

<b>SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS</b> OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30				1 REQUISITION NUMBER REQ-2400-16-0099		PAGE OF 1 14	
2 CONTRACT NO GS-35F-0585J		3 AWARD EFFECTIVE DATE 09/20/2016		4 ORDER NUMBER CPSC-F-16-0082		5 SOLICITATION NUMBER	
7 FOR SOLICITATION INFORMATION CALL:		8 NAME Greg Grayson		9 TELEPHONE NUMBER (No collect calls) 301-504-7725		6 SOLICITATION ISSUE DATE	
9 ISSUED BY CONSUMER PRODUCT SAFETY COMMISSION DIV OF PROCUREMENT SERVICES 4330 EAST WEST HWY ROOM 523 BETHESDA MD 20814				10 THIS ACQUISITION IS <input checked="" type="checkbox"/> UNRESTRICTED OR SET ASIDE % FOR SMALL BUSINESS WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS BUSINESS (WOSB) PROGRAM HUBZONE SMALL BUSINESS EDWOSB SERVICE DISABLED VETERAN-OWNED SMALL BUSINESS (A) SIZE STANDARD			
11 DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED SEE SCHEDULE		12 DISCOUNT TERMS Net 30		13a THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)		13b RATING	
15 DELIVER TO CONSUMER PRODUCT SAFETY COMMISSION OFFICE OF INFORMATION SERVICES 4330 EASTWEST HIGHWAY ROOM 839-23 BETHESDA MD 20814				18 ADMINISTERED BY CONSUMER PRODUCT SAFETY COMMISSION DIV OF PROCUREMENT SERVICES 4330 EAST WEST HWY ROOM 523 BETHESDA MD 20814			
17a CONTRACTOR/OFFEROR COMPUSEARCH SOFTWARE SYSTEMS 21251 RIDGETOP CIRCLE SUITE 100 DUI.LES VA 20166-6501		17b PAYMENT WILL BE MADE BY CPSC Accounts Payable Branch AMZ 160 P.O. Box 25710 Oklahoma City OK 73125		14 METHOD OF SOLICITATION RFQ IFB RFP			
17c CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER				18b SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED SEE ADDENDUM			
19 ITEM NO	20 SCHEDULE OF SUPPLIES/SERVICES			21 QUANTITY	22 UNIT	23 UNIT PRICE	24 AMOUNT
	DUNS Number: [REDACTED] Contracting Officer Representative (COR): Shawn Battle Sbattle@cpsc.gov 301-504-6952  The Contractor shall provide the following prism software license and maintenance services renewal in accordance with GSA contract# GS-35F-0585J and the attached terms and conditions. The attached "CPSC Security Agreement" is hereby incorporated (Use Reverse and/or Attach Additional Sheets as Necessary)						
25 ACCOUNTING AND APPROPRIATION DATA 0100A16DSE-2016-9995400000-EXIT002400-25710						26 TOTAL AWARD AMOUNT (For Govt Use Only) \$172,997.21	
27a SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4 FAR 52.212-3 AND 52.212-5 ARE ATTACHED				27b CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4 FAR 52.212-5 IS ATTACHED		28 CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 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 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/COR/CO OR 			
30b NAME AND TITLE OF SIGNER (Type or print) Lisha Lee, Contract Specialist				30c DATE SIGNED 9/20/16			
31a UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER) 				31c DATE SIGNED 9/22/16			
31b NAME OF CONTRACTING OFFICER (Type or print) Eddie Ahmad							

19 ITEM NO	20 SCHEDULE OF SUPPLIES/SERVICES	21 QUANTITY	22 UNIT	23 UNIT PRICE	24 AMOUNT
	into this delivery order.				
0001	Base Year: 9/27/2016 - 9/26/2017  User Specific Databases (Updates) Item# FY-06	1	EA	1,330.87	1,330.87
0002	PRISM Web (Base 10 seats) Item# WEBM-01	1	EA	85,393.39	85,393.39
0003	PRISM Non-Buyers Item# WEBM-03	90	EA	239.71	21,573.90
0004	FPDS-NG Item# RM-15	1	EA	18,773.59	18,773.59
0005	DBA Support (Gold Plan) Item# DB-01	1	EA	45,025.46	45,025.46
0006	Option Year 1: 9/27/2017 - 9/26/2018  User Specific Databases (Updates) Continued ...	1	EA	1,377.45	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	34 VOUCHER NUMBER	35 AMOUNT VERIFIED CORRECT FOR	36 PAYMENT		37 CHECK NUMBER
PARTIAL      FINAL			COMPLETE	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

