

**ORDER FOR SUPPLIES OR SERVICES**

PAGE OF PAGES  
1 3

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER 05/13/2016		2. CONTRACT NO. (If any) CPSC-I-15-0012		6. SHIP TO: a. NAME OF CONSIGNEE CONSUMER PRODUCT SAFETY COMMISSION	
3. ORDER NO.		4. REQUISITION/REFERENCE NO. REQ-2400-15-0028		b. STREET ADDRESS OFFICE OF INFORMATION SERVICES 4330 EASTWEST HIGHWAY ROOM 706	
5. ISSUING OFFICE (Address correspondence to) CONSUMER PRODUCT SAFETY COMMISSION DIV OF PROCUREMENT SERVICES 4330 EAST WEST HWY ROOM 523 BETHESDA MD 20814				c. CITY BETHESDA	
				d. STATE MD	e. ZIP CODE 20814
7. TO: a. NAME OF CONTRACTOR DEPARTMENT OF HOMELAND SECURITY				f. SHIP VIA	
b. COMPANY NAME				8. TYPE OF ORDER	
c. STREET ADDRESS NATIONAL PROTECTION AND PROGRAMS 245 MURRAY LN SW STOP 410				<input checked="" type="checkbox"/> a. PURCHASE REFERENCE YOUR:  Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.	
d. CITY WASHINGTON		e. STATE DC	f. ZIP CODE 20528-0410		
9. ACCOUNTING AND APPROPRIATION DATA				10. REQUISITIONING OFFICE CONSUMER PRODUCT SAFETY COMMISSION	

11. BUSINESS CLASSIFICATION (Check appropriate box(es))					12. F.O.B. POINT
<input type="checkbox"/> a. SMALL	<input type="checkbox"/> b. OTHER THAN SMALL	<input type="checkbox"/> c. DISADVANTAGED	<input type="checkbox"/> d. WOMEN-OWNED	<input type="checkbox"/> e. HUBZone	Destination
<input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED	<input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM	<input type="checkbox"/> h. EDWOSB			
13. PLACE OF		14. GOVERNMENT B/L NO.		15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date) 10 Days After Award	16. DISCOUNT TERMS Net 30
a. INSPECTION	b. ACCEPTANCE				

**17. SCHEDULE (See reverse for Rejections)**

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	DUNS Number: 965566644 COR: Albert Anders PHONE: (301) 504-7663 EMAIL: aanders@cpsc.gov  THE CONTRACTOR SHALL PERFORM THE FOLLOWING Continued ...					

18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		17(h) TOTAL (Cont. pages)
21. MAIL INVOICE TO:						
SEE BILLING INSTRUCTIONS ON REVERSE	a. NAME CPSC Accounts Payable Branch				\$0.00	17(i) GRAND TOTAL
	b. STREET ADDRESS (or P.O. Box) AMZ 160 P.O. Box 25710				\$0.00	
	c. CITY Oklahoma City	d. STATE OK	e. ZIP CODE 73125			

22. UNITED STATES OF AMERICA BY (Signature)

23. NAME (Typed)   
TITLE: CONTRACTING/ORDERING OFFICER

**ORDER FOR SUPPLIES OR SERVICES  
SCHEDULE - CONTINUATION**

PAGE NO

2

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER  
05/13/2016

CONTRACT NO.  
CPSC-I-15-0012

ORDER NO.

