ORDER FOR SUPPLIES OR SERVICES

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

PAGE 1 OF PAGES 6

1 DATE OF ORDER: 06/19/2009

2 CONTRACT NO (If any): HSHQDC-06-D-00024

3 ORDER NO: HSHQDC-09-J-00153

4 REQUISITION/REFERENCE NO: RNCS-09-00080

5 ISSUING OFFICE (Address correspondence to):
U.S. Dept. of Homeland Security
Office of Procurement Operations
PHA Acquisition Division
245 Murray Lane, SW
Building 410
Washington DC 20528

6 SHIP TO

a NAME OF CONSIGNEE: Department of Homeland Security

b STREET ADDRESS: 245 Murray Lane
Bldg. 410

c CITY: Washington

d STATE: DC

e ZIP CODE: 20528

f SHIP VIA:

7 TO

a NAME OF CONTRACTOR: GENERAL DYNAMICS ONE SOURCE LLC

b COMPANY NAME:

c STREET ADDRESS: 3211 JERMANTOWN ROAD

d CITY: FAIRFAX

e STATE: VA

f ZIP CODE: 22030

8 TYPE OF ORDER

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

X b DELIVERY

Except for billing instructions on the reverse this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract

9 ACCOUNTING AND APPROPRIATION DATA: See Schedule

10 REQUISITIONING OFFICE: Department of Homeland Security

11 BUSINESS CLASSIFICATION (Check appropriate box(es))

a SMALL
X b OTHER THAN SMALL
c DISADVANTAGED
g SERVICE-DISABLED VETERAN-OWNED
d WOMEN-OWNED
e HUBZone
f EMERGING SMALL BUSINESS

12 F.O.B. POINT: Destination

13 PLACE OF

a INSPECTION: Destination

b ACCEPTANCE: Destination

14 GOVERNMENT B/L NO:

15 DELIVER TO F.O.B. POINT ON OR BEFORE (Date): 30 Days After Award

16 DISCOUNT TERMS: Net 30

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: 610320215+0000 The purpose of this Task Order is to provide integration and support services to the National Cyber Security Division (NCSD) United States-Computer Emergency Readiness Team (US-CERT). Continued ...					

18. SHIPPING POINT:

19. GROSS SHIPPING WEIGHT:

20. INVOICE NO:

17(h) TOTAL (Cont pages): $44,953,177.00

21. MAIL INVOICE TO

SEE BILLING INSTRUCTIONS ON REVERSE

a NAME: - Business Office (Invoice Proc.)

b STREET ADDRESS (or P.O. Box): U.S. Dept. of Homeland Security
Bldg. 410
245 Murray Drive, SW

c CITY: Washingt

d STATE: [redacted]

e ZIP CODE: 20528

17(i) GRAND TOTAL: $44,953,177.00

22. UNITED STATES OF AMERICA BY (Signature): [redacted] (b)(6)

23. NAME (Typed): David Ritter

TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (Rev. 4/2008)
Prescribed by GSA/FAR 48 CFR 53.213(e)

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

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

DATE OF ORDER: 06/19/2009
CONTRACT NO: HSHQDC-06-D-00024
ORDER NO: HSHQDC-09-J-00153

ITEM NO (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Admin Office: U.S. Dept. of Homeland Security Office of Procurement Operations PHA Acquisition Division 245 Murray Lane, SW Building 410 Washington DC 20528 Mark For: Department of Homeland Security Office of Procurement Operations 245 Murray Lane Bldg. 410 Washington DC 20528 Period of Performance: 06/20/2009 to 05/19/2010					
0001	24 x 7 Incident Handling Team Support IAW SOW: Tasks 6.2, 6.2.1, 6.2.2, 6.2.3, 6.2.4, 6.2.5, 6.2.6, 6.2.7, 6.2.8, 6.2.9, 6.2.10,6.2.11, 6.2.12, and 6.2.13 (This CLIN covers all reference tasks) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Accounting Info: CS00000-000-K8-40-70-01-001-01-08-0100 -00-00-00-00-GE-OE-2576-CS9080 Funded: [redacted] (b)(4) Accounting Info: CS00000-000-K9-04-01-01-004-90-05-0002 -07-02-00-00-GE-OE-2576-CS9080 Funded [redacted] (b)(4)				[redacted] (b)(4)	
0002	Malicious Code Support IAW SOW: Tasks 6.3, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, and 6.3.7 (This CLIN covers all reference tasks) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Accounting Info: CS00000-000-K9-04-01-01-004-90-05-0002 -07-02-00-00-GE-OE-2576-CS9080 Funded: [redacted] (b)(4) Continued ...					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $11,135,181.00