NAME OF OFFEROR OR CONTRACTOR  
**COMPUSEARCH SOFTWARE SYSTEMS**

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Item# FY-06 Amount: \$1,377.45 (Option Line Item)				
0007	PRISM Web (Base 10 seats) Item# WEBM-01 Amount: \$88,382.16 (Option Line Item)	1	EA	88,382.16	0.00
0008	PRISM Non-Buyers Item# WEBM-03 Amount: \$22,329.00 (Option Line Item)	90	EA	248.10	0.00
0009	FPDS-NG Item# RM-15 Amount: \$19,430.67 (Option Line Item)	1	EA	19,430.67	0.00
0010	DBA Support (Gold Plan) Item# DB-01 Amount: \$46,601.35 (Option Line Item)	1	EA	46,601.35	0.00
0011	Option Year 2: 9/27/2018 - 9/26/2019  User Specific Databases (Updates) Item# FY-06 Amount: \$1,425.66 (Option Line Item)	1	EA	1,425.66	0.00
0012	PRISM Web (Base 10 seats) Item# WEBM-01 Amount: \$91,475.53 (Option Line Item)	1	EA	91,475.53	0.00
0013	PRISM Non-Buyers Item# WEBM-03 Amount: \$23,110.20 (Option Line Item)	90	EA	256.78	0.00
0014	FPDS-NG Item# RM-15 Amount: \$20,110.74 (Option Line Item)	1	EA	20,110.74	0.00

Continued ...

NAME OF OFFEROR OR CONTRACTOR  
COMPUSEARCH SOFTWARE SYSTEMS

ITEM NO (A)	SUPPLIES-SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0015	DBA Support (Gold Plan) Item# DB-01 Amount: \$48,232.40 (Option Line Item)	1	EA	48,232.40	0.00
0016	Option Year 3: 9/27/2019 - 9/26/2020  User Specific Databases (Updates) Item# FY-06 Amount: \$1,475.56 (Option Line Item)	1	EA	1,475.56	0.00
0017	PRISM Web (Base 10 seats) Item# WEBM-01 Amount: \$94,677.18 (Option Line Item)	1	EA	94,677.18	0.00
0018	PRISM Non-Buyers Item# WEBM-03 Amount: \$23,919.30 (Option Line Item)	30	EA	265.77	0.00
0019	FPDS-NG Item# RM-15 Amount: \$20,814.61 (Option Line Item)	1	EA	20,814.61	0.00
0020	DBA Support (Gold Plan) Item# DB-01 Amount: \$49,920.53 (Option Line Item)	1	EA	49,920.53	0.00
0021	Option Year 4: 9/27/2020 - 9/26/2021  User Specific Databases (Updates) Item# FY-06 Amount: \$1,527.20 (Option Line Item)	1	EA	1,527.20	0.00
0022	PRISM Web (Base 10 seats) Item# WEBM-01 Amount: \$97,990.88 (Option Line Item)	1	EA	97,990.88	0.00
0023	PRISM Non-Buyers Continued ...	30	EA	275.07	0.00

NAME OF OFFEROR OR CONTRACTOR  
**COMPUSEARCH SOFTWARE SYSTEMS**

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Item# WEBM-03 Amount: \$24,756.30 (Option Line Item)				
0024	FPDS-NG Item# RM-15 Amount: \$21,543.13 (Option Line Item)	1	EA	21,543.13	0.00
0025	DBA Support (Gold Plan) Item# DB-01 Amount: \$51,667.75 (Option Line Item)	1	FA	51,667.75	0.00
0026	Option Year 5: 9/27/2021 - 9/26/2022  User Specific Databases (Updates) Item# FY-06 Amount: \$1,580.66 (Option Line Item)	1	EA	1,580.66	0.00
0027	PRISM Web (Base 10 seats) Item# WEBM-01 Amount: \$101,420.56 (Option Line Item)	1	FA	101,420.56	0.00
0028	PRISM Non-Buyers Item# WEBM-03 Amount: \$25,623.00 (Option Line Item)	30	EA	284.70	0.00
0029	FPDS-NG Item# RM-15 Amount: \$22,297.14 (Option Line Item)	1	EA	22,297.14	0.00
0030	DBA Support (Gold Plan) Item# DB-01 Amount: \$53,476.12 (Option Line Item)	1	EA	53,476.12	0.00

The total amount of award: \$1,127,262.29. The obligation for this award is shown in box 26.