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
0001	<p>SERVICES FOR THE CONSUMER PRODUCT SAFETY COMMISSION IN ACCORDANCE WITH THE ATTACHED TERMS AND CONDITIONS:</p> <p>Accounting Info: 0100A15DSE-2015-5457500000-EXIT002400-251A0 Period of Performance: 05/13/2016 to 05/12/2017</p> <p>This is to establish a Memorandum of Agreement between The Department of Homeland Security, Office of Cybersecurity and Communications and Consumer Products Safety Commission Relating to the Deployment of EINSTEIN Cybersecurity Capabilities</p> <p>Purpose. CPSC, in furthering its responsibility to provide information security protections for its Internet facing or connected information and information systems, requests that CS&amp;C deploy and operate EINSTEIN cybersecurity capabilities on CPSC information systems to look for network traffic indicating known or suspected malicious cyber activity. CS&amp;C is deploying these EINSTEIN capabilities to CPSC information systems in furtherance of the DHS responsibilities to protect, defend, and reduce vulnerabilities of Federal Systems; compile and analyze information about incidents threatening Federal information security; and inform operators of agency information systems about current and potential information security threats. This Agreement establishes the responsibilities of CPSC and CS&amp;C in connection with the deployment and operation of EINSTEIN capabilities.</p> <p>See attached MOA - at this time no funds are associated with this agreement</p> <p>The total amount of award: \$0.00. The Continued ...</p>	1	LO	0.00	0.00	
TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))					\$0.00	

**ORDER FOR SUPPLIES OR SERVICES  
SCHEDULE - CONTINUATION**

PAGE NO

3

**IMPORTANT:** Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER  
05/13/2016

CONTRACT NO.  
CPSC-I-15-0012

ORDER NO.

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	obligation for this award is shown in box 17(i).					
TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))					\$0.00	

UNCLASSIFIED // FOR OFFICIAL USE ONLY

---

**Memorandum of Agreement**

between

**The Department of Homeland Security,  
Office of Cybersecurity and Communications**

and

**U.S. Consumer Product Safety Commission**

**Relating to the Deployment of EINSTEIN Cybersecurity Capabilities**

- I. **Parties.** This Memorandum of Agreement (Agreement) is entered into between the U.S. Consumer Product Safety Commission (hereinafter CPSC) and the Department of Homeland Security (DHS), Office of Cybersecurity and Communications (CS&C), collectively, "the Parties."
- II. **Authority.** This Agreement is concluded pursuant to authorities applicable to the Parties, including the Homeland Security Act of 2002 (6 U.S.C. §§ 101 et seq., esp. § 230 of the Homeland Security Act); the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §§ 3551-3558); Presidential Policy Directive-21; National Security Presidential Directive-54/Homeland Security Presidential Directive-23; and the Federal Cybersecurity Enhancement Act of 2015 (Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Division N, section 221-229, esp. 223.); and the Consumer Product Safety Act, 15 U.S.C. § 2051 *et. seq.*
- III. **Preexisting Agreements.** This Agreement supersedes previous agreements between the Parties related to the deployment of EINSTEIN capabilities.
- IV. **Scope.** This Agreement covers the EINSTEIN intrusion prevention security services as well as all previously deployed EINSTEIN capabilities (i.e., EINSTEIN 1 and EINSTEIN 2). Any future capabilities will be addressed in a mutually agreed upon modification to this Agreement or new agreement.
- V. **Purpose.** This Agreement establishes the responsibilities of CPSC and CS&C in connection with the deployment and operation of EINSTEIN capabilities, which CS&C will deploy and operate on CPSC information systems to look for network traffic indicating known or suspected malicious cyber activity.
- VI. **Background.**
  - A. The EINSTEIN capabilities are part of the DHS National Cybersecurity Protection System (NCPS), which is controlled and operated by CS&C and its U.S. Computer

Emergency Readiness Team (US-CERT) to protect information and information systems from cybersecurity risks. Deployment of the EINSTEIN capabilities to agency information systems<sup>1</sup> enhances the ability of participating agencies to provide effective information security protection for their information and information systems. It also provides US-CERT with the ability to carry out DHS cybersecurity responsibilities under applicable authorities and Executive Branch direction in support of the following core cybersecurity mission areas:

- Protection – protecting participating agency information and information systems through the detection and prevention of intrusions and the mitigation of known or suspected cybersecurity threats;
  - Victim Identification – identifying compromised agency information systems, system components, or host computers to permit participating agencies to locate compromised hosts, components, and systems and respond to cyber incidents;
  - Situational Awareness – developing and maintaining overall situational awareness regarding the cybersecurity status of agency information systems; and
  - Discovery – identifying and analyzing new or emerging cybersecurity threats targeting agency information systems to enhance these protection, victim identification, and situational awareness missions.
- B. The DHS cybersecurity mission is furthered through the deployment of three EINSTEIN capabilities: the collection and analysis of connection summary, commonly called “net flow”, data; signature-based intrusion detection; and intrusion prevention and real-time threat mitigation with enhanced net flow and intrusion detection. These complementary capabilities provide a more complete view of an agency’s information system as well as the ability for US-CERT to obtain consolidated cybersecurity situational awareness across all agency information systems.
- C. EINSTEIN capabilities are provided through a combination of commercial off-the-shelf hardware and software, government developed software, and commercially available managed security services enhanced by DHS-provided information. All system and service components are deployed in appropriately secured DHS-operated and/or approved government or contractor facilities. EINSTEIN functional capabilities are under the operational control of US-CERT and are operated by US-CERT personnel or by government contractor personnel in accordance with the DHS cybersecurity mission.

---

<sup>1</sup> The terms “agency” and “agency information system” are defined in section 230 of the Homeland Security Act of 2002, as added by the Federal Cybersecurity Enhancement Act of 2015. To define the term “agency,” section 230 of the Homeland Security Act refers to the definition of “agency” in 44 U.S.C. § 3502. The scope of agency information systems covered under this Memorandum of Agreement includes the information systems of any agency as defined in 44 U.S.C. § 3502, but does not include information systems of the Department of Defense, national security systems as defined in 40 U.S.C. § 11103, or information systems of an element of the intelligence community.

- D. EINSTEIN capabilities are deployed at Office of Management and Budget (OMB)-approved Agency Trusted Internet Connection Access Providers (TICAPs), Managed Trusted Internet Protocol Service (MTIPS) enclaves servicing General Services Administration (GSA) Network customers, and Internet service provider (ISP) intrusion prevention system enclaves.
- VII. Responsibilities. As part of CPSC's request to receive EINSTEIN capabilities from CS&C and CS&C's agreement to provide those capabilities to CPSC, the Parties agree on the following responsibilities.
- A. Agency Responsibilities.
    - 1. General Responsibilities.
      - a. Designate a technical point of contact to coordinate with CS&C on matters involving implementation of EINSTEIN capabilities;
      - b. Designate an operational point of contact who will facilitate information sharing related to operational cybersecurity incidents impacting CPSC's network, who must hold an active TOP SECRET/SCI security clearance if agency desires access to classified information about such incidents;
      - c. Designate a legal point of contact to coordinate with CS&C on matters involving legal or policy changes related to EINSTEIN and the releasing of any information related to EINSTEIN to the public or in connection with any other requests, inquiries, court proceedings or other legal process.
      - d. Work through the CPSC technical point of contact to identify an authorized individual who will provide feedback to CS&C during test events for EINSTEIN capabilities and, as necessary, actively participate in test events;
      - e. If requesting additional analytic or troubleshooting support, provide CS&C with any available and appropriate CPSC network map of internal systems and network topology diagrams to aid analysis, troubleshooting, and incident response by US-CERT and notify, in writing, the CS&C technical point of contact within 30 days of when the network topology is modified;
      - f. Enter into a Service Level Agreement (SLA) with US-CERT to further define information exchange, services and deliverables in connection with EINSTEIN operations.
      - g. Notify the CS&C technical point of contact of any circumstances that would impact the operations of the EINSTEIN equipment, including any planned or proposed network modifications affecting EINSTEIN equipment functionality;