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

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

DATE OF ORDER: 06/19/2009
CONTRACT NO: HSHQDC-06-D-00024
ORDER NO: HSHQDC-09-J-00153

ITEM NO (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Accounting Info: CS00000-000-K9-04-01-01-004-90-05-0002 -07-05-00-00-GE-OE-2576-CS9080 Funded: (b)(4) Accounting Info: CS00000-000-K9-04-01-01-004-90-05-0002 -07-03-00-00-GE-OE-2576-CS9080 Funded: (b)(4)					
0003	Strategic Analysis Services IAW SOW: Tasks 6.4, 6.4.1, 6.4.2, 6.4.3, 6.4.4, 6.4.5, 6.4.6, 6.4.7, 6.4.8, and 6.4.9 (This CLIN covers al reference tasks) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Accounting Info: CS00000-000-K9-04-01-01-004-90-05-0002 -07-03-00-00-GE-OE-2576-CS9080 Funded: (b)(4) Accounting Info: CS00000-000-K9-04-01-01-001-90-05-0002 -05-04-05-00-GE-OE-2576-CS9080 Funded: (b)(4) Accounting Info: CS00000-000-K9-04-01-01-001-90-05-0002 -05-02-02-00-GE-OE-2576-CS9080 Funded (b)(4)			(b)(4)		
0004	Situational Awareness (EINSTEIN) IAW SOW : Tasks 6.5, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, and 6.5.6 (This CLIN covers all reference tasks) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Accounting Info: CS00000-000-K9-04-01-01-001-90-05-0002 -05-02-02-00-GE-OE-2576-CS9080 Funded (b)(4) Accounting Info: CS00000-000-K9-04-01-01-001-90-05-0002 -05-04-01-00-GE-OE-2576-CS9080 Funded: (b)(4) Continued ...					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $15,448,707.00

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

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

DATE OF ORDER: 06/19/2009
CONTRACT NO: HSHQDC-06-D-00024
ORDER NO: HSHQDC-09-J-00153

ITEM NO (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
0005	Information Support Services IAW SOW: Tasks 6.6, 6.6.1, 6.6.2, 6.6.3, 6.6.4, 6.6.5 and 6.6.6. This CLIN covers all reference tasks) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Accounting Info: CS00000-000-K9-04-01-01-001-90-05-0002-05-04-01-00-GE-OE-2576-CS9080 Funded: (b)(4) Accounting Info: CS00000-000-K9-04-01-01-002-90-05-0002-05-03-01-00-GE-OE-2576-CS9080 Funded: (b)(4)				(b)(4)	
0006	Surge Support IAW SOW: Task 8.0 Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Accounting Info: CS00000-000-K9-04-01-01-002-90-05-0002-05-03-01-00-GE-OE-2576-CS9080 Funded: (b)(4)					
0007	Travel-Not to Exceed IAW SOW: 12.0 (Cost Reimbursement) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Accounting Info: CS00000-000-K9-04-01-01-002-90-05-0002-05-03-01-00-GE-OE-2576-CS9080 Funded: (b)(4)					
0008	Other Direct Costs (ODC) IAW SOW: 13.0 (Cost Reimbursement) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Accounting Info: CS00000-000-K9-04-01-01-002-90-05-0002 Continued ...					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $9,212,764.00

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

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

DATE OF ORDER 06/19/2009 | CONTRACT NO HSHQDC-06-D-00024 | ORDER NO HSHQDC-09-J-00153

ITEM NO (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	-05-03-01-00-GE-OE-2576-CS9080 Funded: (b)(4)					
0009	Other Direct Costs (ODC) IAW SOW: 6.5.1 NCPS Block 2.1 Security Incident and Event Management (SIEM) (Cost Reimbursement) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Accounting Info: CS00000-000-K9-04-01-01-002-90-05-0002 -05-03-01-00-GE-OE-2576-CS9080 Funded (b)(4) Accounting Info: CS00000-000-K9-04-01-01-003-90-05-0002 -05-02-03-00-GE-OE-2576-CS9080 Funded (b)(4)				(b)(4)	
0010	Task Order Management IAW SOW: Tasks 6.1, 6.1.1, 6.1.2, 6.1.3, 6.1.4, and 6.1.5 (This CLIN cover all reference tasks) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Accounting Info: CS00000-000-K9-04-01-01-003-90-05-0002 -05-02-03-00-GE-OE-2576-CS9080 Funded: (b)(4)					
0011	Workspace Services IAW SOW: Task 7.0 (Not Separately Priced) Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Accounting Info: Funded (b)(4)					
0012	Transition Plan IAW SOW: Task 6.9 Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Continued ...					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $9,156,525.00

AUTHORIZED FOR LOCAL REPODUCTION
PREVIOUS EDITION NOT USABLE

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

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

DATE OF ORDER	CONTRACT NO	ORDER NO
06/19/2009	HSHQDC-06-D-00024	HSHQDC-09-J-00153

ITEM NO (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Accounting Info: CS00000-000-F9-04-01-01-003-90-05-0002 -05-02-03-00-GE-OE-2576-CS9080 Funded: (b)(4) The total amount of award: $44,953,177.00. The obligation for this award is shown in box 17(i).					
	TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))				$0.00	

AUTHORIZED FOR LOCAL REPODUCTION
PREVIOUS EDITION NOT USABLE

CONTRACTOR SIGNATURE PAGE

[redacted] (b)(4), (b)(6)

Manager Contracts

For General Dynamics One Source, LLC

19 June 2009

Date

I. This is a hybrid type task order, containing time and material (T&M), firm-fixed-price, and cost reimbursable Contract Line Item Numbers (CLINs).