**LCIA CONTRACTOR'S NOTE**

**ATTENTION GOVERNMENT VENDOR**

**A. BILLING INSTRUCTIONS**

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

1. The name and address of the business concern (and separate remittance address, if applicable).
2. **Do NOT** include Taxpayer Identification Number (TIN) on invoices sent via e-mail.
3. Invoice date.
4. Invoice number.
5. The contract or purchase order number (see block 2 of OF347 and block 4 of SF1449 on page 1 of this order), or other authorization for delivery of goods or services.
6. Description, price and quantity of goods or services actually delivered or rendered.
7. Shipping cost terms (if applicable).
8. Payment terms.
9. Other substantiating documentation or information as specified in the contract or purchase order.
10. Name, title, phone number and mailing address of responsible official to be notified in the event of a deficient invoice.

**ORIGINAL VOUCHERS/INVOICES SHALL BE SENT TO:**

**PREFERRED: 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](mailto:9-AMC-AMZ-CPSC-Accounts-Payable@faa.gov).

**B. 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 [9-AMC-AMZ-CPSC-Accounts-Payable@faa.gov](mailto: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](mailto:AClark@cpsc.gov).

**C. INSPECTION & ACCEPTANCE PERIOD**

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

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

Contact: Greg Grayson Contract Specialist at [ggrayson@cpsc.gov](mailto:ggrayson@cpsc.gov) or (301) 504-7725

**E. PROCESSING INSTRUCTIONS FOR REQUESTING OFFICES**

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

**F. PROPERTY/EQUIPMENT PURCHASES**

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

(End of clause)

**LC 5 Contracting Officer's Representative (COR) Designation**

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

Name: Shawn Battle

Division: Office of Information Technology

Telephone: 301-504-6952

Email: [Sbattle@cpsc.gov](mailto:Sbattle@cpsc.gov)

b. The CPSC COR is responsible for:

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

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



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

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

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

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

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

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

(End of Clause)

#### **LC 22 Handling of Confidential Information**

a. If the Contractor obtains confidential business information about any company in connection with performance of this contract, either from the CPSC, the other company itself, or any other source, the Contractor agrees that it will hold the information in confidence and not disclose it either to anyone outside the CPSC or to any Contractor employee not involved in performance of this contract.

b. Failure by the contractor to comply with the terms of this clause may be treated as a default pursuant to the terms of this contract.

(End of clause)

#### **LC 29 In- and Out-Processing Requirements**

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

(End of Clause)

#### **LC 30 Security and Personal Identity Verification Procedures**

a. The performance of this contract requires contractor employees to have access to CPSC facilities and/or systems. In accordance with Homeland Security Presidential Directive-12 (HSPD-12), all such employees must comply with agency personal identity

verification (PIV) procedures. Contractor employees who do not already possess a current PIV Card acceptable to the agency shall be required to provide personal background information, undergo a background investigation (NACI or other OPM-required or approved investigation), including an FBI National Criminal History Fingerprint Check prior to being permitted access to any such facility or system. CPSC may accept PIV issued by another Federal Government agency but shall not be required to do so. No contractor employee will be permitted access to a CPSC facility or system without approval under the PIV process.

b. 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.

1. 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.

(End of Clause)

### **LC 31 Restrictions on Use of Information**

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

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

(End of Clause)

### **LC 32 Standards of Conduct**

1. Government contractors must conduct themselves with the highest degree of integrity and honesty. Contractors shall have standards of conduct and internal control systems that:

- a. Are suitable to the size of the company and the extent of their involvement in Government contracting,
- b. Promote such standards,
- c. Facilitate timely discovery and disclosure of improper conduct in connection with Government contracts, and
- d. Ensure corrective measures are promptly instituted and carried out.

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

The contractor shall provide, for all employees:

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

(End of Clause)

#### **LC 33 Contractor Personnel**

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

(End of Clause)

#### **52.217-8 Option to Extend Services.**

Option to Extend Services (Nov 1999)

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

(End of clause)

#### **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 15 days; provided that the Government gives the Contractor a

preliminary written notice of its intent to extend at least 30 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 five years.

