapproval, if appropriate.

**E. ALL OTHER INFORMATION RELATING TO THE PURCHASE ORDER**

Contact: Robert J. Frost 301 504-7116.

**F. 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.

**G. 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 Services Management Officer (Jim Shupe) in the Facilities Management Support Services Branch (Room 520). 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 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 21 DISCLOSURE OF INFORMATION**

a. The Contractor shall submit to the Commission any report, manuscript or other document containing the results of work performed under this contract. This document shall not be published or otherwise disclosed by the contractor.

b. Should the contractor subsequently apply to the Consumer Product Safety Commission for permission to publish documents containing the results of this work and the release is approved in writing, 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-D-10-0003. 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.

**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 (below) from each employee who will work on this contract or have access to data obtained or developed under this contract.

I, (employee name, signature and date here) agree that I 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.

**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 Technical Representative (COTR). 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 COTR 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 COTR within five (5) days of written notification from the COTR of those contractor employees requiring background investigations.

f. Upon completion of the investigation, the COTR 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 COTR 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 COTR 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.

1. The COTR shall be responsible for proper separation of contracted employees at the Consumer Product Safety Commission. The COTR 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.

(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.

### 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

4

**LC 34 Technology Additions/Substitutions**

- a. Due to the rapidly changing field of information technology (IT) and potential advancements during performance of this contract, the contractor may propose technological upgrades, additions and substitutions to enhance performance of IT delivered under the contract. The Contractor shall request changes in writing to the Contracting Officer and shall provide full documentation on any proposed additions/substitutions.
- b. Any proposed changes must comply with these conditions:
- 1) The additional/substituted item(s) shall be fully compatible with item(s) in the CLIN as appropriate;
  - 2) The additional/substituted item(s) shall meet or exceed all specifications applicable to the original item(s);
  - 3) The additional/substituted item(s) shall meet all of the marketability requirements of the specification to ensure field-proven, COTS systems and configurations.
- c. Any proposed change, if accepted by the Government, shall be made via a written modification to the contract.
- d. The fact that the Contractor requests, and the Government accepts, an addition/substitution shall not automatically extend the required delivery dates of any items. Upon approval and acceptance of a replacement, CPSC and the Contractor may mutually agree to a reasonable extension of the required delivery dates.
- e. If it is determined that additional work is required, specific changes may be made to task descriptions or additional tasks added. Any such changes will be made through mutual agreement between the Government and the contractor and will be finalized through a bilateral modification to the contract.