II. The contractor shall perform all work set forth in the statement of work, the instructions contained herein, and all terms and conditions of the Department of Homeland Security (DHS) Enterprise Acquisition Gateway for Leading-Edge Solutions (EAGLE) contract number **HSHQDC-06-D-00024**.

III. Labor Categories, Unit Prices Per Hour and Payment

The contractor shall provide the following types of labor at the corresponding unit price per hour in accordance with the terms of this task order. The unit price per hour is inclusive of the hourly wage plus any applicable labor overhead, General and Administrative (G&A) expenses, and profit. Payment shall be made to the contractor upon delivery to and acceptance by the Government office requesting services. The total amounts billed shall be derived by multiplying the actual number of hours worked per category by the corresponding price per hour.
Statement of Work Tasks 6.2, 6.2.1, 6.2.2, 6.2.3, 6.2.4, 6.2.5, 6.2.6, 6.2.7, 6.2.8, 6.2.9, 6.2.10, 6.2.11, 6.2.12, 6.2.13,6.3, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.7, 6.4, 6.4.1, 6.4.2, 6.4.3, 6.4.4, 6.4.5, 6.4.6, 6.4.7, 6.4.8, 6.4.9, 6.5, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.6, 6.6, 6.6.1, 6.6.2, 6.6.3, 6.6.4, 6.6.5, 6.6.6, 8.0

BASE PERIOD

EAGLE Labor Category #	EAGLE Govt. Labor Category Title	Rate	Hours
	GOVERNMENT SITE		
[redacted]			

(b)(4)

IV. Federal Acquisition Regulation Clauses and Provisions

52.204-2 SECURITY REQUIREMENTS (AUG 1996)

(a) This clause applies to the extent that this contract involves access to information classified "Confidential," "Secret," or "Top Secret."

(b) The Contractor shall comply with—

(1) The Security Agreement (DD Form 441), including the *National Industrial Security Program Operating Manual* (DoD 5220.22-M); and

(2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.

(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

(End of clause)

FAR 52.204-9 PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (NOV 2006)

(a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, as amended, and Federal Information Processing Standards Publication (FIPS PUB) Number 201, as amended.

(b) The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system. (End of clause)

FAR 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six (6) months. The Contracting Officer may exercise the option by written notice to the Contractor within seven (45) days.

(End of clause)

52.227-14 RIGHTS IN DATA – GENERAL (DEC 2007)

(a) *Definitions.* As used in this clause—

"Computer database" or "database means" a collection of recorded information in a form capable of, and for the purpose of, being stored in, processed, and operated on by a computer. The term does not include computer software.

"Computer software"—

(1) Means

(i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and

(ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

(2) Does not include computer databases or computer software documentation.

"Computer software documentation" means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.

"Data" means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

"Form, fit, and function data" means data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, and data identifying source, size, configuration, mating and attachment characteristics, functional characteristics, and performance requirements. For computer software it means data identifying source, functional characteristics, and performance requirements but specifically excludes the source code, algorithms, processes, formulas, and flow charts of the software.

"Limited rights" means the rights of the Government in limited rights data as set forth in the Limited Rights Notice of paragraph (g)(3) if included in this clause.

"Limited rights data" means data, other than computer software, that embody trade secrets or are commercial or financial and confidential or privileged, to the extent that such data pertain to items, components, or processes developed at private expense, including minor modifications.

"Restricted computer software" means computer software developed at private expense and that is a trade secret, is commercial or financial and confidential or privileged, or is copyrighted computer software, including minor modifications of the computer software.

"Restricted rights," as used in this clause, means the rights of the Government in restricted computer software, as set forth in a Restricted Rights Notice of paragraph (g) if included in this clause, or as otherwise may be provided in a collateral agreement incorporated in and made part of this contract, including minor modifications of such computer software.

"Technical data" means recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer databases and computer software documentation). This term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration. The term includes recorded information of a scientific or technical nature that is included in computer databases (See 41 U.S.C. 403(8)).

"Unlimited rights" means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

(b) Allocation of rights.

(1) Except as provided in paragraph (c) of this clause, the Government shall have unlimited rights in—

(i) Data first produced in the performance of this contract;

(ii) Form, fit, and function data delivered under this contract;

(iii) Data delivered under this contract (except for restricted computer software) that constitute manuals or instructional and training material for installation, operation, or routine maintenance and repair of items, components, or processes delivered or furnished for use under this contract; and

(iv) All other data delivered under this contract unless provided otherwise for limited rights data or restricted computer software in accordance with paragraph (g) of this clause.