- h. Manage and maintain all contractual relationships with CPSC ISPs and any other service providers regarding the delivery of CPSC traffic;
- i. Notify the CS&C technical point of contact in writing of any changes to CPSC Internet services that could potentially impact EINSTEIN operations, including provisioned Internet service bandwidth, addition or deletion to the IP addresses previously provided to CS&C that are assigned to or otherwise associated with CPSC traffic for Internet service, or changes in ISPs or service level agreements;
- j. Within 30 days of when DHS notifies that its intrusion prevention security services ISP is prepared to provide services, and if requested by CS&C or its intrusion prevention security services ISP, authorize, through a Letter of Agency similar to the model in Appendix D, participating intrusion prevention security services ISPs to fully cooperate with DHS in deploying EINSTEIN capabilities on CPSC's networks, to reroute, modify, and/or reconfigure any of CPSC's Internet traffic handled by such ISPs, in accordance with the requirements of this Agreement, and to disclose to US-CERT CPSC network traffic and any information relating to CPSC's networks that is necessary to accomplish the EINSTEIN deployment described in this Agreement;
- k. Provide CS&C with a complete and accurate list of Internet Protocol (IP) addresses associated with CPSC traffic assigned by each participating intrusion prevention security services ISP and inform the CS&C technical point of contact in writing of any planned changes to that IP address list at least 30 days prior to implementation of the change by the ISP;
- l. Ensure that the IP addresses provided to CS&C under section VII.A.1.k are associated exclusively with federal government traffic, and do not contain any IP addresses associated with non-federal traffic;
- m. Modify or otherwise conform existing or future contracts, service level agreements, or other relationships with participating intrusion prevention security services ISPs, as necessary, to enable the in-line delivery of intrusion prevention security services capabilities as part of the delivery of CPSC traffic, modify Service Level Agreements as necessary to account for the operation of EINSTEIN equipment, and enable the Parties to carry out their responsibilities under this Agreement;
- n. Share with US-CERT all summary and statistical information and analysis developed by CPSC using EINSTEIN data provided to CPSC by CS&C;
- o. Coordinate, as appropriate, with Federal entities that have law enforcement and other cybersecurity responsibilities related to any cyber incidents detected through EINSTEIN operations;

- p. Revise, as necessary, any applicable CPSC external website privacy policies to include notice of the deployment of the EINSTEIN capabilities (model language that may be appropriate for such agency website privacy policies is provided in Appendix C);
  - q. Notify the CS&C technical and/or legal point of contact of any legal or policy changes affecting the ability to lawfully implement the EINSTEIN capabilities on CPSC's networks;
  - r. Serve as the "agency of record" for any CPSC information collected by CS&C through EINSTEIN operations, and respond to any requests for CPSC information received in accordance with the Freedom of Information Act (FOIA); congressional, Government Accountability Office, or Inspector General inquiries; court proceedings; or other legal process; and
  - s. Coordinate with the CS&C technical and legal points of contact pursuant to section VII.B.17 before releasing any technical, engineering, or operational information related to EINSTEIN equipment, capabilities, and operations to the public or in connection with any requests received in accordance with the FOIA; congressional, Government Accountability Office, or Inspector General inquiries; court proceedings; or other legal process.
  - t. In accordance with section 223 of the Federal Cybersecurity Enhancement Act of 2015, no later than December 18, 2016, apply and continue to utilize initial EINSTEIN capabilities made available by CS&C to all information traveling between an information system owned or operated by CPSC and any information system other than an information system owned or operated by CPSC. Apply and continue to utilize any new intrusion detection and prevention capabilities or improvements to existing capabilities to all information traveling between an information system owned or operated by CPSC and any information system other than an information system owned or operated by CPSC, no later than six (6) months after the date on which CS&C makes available the new capabilities or improvements.
2. Additional Responsibilities for OMB Approved TICAPs.
- a. Provide a secured location for the installation and maintenance of any EINSTEIN equipment to be installed at the agency TICAP or other agency location;
  - b. Ensure continued availability of any EINSTEIN equipment installed at the agency TICAP or other agency location;
  - c. Ensure that the EINSTEIN equipment installed at the agency TICAP or other agency location is used for EINSTEIN operations only;