(End of clause)

# Security Agreement

Between Compusearch Software Systems and the Consumer  
Product Safety Commission

August 2016

US Consumer Product Safety Commission



UNITED STATES OF AMERICA  
CONSUMER PRODUCT  
SAFETY COMMISSION

Compusearch Software Systems

US Consumer Product Safety Commission  
4330 East West Highway  
Bethesda, MD 20814

## OFFICIAL USE ONLY

### SECTION 1 – PURPOSE-DATA SECURITY REQUIREMENTS

The requirements of this data security agreement between Compusearch Software Systems, hereafter referred to as "Compusearch", and the US Consumer Product Safety Commission, hereafter referred to as CPSC, are for the express purpose of protecting confidential, privacy, proprietary, and sensitive data owned by or entrusted to CPSC. Access to CPSC systems, applications, and data by Compusearch employees are allowed solely for the purpose of providing PRISM software maintenance and support system services for CPSC under CPSC contract no. CPSC-F-16-0082.

### SECTION 2 – SECURITY CONSIDERATIONS

To the extent required to provide PRISM software maintenance and support system services in accordance with agency rules for the operation of the *PRISM database (PrismProdDB)*, Compusearch employees are allowed access to CPSC production systems—which may contain personally identifiable information (PII), proprietary, or other types of sensitive internal information. However, proper protection of this information is essential to the interests of CPSC. These interests include maintaining public confidence, trade secret protection, and preservation of personal privacy. As detailed in the requirements below, special care must be taken to prevent disclosure of any sensitive CPSC information.

All Compusearch employees who are granted access to CPSC networks, systems, applications, and/or data are expected to adhere to the following rules:

1. Contractor employees must comply with agency personal identity verification (PIV) requirements and use individual user accounts to access CPSC systems.
2. Access granted under CPSC contract no. CPSC-F-16-0082 is only for work associated with providing PRISM software maintenance and support system services. Performance of any unrelated and/or unauthorized actions will result in the immediate termination of system access.
3. Access will only be for the period stated in the contract. Thereafter, all accounts, passwords, and access associated with the contract will be revoked immediately.
4. To maintain account and password security, disclosure of any system account information or system passwords to any unauthorized third-party is prohibited.
5. Exhibiting or divulging the contents of any record or report to any person except in the execution of normal duties associated with this contract is prohibited.
6. Using any data accessed with any CPSC accounts associated with this contract for unauthorized purposes is prohibited.
7. No official record, report, database, or copy thereof, may be removed from CPSC premises or CPSC systems without prior written permission.
8. Contractor employees are prohibited from modifying, altering, or otherwise changing any CPSC system component or configuration not authorized for the maintenance and support of the PRISM system. Contractor employees are prohibited from issuing any system commands or running any software, scripts, or programs on the CPSC production network without prior authorization.

OFFICIAL USE ONLY



9. Contractor employees must hold confidential and/or personal privacy-related information in strict confidence and not disclose such information to any unauthorized third-party.
10. The Contractor must notify the CPSC COR immediately upon the termination of any contract employee so that account access, passwords, remote access, or other forms of access can be revoked.
11. The Contractor must notify the CPSC ISSO immediately upon the discovery—or suspected discovery—of any type of security incident or data breach affecting or that might potentially affect the CPSC network.

### SECTION 3 – ORGANIZATIONAL CONTACTS

Name	Title	E-mail	Phone
Patrick Manley	CISO	pmanley@cpsc.gov	301-504-7734
Bobby Sanderson	ISSO	bsanderson@cpsc.gov	301-504-7832
Shawn Battie	COR	SBattie@cpsc.gov	301-504-6952

Table 1, CPSC Contacts

Name	Title	E-mail	Phone
John Bria	Project Manager	johnb@compusearch.com	571-449-4059

Table 2, Compusearch Software Systems' Contacts

### SECTION 4 – DATA SENSITIVITY

PRISM users enter their requirements for supplies and services into the system from the desktop. Requests are then assigned to a contract specialist who solicits, negotiates, awards and administers the contracts. Awards include complex contracts such as indefinite quantity and labor hour contracts, purchase orders, delivery orders, and interagency and cooperative agreements.

The PRISM database (PrismProdDB) may contain financial, sensitive, confidential, and proprietary information.

The PRISM application is categorized at the "moderate" level.

Compusearch DBA will only be granted access to:

- o Production Database Host: PRISMPRODDB1
  - Production Database Names: PRISM and ADHOC
  - Production Web Server: PRISMPRODAPP
- o Test Database Host: NEWTEST
  - Test Database Names: TEST and ADHOC
  - Test Web Server: PRISMTESTAPP2

**SECTION 5 – INCIDENT REPORTING**

If sensitive information has been inappropriately disclosed, or is believed to have been inappropriately disclosed, the circumstances must be reported immediately to the CPSC ISSO. It is CPSC's responsibility to determine whether the disclosure or suspected disclosure must be reported to third parties such as US-CERT, law enforcement personnel, the public, and others.