(2) The Contractor shall have the right to—

(i) Assert copyright in data first produced in the performance of this contract to the extent provided in paragraph (c)(1) of this clause;

(ii) Use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, unless provided otherwise in paragraph (d) of this clause;

(iii) Substantiate the use of, add, or correct limited rights, restricted rights, or copyright notices and to take other appropriate action, in accordance with paragraphs (e) and (f) of this clause; and

(iv) Protect from unauthorized disclosure and use those data that are limited rights data or restricted computer software to the extent provided in paragraph (g) of this clause.

(c) Copyright—

(1) Data first produced in the performance of this contract.

(i) Unless provided otherwise in paragraph (d) of this clause, the Contractor may, without prior approval of the Contracting Officer, assert copyright in scientific and technical articles based on or containing data first produced in the performance of this contract and published in academic, technical or professional journals, symposia proceedings, or similar works. The prior, express written permission of the Contracting Officer is required to assert copyright in all other data first produced in the performance of this contract.

(ii) When authorized to assert copyright to the data, the Contractor shall affix the applicable copyright notices of 17 U.S.C. 401 or 402, and an acknowledgment of Government sponsorship (including contract number).

(iii) For data other than computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly by or on behalf of the Government. For computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted computer software to reproduce, prepare derivative works, and perform publicly and display publicly (but not to distribute copies to the public) by or on behalf of the Government.

(2) *Data not first produced in the performance of this contract.* The Contractor shall not, without the prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract unless the Contractor—

(i) Identifies the data; and

(ii) Grants to the Government, or acquires on its behalf, a license of the same scope as set forth in paragraph (c)(1) of this clause or, if such data are restricted computer software, the Government shall acquire a copyright license as set forth in paragraph (g)(4) of this clause (if included in this contract) or as otherwise provided in a collateral agreement incorporated in or made part of this contract.

(3) *Removal of copyright notices.* The Government will not remove any authorized copyright notices placed on data pursuant to this paragraph (c), and will include such notices on all reproductions of the data.

(d) *Release, publication, and use of data.* The Contractor shall have the right to use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, except—

(1) As prohibited by Federal law or regulation (*e.g.*, export control or national security laws or regulations);

(2) As expressly set forth in this contract; or

(3) If the Contractor receives or is given access to data necessary for the performance of this contract that contain restrictive markings, the Contractor shall treat the data in accordance with such markings unless specifically authorized otherwise in writing by the Contracting Officer.

(e) Unauthorized marking of data.

(1) Notwithstanding any other provisions of this contract concerning inspection or acceptance, if any data delivered under this contract are marked with the notices specified in paragraph (g)(3) or (g) (4) if included in this clause, and use of the notices is not authorized by this clause, or if the data bears any other restrictive or limiting markings not authorized by this contract, the Contracting Officer may at any time either return the data to the Contractor, or cancel or ignore the markings. However, pursuant to 41 U.S.C. 253d, the following procedures shall apply prior to canceling or ignoring the markings.

(i) The Contracting Officer will make written inquiry to the Contractor affording the Contractor 60 days from receipt of the inquiry to provide written justification to substantiate the propriety of the markings;

(ii) If the Contractor fails to respond or fails to provide written justification to substantiate the propriety of the markings within the 60-day period (or a longer time approved in writing by the Contracting Officer for good cause shown), the Government shall have the right to cancel or ignore the markings at any time after said period and the data will no longer be made subject to any disclosure prohibitions.

(iii) If the Contractor provides written justification to substantiate the propriety of the markings within the period set in paragraph (e)(1)(i) of this clause, the Contracting Officer will consider such written justification and determine whether or not the markings are to be cancelled or ignored. If the Contracting Officer determines that the markings are authorized, the Contractor will be so notified in writing. If the Contracting Officer determines, with concurrence of the head of the contracting activity, that the markings are not authorized, the Contracting Officer will furnish the Contractor a written determination, which determination will become the final agency decision regarding the appropriateness of the markings unless the Contractor files suit in a court of competent jurisdiction within 90 days of receipt of the Contracting Officer's decision. The Government will continue to abide by the markings under this paragraph (e)(1)(iii) until final resolution of the matter either by the Contracting Officer's determination becoming final (in which instance the Government will thereafter have the right to cancel or ignore the markings at any time and the data will no longer be made subject to any disclosure prohibitions), or by final disposition of the matter by court decision if suit is filed.

(2) The time limits in the procedures set forth in paragraph (e)(1) of this clause may be modified in accordance with agency regulations implementing the Freedom of Information Act (5 U.S.C. 552) if necessary to respond to a request thereunder.

(3) Except to the extent the Government's action occurs as the result of final disposition of the matter by a court of competent jurisdiction, the Contractor is not precluded by paragraph (e) of the clause from bringing a claim, in accordance with the Disputes clause of this contract, that may arise as the result of the Government removing or ignoring authorized markings on data delivered under this contract.

(f) Omitted or incorrect markings.