- d. Provide authorized CS&C personnel escorted access to CPSC Internet Access Provider once coordinated through CPSC TICAP and provide logistic support in the form of rack space, electricity, Internet connectivity, and any infrastructure support necessary to support communication and remote administration between CS&C and the EINSTEIN equipment; and
  - e. Work through the CPSC technical point of contact to aid CS&C system administrators in managing the EINSTEIN equipment, oversee the maintenance performed by CS&C, and aid in these tasks when remote capability is not possible.
3. Additional Responsibilities for MTIPS Enclave Users.
- a. Ensure, in conjunction with Networkx MTIPS vendor, that the CPSC traffic is routed through the TIC portal; and
  - b. Ensure the CS&C technical point of contact is notified of all changes in CPSC security policy related to the MTIPS connections that would change the characterization of network traffic.
- B. Responsibilities of CS&C.
- 1. Provide at no cost to CPSC the CS&C labor, hardware, and software necessary to deploy and operate EINSTEIN equipment at CPSC TICAPs, MTIPS enclaves, and participating intrusion prevention security services ISP locations;
  - 2. Designate appropriate legal, technical, and operational points of contact to coordinate with CPSC on issues related to EINSTEIN equipment, capabilities, or operations;
  - 3. Host collaborative events to bring together representatives of the various agencies protected by EINSTEIN capabilities;
  - 4. Provide guidance and support on the deployment and implementation of EINSTEIN equipment and operations;
  - 5. Provide technical assistance as necessary if CPSC is not otherwise able to provide network topology information in accordance with section VII.A.1.e;
  - 6. Install EINSTEIN equipment at applicable CPSC TICAPs, MTIPS enclaves, and participating intrusion prevention security services ISP locations in accordance with both FISMA and National Institute of Standards and Technology standards and guidelines;

7. Provide, as needed and requested by CPSC, an authorization memorandum, test reports, and other procedures or information related to certification and accreditation or other applicable security policies;
8. Perform ongoing system administration, patching, testing, and configuration management of the EINSTEIN equipment;
9. Maintain and operate EINSTEIN equipment in accordance with all applicable CS&C procedures;
10. Protect through appropriate means any CPSC Customer Proprietary Network Information (CPNI), including agency bandwidth, Internet Protocol (IP) address blocks, and service access locations that are provided to CS&C in accordance with section VII.A.1.j and VII.A.1.k;
11. Encrypt all data communications from EINSTEIN equipment at TICAP or MTIPS locations to CS&C;
12. Conduct EINSTEIN operations, including information sharing and support for appropriate cybersecurity responsibilities of other Federal entities, as authorized by law and in a manner that protects the privacy and other legal rights of persons. In accordance with section 230(c) of the Homeland Security Act as added by the Federal Cybersecurity Enhancement Act of 2015, retain, use and disclose CPSC information obtained in connection with this Agreement only to protect information and information systems from cybersecurity risks, and ensure that EINSTEIN operations are reasonably necessary for the purpose of protecting agency information and agency information systems from cybersecurity risks;
13. Provide relevant training to CPSC authorized personnel, including training to enable the analysis of CPSC net flow data collected through EINSTEIN operations and made available to CPSC by CS&C;
14. Maintain and provide to CPSC and other participating agencies a collection of summary and statistical reports based on EINSTEIN data on which CS&C will perform timely cross-agency analysis of cybersecurity threats, cyber incidents, and identified network anomalies;
15. Serve as the "agency of record" for information related to EINSTEIN equipment, capabilities, and operations and respond to any requests for such information received in accordance with the FOIA; congressional, Government Accountability Office, or Inspector General inquiries; court proceedings; or other legal process;
16. Coordinate with the CPSC technical and legal points of contact pursuant to section VII.A.1.s before releasing any CPSC information collected by US-