**SECTION 6 – SECURITY POLICY AND PROCEDURES**

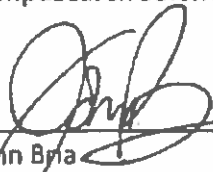
The security policies, standards, and guidelines are issued by the Executive and Legislative branches, and by federal departments and agencies. This agreement must comply with security policies and standards applicable to Compusearch and CPSC, including:

- CPSC Rules of Behavior (appendix A)
- Information Security Awareness online training

**SECTION 7 – AGREEMENT**

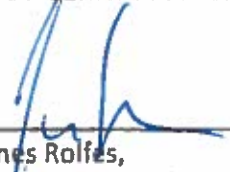
I have read, understand, and agree to comply with the policies, rules, and conditions governing access to the U.S. Consumer Product Safety Commission's computer systems, applications, and data. This security agreement will be reviewed at least every three (3) years to verify that the provisions of the agreement remain the same. This agreement may be terminated upon 30 days advanced notice by either party or in the event of a security exception that would necessitate an immediate response.

**Compusearch Software Systems**

  
\_\_\_\_\_  
John Bria  
Project Manager

9/20/16  
Date

**US Consumer Product Safety Commission**

  
\_\_\_\_\_  
James Rolfes,  
Authoring Official

9/21/2011  
Date

## Appendix A: Rules of Behavior

The *Consumer Product Safety Commission* (CPSC) makes available to its employees, consultants, and contractors access to one or more information systems—including individual computers, network file systems, e-mail, database systems, Intranet, and Internet access. All information system users should be aware that these services are solely for the purpose of facilitating and supporting CPSC business. All employees and authorized system users are responsible for using these resources in a professional, ethical, and lawful manner.

CPSC established the following *Rules of Behavior* to govern the use of its information system resources and privacy data (i.e., personally identifiable information (PII)). All CPSC employees and authorized system users must comply with these regulations or be subject to disciplinary action.

*Note: Personally Identifiable Information (PII) is any information in paper or electronic form: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., Indirect Identification. (These data elements may include a combination of gender, race, birth date, geographic indicator and other descriptors).*

### General Use

1. Executive Branch employees do not have a right to, nor should they have an expectation of privacy while using any Government office equipment, at any time, including accessing the internet or using electronic mail. To the extent that employees wish that their private activities remain private, they should avoid using any Agency office equipment, including computers, the Internet, or electronic mail –Directive 0720.1.
2. By using Government office equipment, Executive Branch employees imply their consent to disclosing the content of any files or information maintained or transmitted on government computer equipment.
3. By using CPSC office equipment, consent to monitoring and recording is implied with or without cause, including (but not limited to) accessing the internet or using electronic mail. Any use of government communications resources is made with the understanding that such use is generally not private and is not anonymous.
4. System managers do employ monitoring tools to detect improper use. Details of electronic communications may be disclosed to agency officials who have a “need to know” in the performance of their duties. Agency officials, such as system managers, may access any electronic communications.
5. CPSC reserves the right to audit computer and network usage on a periodic basis to ensure compliance with this policy.

### Security

1. System passwords should be kept secure and network accounts should not be shared. Users are responsible for the security of their passwords and accounts.

2. Users must exercise caution when opening attachments or clicking on links received in unsolicited email messages as such attachments or links may cause the user's computer to become infected with viruses, worms, or Trojan horse code.
3. The assigned user of an individual computer system is considered to be the *guardian* of the equipment and is expected to use reasonable safeguards to protect the equipment. If the equipment is damaged, lost, stolen, or is otherwise unavailable for normal business activities, the assigned user must immediately notify the *Property Custodian* for his/her department and the *Agency's Information Systems Security Officer (ISSO)*.
4. Any "sensitive" electronic information that is transmitted or otherwise transported outside of the CPSC network must be encrypted with a Government-standard encryption software tool.
5. Users must promptly report all information systems security violations, alerts, and vulnerabilities to the *CPSC Helpdesk*.