(1) Data delivered to the Government without any restrictive markings shall be deemed to have been furnished with unlimited rights. The Government is not liable for the disclosure, use, or reproduction of such data.

(2) If the unmarked data has not been disclosed without restriction outside the Government, the Contractor may request, within 6 months (or a longer time approved by the Contracting Officer in writing for good cause shown) after delivery of the data, permission to have authorized notices placed on the data at the Contractor's expense. The Contracting Officer may agree to do so if the Contractor—

(i) Identifies the data to which the omitted notice is to be applied;

(ii) Demonstrates that the omission of the notice was inadvertent;

(iii) Establishes that the proposed notice is authorized; and

(iv) Acknowledges that the Government has no liability for the disclosure, use, or reproduction of any data made prior to the addition of the notice or resulting from the omission of the notice.

(3) If data has been marked with an incorrect notice, the Contracting Officer may—

(i) Permit correction of the notice at the Contractor's expense if the Contractor identifies the data and demonstrates that the correct notice is authorized; or

(ii) Correct any incorrect notices.

(g) Protection of limited rights data and restricted computer software.

(1) The Contractor may withhold from delivery qualifying limited rights data or restricted computer software that are not data identified in paragraphs (b)(1)(i), (ii), and (iii) of this clause. As a condition to this withholding, the Contractor shall—

(i) Identify the data being withheld; and

(ii) Furnish form, fit, and function data instead.

(2) Limited rights data that are formatted as a computer database for delivery to the Government shall be treated as limited rights data and not restricted computer software.

(3) [Reserved]

(h) *Subcontracting.* The Contractor shall obtain from its subcontractors all data and rights therein necessary to fulfill the Contractor's obligations to the Government under this contract. If a subcontractor refuses to accept terms affording the Government those rights, the Contractor shall promptly notify the Contracting Officer of the refusal and shall not proceed with the subcontract award without authorization in writing from the Contracting Officer.

(i) *Relationship to patents or other rights.* Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Government.

(End of clause)

Alternate II (Dec 2007).

(g)(3) Notwithstanding paragraph (g)(1) of this clause, the contract may identify and specify the delivery of limited rights data, or the Contracting Officer may require by written request the delivery of limited rights

data that has been withheld or would otherwise be entitled to be withheld. If delivery of that data is required, the Contractor shall affix the following "Limited Rights Notice" to the data and the Government will treat the data, subject to the provisions of paragraphs (e) and (f) of this clause, in accordance with the notice:

LIMITED RIGTHS NOTICE (DEC 2007)

(a) These data are submitted with limited rights under Government Contract No. _**HSHQDC-06-D-00024/HSHQDC-09-J-00153**_ (and subcontract _____, if appropriate). These data may be reproduced and used by the Government with the express limitation that they will not, without written permission of the Contractor, be used for purposes of manufacture nor disclosed outside the Government; except that the Government may disclose these data outside the Government for the following purposes, if any; provided that the Government makes such disclosure subject to prohibition against further use and disclosure: [*Agencies may list additional purposes as set forth in 27.404-2(c)(1) or if none, so state.*]

(b) This notice shall be marked on any reproduction of these data, in whole or in part.

(End of notice)

FAR 52.232-7 PAYMENTS UNDER TIME-and-MATERIALS and LABOR-HOUR CONTRACTS (FEB 2007)

The Government will pay the Contractor as follows upon the submission of vouchers approved by the Contracting Officer or the authorized representative:

(a) *Hourly rate.*

(1) *Hourly rate* means the rate(s) prescribed in the contract for payment for labor that meets the labor category qualifications of a labor category specified in the contract that are—

(i) Performed by the Contractor;

(ii) Performed by the subcontractors; or

(iii) Transferred between divisions, subsidiaries, or affiliates of the Contractor under a common control.

(2) The amounts shall be computed by multiplying the appropriate hourly rates prescribed in the Schedule by the number of direct labor hours performed.

(3) The hourly rates shall be paid for all labor performed on the contract that meets the labor qualifications specified in the contract. Labor hours incurred to perform tasks for which labor qualifications were specified in the contract will not be paid to the extent the work is performed by employees that do not meet the qualifications specified in the contract, unless specifically authorized by the Contracting Officer.

(4) The hourly rates shall include wages, indirect costs, general and administrative expense, and profit. Fractional parts of an hour shall be payable on a prorated basis.

(5) Vouchers may be submitted once each month (or at more frequent intervals, if approved by the Contracting Officer), to the Contracting Officer or authorized representative. The Contractor shall substantiate

vouchers (including any subcontractor hours reimbursed at the hourly rate in the schedule) by evidence of actual payment and by—

(i) Individual daily job timekeeping records;

(ii) Records that verify the employees meet the qualifications for the labor categories specified in the contract; or

(iii) Other substantiation approved by the Contracting Officer.

(6) Promptly after receipt of each substantiated voucher, the Government shall, except as otherwise provided in this contract, and subject to the terms of paragraph (e) of this clause, pay the voucher as approved by the Contracting Officer or authorized representative.