CERT through EINSTEIN operations in connection with any requests received in accordance with the FOIA; congressional, Government Accountability Office, or Inspector General inquiries; court proceedings; or other legal process;

17. As requested, share ISP thresholds levels specified for the service for performance requirements with the agencies.

VIII. Authorization for In-line Traffic Inspection and Modification. CPSC recognizes that certain EINSTEIN operations will include a range of capabilities designed to prevent specific cyber intrusions into CPSC information systems and mitigate specific cyber threats to CPSC information and information systems. Such activity which may include the interception, potential modification, use, and disclosure of CPSC traffic, as well as sending commands to CPSC information systems for the purpose of identifying such systems, is authorized by CPSC in order to protect CPSC information and information systems and provide real-time mitigation of specific cyber threats, in accordance with this Agreement.

IX. Government contractors. CPSC recognizes that certain EINSTEIN operations will be undertaken by entities acting under contract to DHS. Such contractors, which will include Internet services providers, will conduct their activities in accordance with DHS requirements, which DHS shall ensure are consistent with the terms of this Agreement.

X. Certification. CPSC certifies that its log-on consent banners or notices, terms-of-use policies or user agreements, computer training programs, and any other mechanisms used to notify users and obtain their consent to the terms and conditions of computer use clearly demonstrate to CPSC computer users and obtain their consent that:

- users have no expectation of privacy regarding any communications or information transiting, stored on, or traveling to or from CPSC information systems;
- the Government routinely monitors communications occurring on CPSC information systems for any lawful government purpose including, but not limited to, monitoring network operations, quality control, employee misconduct investigations, law enforcement investigations, and counterintelligence investigations;
- at any time, the Government may for any lawful government purpose monitor, intercept, search, and seize communications or information transiting, stored on, or traveling to or from CPSC information systems;
- any communications or information transiting, stored on, or traveling to or from CPSC information systems may be disclosed or used for any lawful government purpose; and
- CPSC information systems include computers, computer networks, and all devices and storage media attached to a(n) CPSC network or to a computer on such network.

For purposes of the certification, CPSC shall ensure that references to monitoring by the Government are sufficient to address activities undertaken by the Government's contractors, including activities undertaken in accordance with Section IX.

CPSC will notify CS&C promptly of any changes to its log-on consent banners or notices, terms-of-use policies or user agreements, computer training programs, and any other mechanisms used to notify users and obtain their consent to the terms and conditions of

computer use that affect the above certification. Model language for the log-on consent banner and user agreement that agencies may wish to use to meet the requirements of the above certification is attached as Appendices A and B to this Agreement.

XI. Points of Contact. Liaison will be maintained between the following offices:

A. Technical Matters

Name:	Denis Suski	Danny Toler
Office:	Network Engineering Branch	DHS, CS&C
Position:	Branch Chief	Director, Network Security Deployment and NCPS Program Manager
Phone:	(301) 504-6724	(703) 235-3984
Email:	dsuski@cpsec.gov	danny.toler@hq.dhs.gov

B. Operational Matters

Name:	Bobby Sanderson	US-CERT
Office:	IT Security	DHS, CS&C
Position:	ISSO	US-CERT SWO
Phone:	(301) 504-7832	(888) 282-0870
Email:	bsanderson@cpsec.gov	swo@us-cert.gov

C. Legal Matters

Name:	Mary Boyle	Office of General Counsel
Office:	Office of the General Counsel	DHS, Office of General Counsel
Position:	Acting General Counsel	National Protection and Programs Directorate Law Division
Phone:	(301) 504-7859	(703) 235-5222 or (703) 235-5223
Email:	mboyle@cpsec.gov	ogc-cyber@hq.dhs.gov

XII. Other Provisions. Nothing in this Agreement is intended to conflict with current law. If a term of this Agreement is inconsistent with any applicable law, then that term shall be invalid, but the remaining terms and conditions of this Agreement shall remain in full force and effect.