#### Computer/Network Use

1. Unauthorized duplication of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CPSC (or authorized user) does not have a license for is strictly prohibited – *Directives 0780.0, 0780.1 & 0820.5*.
2. Users may not install non-authorized software – *Directives 0780.0, 0780.1 & 0820.5*.
3. Users may not install non-authorized hardware – *Directive 0720.1*.
4. Users may not change computer operating system configurations, upgrade existing operating systems, or install new operating systems. If such changes are required, they must be requested through the CPSC Help Desk.
5. Users must use "Software/Hardware Installation Request Form" (available on *CPSCnet*) to request authorization for software/hardware installations. Requests must be approved prior to installation – *Directives 0780.0, 0780.1 & 1522.1*.
6. Users may only use CPSC computer equipment for government business and limited personal use as described in CPSC *Directive 0720.1*.
7. Deliberately introducing any type of malicious software into the CPSC network or computer systems (e.g., viruses, worms, Trojan horses, etc.) is strictly prohibited.
8. Revealing your CPSC computer account information to others or allowing use of your account or computer equipment by others, including family or household members, is strictly prohibited – *Directive 0720.1*.
9. Using a CPSC computer system or account to engage in viewing, procuring, or transmitting sexually explicit material is strictly prohibited.

10. Using a CPSC computer system or account to engage in any illegal or unethical activity is strictly prohibited.
11. Using a CPSC computer system or account to engage in any personal business enterprise is strictly prohibited.
12. Deliberately breaching CPSC system security defenses or otherwise attempting to circumvent established security procedures and practices is strictly prohibited.
13. CPSC-provided removable media (thumb drives, CDs, DVDs, etc.) should not be used in computers not owned by CPSC. Removable media not provided by CPSC (e.g., personally owned, visitor, contractor, vendor, etc.) should not be used in CPSC computers.
14. CPSC federal and contract staff may access CPSC data, using Personally Owned Devices (POE) through the CPSC Virtual Desktop Infrastructure (VDI). POE includes but is not limited to computers, tablets and smartphones.

#### Electronic Mail/Communications

1. The use of a CPSC electronic mail account for the creation or forwarding of mass advertising, chain, or other bulk mail messages of any type is strictly prohibited.
2. Any form of harassment using a CPSC electronic mail account, telephone, cell phone, or other telecommunications device, whether through language, frequency, or size of messages, is strictly prohibited.
3. The use of *Instant Messaging* or *Chat* programs (other than messaging software provided by EXIT) on a CPSC computer system is strictly prohibited.
4. File sharing between the CPSC network and any external network using Peer-to-Peer (P2P) software or network protocols such as FTP and Telnet is strictly prohibited.
5. Any electronic mail sent by a CPSC employee using a CPSC electronic mail account must contain a disclaimer stating that the opinions/information expressed are their own and not necessarily those of CPSC, unless required to do otherwise.
6. Employees create Federal records when they conduct agency business using personal electronic messaging accounts or devices. Personal electronic messaging accounts or devices should only be used in exceptional circumstances when official accounts are unavailable. The Federal Records Act (44 U.S.C. 2911 as amended by Pub. L. 113-187) states: (a) In General. – An officer or employee of an executive agency may not create or send a record using a non-official electronic messaging account unless such officer or employee – (1) copies an official electronic messaging account of the officer or employee in the original creation or transmission of the record; or (2) forwards a complete copy of the record to an official electronic messaging account of the officer or employee not later than 20 days after the original creation or transmission of the record.

#### Protecting Personally Identifiable Information (PII)

1. Access to PII should be limited to employees with a legitimate need to know.
2. Each employee is responsible for knowing what personal information is in his/her control (stored in paper or electronic files) and keeping only what is needed to perform work assignments.
3. The use of social security numbers must only be for official and lawful purposes.
4. Each employee is responsible for being familiar with agency Personally Identifiable Information Protection Policy (CPSC Directive 1435.1 and policy guidance) and office procedures for protecting the information.
5. PII, in electronic form, must only be stored on the CPSC network, a CPSC-issued laptop with access control and encryption technology, an encrypted thumb drive (CPSC provided) or authorized backup media (e.g., backup tapes).
6. Employees must store paper documents, files, and media containing PII in a locked room or in a locked file cabinet when not in use.
7. PII must not be accessed, processed, transmitted, or stored using a personally owned computer, PDA, phone, or other mobile device.
8. Each employee is responsible for properly disposing of information containing PII in accordance with office procedures and records schedules.
9. If PII is lost, stolen, or disclosed to unauthorized parties, or suspected of being lost, stolen or disclosed to unauthorized parties, its Owner and the Information Systems Security Officer must be notified immediately.

#### **Social Media**

1. Provisions for general use, security, computer/network use, electronic mail/communications, and protecting personally identifiable information (PII) all apply for authorized use of official agency social media accounts.
2. Employees should use caution when providing both personal and work-related information on social media sites.