(7) Unless otherwise prescribed in the Schedule, the Contracting Officer may unilaterally issue a contract modification requiring the Contractor to withhold amounts from its billings until a reserve is set aside in an amount that the Contracting Officer considers necessary to protect the Government's interests. The Contracting Officer may require a withhold of 5 percent of the amounts due under paragraph (a) of this clause, but the total amount withheld for the contract shall not exceed $50,000. The amounts withheld shall be retained until the Contractor executes and delivers the release required by paragraph (g) of this clause.

(8) Unless the Schedule prescribes otherwise, the hourly rates in the Schedule shall not be varied by virtue of the Contractor having performed work on an overtime basis. If no overtime rates are provided in the Schedule and overtime work is approved in advance by the Contracting Officer, overtime rates shall be negotiated. Failure to agree upon these overtime rates shall be treated as a dispute under the Disputes clause of this contract. If the Schedule provides rates for overtime, the premium portion of those rates will be reimbursable only to the extent the overtime is approved by the Contracting Officer.

(b) *Materials.*

(1) or the purposes of this clause—

(i) *Direct materials* means those materials that enter directly into the end product, or that are used or consumed directly in connection with the furnishing of the end product or service.

(ii) *Materials* means—

(A) Direct materials, including supplies transferred between divisions, subsidiaries, or affiliates of the Contractor under a common control;

(B) Subcontracts for supplies and incidental services for which there is not a labor category specified in the contract;

(C) Other direct costs (*e.g.*, incidental services for which there is not a labor category specified in the contract, travel, computer usage charges, etc.); and

(D) Applicable indirect costs.

(2) If the Contractor furnishes its own materials that meet the definition of a commercial item at 2.101, the price to be paid for such materials shall not exceed the Contractor's established catalog or market price, adjusted to reflect the—

(i) Quantities being acquired; and

(ii) Actual cost of any modifications necessary because of contract requirements.

(3) Except as provided for in paragraph (b)(2) of this clause, the Government will reimburse the Contractor for allowable cost of materials provided the Contractor—

(i) Has made payments for materials in accordance with the terms and conditions of the agreement or invoice; or

(ii) Ordinarily makes these payments within 30 days of the submission of the Contractor's payment request to the Government and such payment is in accordance with the terms and conditions of the agreement or invoice.

(4) Payment for materials is subject to the Allowable Cost and Payment clause of this contract. The Contracting Officer will determine allowable costs of materials in accordance with Subpart 31.2 of the Federal Acquisition Regulation (FAR) in effect on the date of this contract.

(5) The Contractor may include allocable indirect costs and other direct costs to the extent they are—

(i) Comprised only of costs that are clearly excluded from the hourly rate;

(ii) Allocated in accordance with the Contractor's written or established accounting practices; and

(iii) Indirect costs are not applied to subcontracts that are paid at the hourly rates.

(6) To the extent able, the Contractor shall—

(i) Obtain materials at the most advantageous prices available with due regard to securing prompt delivery of satisfactory materials; and

(ii) Take all cash and trade discounts, rebates, allowances, credits, salvage, commissions, and other benefits. When unable to take advantage of the benefits, the Contractor shall promptly notify the Contracting Officer and give the reasons. The Contractor shall give credit to the Government for cash and trade discounts, rebates, scrap, commissions, and other amounts that have accrued to the benefit of the Contractor, or would have accrued except for the fault or neglect of the Contractor. The Contractor shall not deduct from gross costs the benefits lost without fault or neglect on the part of the Contractor, or lost through fault of the Government.

(7) Except as provided for in 31.205-26(e) and (f), the Government will not pay profit or fee to the prime Contractor on materials.

(c) If the Contractor enters into any subcontract that requires consent under the clause at 52.244-2, Subcontracts, without obtaining such consent, the Government is not required to reimburse the Contractor for any costs incurred under the subcontract prior to the date the Contractor obtains the required consent. Any reimbursement of subcontract costs incurred prior to the date the consent was obtained shall be at the sole discretion of the Government.

(d) *Total cost.* It is estimated that the total cost to the Government for the performance of this contract shall not exceed the ceiling price set forth in the Schedule, and the Contractor agrees to use its best efforts to perform the work specified in the Schedule and all obligations under this contract within such ceiling price. If at any time the Contractor has reason to believe that the hourly rate payments and material costs that will accrue in performing this contract in the next succeeding 30 days, if added to all other payments and costs previously accrued, will exceed 85 percent of the ceiling price in the Schedule, the Contractor shall notify the Contracting Officer giving a revised estimate of the total price to the Government for performing this contract with supporting reasons and documentation. If at any time during performing this contract, the Contractor has reason to believe that the total price to the Government for performing this contract will be substantially greater or less than the then stated ceiling price, the Contractor shall so notify the Contracting Officer, giving a revised estimate of the total price for performing this contract, with supporting reasons and documentation. If at any time during performing this contract, the Government has reason to believe that the work to be required in performing this contract will be substantially greater or less than the stated ceiling price, the Contracting Officer will so advise the Contractor, giving the then revised estimate of the total amount of effort to be required under the contract.