XIII. Effective Date. This Agreement is effective on the date of the final signature.

XIV. Modification. The Parties may modify this Agreement by written agreement, signed by authorized representatives of both Parties.

XV. Termination. If it becomes necessary to terminate this Agreement, the terminating Party shall notify the technical points of contact in writing at least 30 calendar days prior to the intended date of termination. CPSC and CS&C shall cooperate to reach a mutually agreeable termination date.

XVI. **Costs.** This Agreement does not obligate any funds. Each party shall remain responsible for its own costs to perform its responsibilities under this Agreement.

XVII. **Dispute Resolution.** The Parties will make their best efforts to amicably resolve disputes that may arise under this Agreement through discussions. If resolution cannot be reached, the Parties will solicit the views and mediation of the above referenced technical points of contact. If those views or mediation cannot be obtained, or fail to resolve the matter, the issue will be elevated through the respective signatories to this Agreement for resolution.

Approved By:

U.S. Consumer Product Safety Commission

Department of Homeland Security

JAMES  
ROLFES

Digitally signed by JAMES ROLFES  
DN: c=US, o=U.S. Government,  
ou=Consumer Product Safety  
Commission, cn=JAMES ROLFES,  
0.9.2342.19200300.100.1.1-610010011163  
#2  
Date: 2016.05.03 13:14:41 -0400



James Rolfes  
Chief Information Officer  
U.S. Consumer Product Safety Commission  
Date \_\_\_\_\_

Andy Ozment  
Assistant Secretary  
Office of Cybersecurity & Communications  
Date 5/13/16

APPENDIX A

MODEL LANGUAGE FOR  
LOG-ON BANNERS  
FOR COMPUTERS

- You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
  - You have no reasonable expectation of privacy regarding any communications or information transiting, stored on, or traveling to or from this information system. At any time, the government may for any lawful government purpose monitor, intercept, search, and seize any communication or information transiting, stored on, or traveling to or from this information system.
  - Any communications or information transiting, stored on, or traveling to or from this information system may be disclosed or used for any lawful government purpose.

[click button: "I AGREE"]

NOTE: For purposes of such banners, agencies shall ensure that references to monitoring by the government are sufficient to address activities undertaken by government contractors.

APPENDIX B

MODEL LANGUAGE FOR  
USER AGREEMENT

By signing this document, you understand and consent to the following when you access this agency's information systems, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices (e.g., BlackBerry, PDA, etc.) and storage media (e.g., thumb drive, flash drive, etc.) attached to this network or to a computer on this network:

- You are accessing a U.S. Government information system that is provided for U.S. Government-authorized use only;
- Unauthorized or improper use of the information system may result in disciplinary action, as well as civil and criminal penalties;
- The Government, acting directly or through its contractors, routinely monitors communications occurring on this information system. You have no reasonable expectation of privacy regarding any communications or data transiting, stored on, or traveling to or from this information system. At any time, the government may for any lawful government purpose monitor, intercept, search, and seize any communication or data transiting, stored, or traveling to or from this information system;
- Any communications or data transiting, stored on, or traveling to or from this information system may be disclosed or used for any lawful government purpose.

*I understand and consent.*

<<SIGNATURE BLOCK TO BE INSERTED LATER>>

APPENDIX C

MODEL LANGUAGE FOR  
PRIVACY POLICY

<<AGENCY NAME>> information systems may be protected by EINSTEIN cybersecurity capabilities, under the operational control of the U.S. Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT). Electronic communications with <<AGENCY NAME>> may be scanned by government-owned or contractor equipment to look for network traffic indicating known or suspected malicious cyber activity, including malicious content or communications. Electronic communications within <<AGENCY NAME>> will be collected or retained by US-CERT only if they are associated with known or suspected cyber threats. US-CERT will use the information collected through EINSTEIN to analyze the known or suspected cyber threat and help <<AGENCY NAME>> and other agencies respond and better protect their computers and networks.