(e) *Ceiling price.* The Government will not be obligated to pay the Contractor any amount in excess of the ceiling price in the Schedule, and the Contractor shall not be obligated to continue performance if to do so would exceed the ceiling price set forth in the Schedule, unless and until the Contracting Officer notifies the Contractor

in writing that the ceiling price has been increased and specifies in the notice a revised ceiling that shall constitute the ceiling price for performance under this contract. When and to the extent that the ceiling price set forth in the Schedule has been increased, any hours expended and material costs incurred by the Contractor in excess of the ceiling price before the increase shall be allowable to the same extent as if the hours expended and material costs had been incurred after the increase in the ceiling price.

(f) *Audit.* At any time before final payment under this contract, the Contracting Officer may request audit of the vouchers and supporting documentation. Each payment previously made shall be subject to reduction to the extent of amounts, on preceding vouchers, that are found by the Contracting Officer or authorized representative not to have been properly payable and shall also be subject to reduction for overpayments or to increase for underpayments. Upon receipt and approval of the voucher designated by the Contractor as the "completion voucher" and supporting documentation, and upon compliance by the Contractor with all terms of this contract (including, without limitation, terms relating to patents and the terms of paragraph (g) of this clause), the Government shall promptly pay any balance due the Contractor. The completion voucher, and supporting documentation, shall be submitted by the Contractor as promptly as practicable following completion of the work under this contract, but in no event later than 1 year (or such longer period as the Contracting Officer may approve in writing) from the date of completion.

(g) *Assignment and Release of Claims.* The Contractor, and each assignee under an assignment entered into under this contract and in effect at the time of final payment under this contract, shall execute and deliver, at the time of and as a condition precedent to final payment under this contract, a release discharging the Government, its officers, agents, and employees of and from all liabilities, obligations, and claims arising out of or under this contract, subject only to the following exceptions:

(1) Specified claims in stated amounts, or in estimated amounts if the amounts are not susceptible of exact statement by the Contractor.

(2) Claims, together with reasonable incidental expenses, based upon the liabilities of the Contractor to third parties arising out of performing this contract, that are not known to the Contractor on the date of the execution of the release, and of which the Contractor gives notice in writing to the Contracting Officer not more than 6 years after the date of the release or the date of any notice to the Contractor that the Government is prepared to make final payment, whichever is earlier.

(3) Claims for reimbursement of costs (other than expenses of the Contractor by reason of its indemnification of the Government against patent liability), including reasonable incidental expenses, incurred by the Contractor under the terms of this contract relating to patents.

(h) *Interim payments on contracts for other than services.*

(1) Interim payments made prior to the final payment under the contract are contract financing payments. Contract financing payments are not subject to the interest penalty provisions of the Prompt Payment Act.

(2) The designated payment office will make interim payments for contract financing on the 30th day after the designated billing office receives a proper payment request. In the event that the Government requires an audit or other review of a specific payment request to ensure compliance with the terms and conditions of the contract, the designated payment office is not compelled to make payment by the specified due date.

(i) *Interim payments on contracts for services.* For interim payments made prior to the final payment under this contract, the Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR part 1315.

(End of clause)

FAR 52.243-3 CHANGES—TIME-and-MATERIALS or LABOR-HOURS (SEPT 2000)

(a) The Contracting Officer may at any time, by written order, and without notice to the sureties, if any, make changes within the general scope of this contract in any one or more of the following:

(1) Description of services to be performed.

(2) Time of performance (*i.e.,* hours of the day, days of the week, etc.).

(3) Place of performance of the services.

(4) Drawings, designs, or specifications when the supplies to be furnished are to be specially manufactured for the Government in accordance with the drawings, designs, or specifications.

(5) Method of shipment or packing of supplies.

(6) Place of delivery.

(7) Amount of Government-furnished property.

(b) If any change causes an increase or decrease in any hourly rate, the ceiling price, or the time required for performance of any part of the work under this contract, whether or not changed by the order, or otherwise affects any other terms and conditions of this contract, the Contracting Officer will make an equitable adjustment in any one or more of the following and will modify the contract accordingly:

(1) Ceiling price.

(2) Hourly rates.

(3) Delivery schedule.

(4) Other affected terms.

(c) The Contractor shall assert its right to an adjustment under this clause within 30 days from the date of receipt of the written order. However, if the Contracting Officer decides that the facts justify it, the Contracting Officer may receive and act upon a proposal submitted before final payment of the contract.

(d) Failure to agree to any adjustment will be a dispute under the Disputes clause. However, nothing in this clause excuses the Contractor from proceeding with the contract as changed.