For additional information about EINSTEIN capabilities, please see the EINSTEIN program-related Privacy Impact Assessments available on the DHS cybersecurity privacy website ([http://www.dhs.gov/files/publications/editorial\\_0514.shtm#4](http://www.dhs.gov/files/publications/editorial_0514.shtm#4)) along with other information about the federal government's cybersecurity activities.

Eddie Ahmad  
Contracting Officer  
Division of Procurement Services



Tel: 301-504-7884  
Fax: 301-504-0628  
Email: knutes@cpsc.gov

U.S. CONSUMER PRODUCT SAFETY COMMISSION  
BETHESDA, MD 20814

LETTER OF AGENCY

DATE: 28 April 2016

TO: Verizon Business

To Whom It May Concern,

Please be advised that, pursuant to a Memorandum of Agreement with the Department of Homeland Security (DHS) dated 5/13/2016 (attached as Exhibit 1) (MOA), the U.S. Consumer Product Safety Commission (hereinafter "CPSC") is participating in the deployment of EINSTEIN Intrusion Prevention Security Services (IPSS) on its networks for network security purposes, to look for network traffic indicating known or suspected malicious cyber activity. CPSC hereby authorizes and requests that Verizon Business (hereinafter "Verizon") fully cooperate with DHS in deploying EINSTEIN capabilities on CPSC's networks. CPSC authorizes Verizon to reroute, modify, and/or reconfigure any of CPSC's Internet traffic handled by Verizon, in accordance with the requirements of the MOA. Such Verizon operations on CPSC network traffic are consistent with CPSC login banners and computer use policies and procedures.

CPSC understands that deployment of the IPSS capabilities on its network (1) may impact services provided by Verizon, and (2) may require CPSC to modify service level agreements (SLA) that relate to such services occurring after CPSC Internet traffic routes through the EINSTEIN IPSS infrastructure so that no penalties or obligations accrue against the ISP for service impacts that result from application of the EINSTEIN IPSS to CPSC's traffic. CPSC agrees to negotiate with Verizon to evaluate and modify, as necessary, SLAs and other applicable provisions of the Network or any other contractual vehicles through which Verizon provides Internet services to CPSC in light of the deployment of EINSTEIN capabilities. CPSC understands that until such time as Verizon notifies DHS that such modifications have been made, as necessary, to the applicable contracts, DHS will not deploy EINSTEIN IPSS on CPSC's networks. CPSC understands that applicable EINSTEIN service levels will be governed by a separate Service Level Agreement between DHS and Verizon.

CPSC also authorizes Verizon to disclose CPSC network traffic to the Office of Cybersecurity and Communications (CS&C) within DHS, and to disclose to CS&C any information relating to CPSC's networks that is necessary to accomplish the EINSTEIN deployment described in the MOA. CPSC recognizes that the information to be disclosed may include Customer Proprietary Network Information (CPNI) or other categories of information the disclosure of which requires customer consent. The undersigned is fully authorized to deliver such consent on behalf of CPSC and hereby does so.

Page 2

CPSC asks that Verizon give full cooperation and compliance to all requests in the specified matters from DHS. This letter shall complement all letters of agency prior to the above date and shall remain in effect until it is specifically cancelled in writing by CPSC, with a 30 day wind-down period to cease operations.

Sincerely,

A handwritten signature in black ink, appearing to read "J. Rolfes", with a long horizontal flourish extending to the right.

James C. Rolfes, Chief Information Officer

Cc: Danny Toler  
Director, Network Security Deployment and NCPS Program Manager  
Office of Cybersecurity and Communications  
Department of Homeland Security