(End of clause)

V. DEPARTMENT OF HOMELAND SECURITY ACQUISITION REGULATION (HSAR) PROVISIONS AND CLAUSES

HSAR 3052.204-70 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JUN 2006)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's

proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of clause)

HSAR 3052.204-71 CONTRACTOR EMPLOYEE ACCESS (JUN 2006)

(a) *Sensitive Information,* as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of S SI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

ALTERNATE I
(JUN 2006)

When the contract will require contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract.

Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) The individual must be a legal permanent resident of the U. S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;

(2) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and

(3) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

(End of clause)

POST-AWARD INSTRUCTIONS REGARDING SECURITY REQUIREMENTS FOR CONTRACTS/ORDERS

1. The procedures outlined below shall be followed for the DHS Security Office to process background investigations and suitability determinations, as required, in a timely and efficient manner.

2. Carefully read the security clauses in the contract. Compliance with the security clauses in the contract is not optional.

3. Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Security Office. Prospective Contractor employees shall submit the following completed forms to the DHS Security Office. The Standard Form 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the DHS Security Office no less than thirty

(30) days before the start date of the contract or thirty (30) days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

a. Standard Form 85P, "Questionnaire for Public Trust Positions"

b. FD Form 258, "Fingerprint Card" (2 copies)

c. DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"

d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

Only complete packages will be accepted by the DHS Security Office. Specific instructions on submission of packages will be provided upon award of the contract.

4. DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Security Office.

   Contractor employees waiting for an EOD decision may begin work on the contract provided they do not access sensitive Government information. Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by a Government employee. This limited access is to allow Contractors to attend briefings and non-recurring meetings in order to begin transition work.

5. The DHS Security Office shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Technical Representative (COTR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COTR, referencing the pass or card number, name of individual to who it was issued and the last known location and disposition of the pass or card.

6. [If HSAR 3052.204-71 Alternative clauses are used, Section 6 instructions apply.]

   ***** USE THE FOLLOWING ONLY WITH HSAR 3052.204-71 ALT 1 CONTRACTS *****

   When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

   Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results

in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

***** USE THE FOLLOWING ONLY WITH HSAR 3052.204-71 ALT 2 CONTRACTS *****

See HSAR 3052.204-71 (g) (Alt 2) for alternative citizenship requirements for non IT contracts.

7. Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the government do not relieve a contractor from performing under the terms of the contract.
8. Your POC at the Security Office is:
   DHS, Office of Security
   Personnel Security Staff
   Attn: Ronnie Mitchell
   Washington DC 20528
   Telephone: (b)(6)

HSAR 3052.209-70 PROHIBITION ON CONTRACTS WITH CORPORATE EXPATRIATES (JUN 2006)

(a) Prohibitions.

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) Definitions. As used in this clause:

Expanded Afiliated Group means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting `more than 50 percent' for `at least 80 percent' each place it appears.

Foreign Incorporated Entity means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

Inverted Domestic Corporation. A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;

(2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—

(i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or

(ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and

(3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

Person, domestic, and foreign have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

(1) *Certain Stock Disregarded.* For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:

(i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or

(ii) stock of such entity which is sold in a public offering related to the acquisition described in subsection (b)(1) of Section 835 of the Homeland Security Act, 6 U.S.C. 395(b)(1).

(2) Plan Deemed In Certain Cases. If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.

(3) Certain Transfers Disregarded. The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) Special Rule for Related Partnerships. For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395(b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) Treatment of Certain Rights.

(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:

(i) warrants;

(ii) options;

(iii) contracts to acquire stock;

(iv) convertible debt instruments; and

(v) others similar interests.

(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of Section 835.

(f) Disclosure. The offeror under this solicitation represents that [Check one]: __ it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.104-70 through 3009.104-73;

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.104-70 through 3009.104-73, but it has submitted a request for waiver pursuant to 3009.104-74, which has not been denied; or

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.104-70 through 3009.104-73, but it plans to submit a request for waiver pursuant to 3009.104-74.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(End of provision)

HSAR 3052.209-72 ORGANIZATIONAL CONFLICT OF INTEREST (JUN 2006)

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting [**Access to non-public information gained in the performance of a DHS contract that could provide them with an unfair advantage regarding the instant acquisition**].

(b) If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents, to the best of its knowledge that:

___ (1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or

___ (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included a mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes the conflict can be avoided, neutralized, or mitigated, the offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror,

and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or dive stures that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

(End of provision)

HSAR 3052.209-73 LIMITATION OF FUTURE CONTRACTING (JUN 2006)

(a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective offerors is invited to FAR Subpart 9.5--Organizational Conflicts of Interest.

(b) The nature of this conflict involves the preparing of specifications or work statements for future acquisitions related to the program.

(c) The restrictions upon future contracting are as follows:
(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.
(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

HSAR 3052.215-70 KEY PERSONNEL OR FACILITIES (DEC 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

Key Personnel under this task order [redacted] (b)(6) (b)(6)

(End of clause)

HSAR 3052.242-71 DISSEMINATION OF CONTRACT INFORMATION (DEC 2003)

The Contractor shall not publish, permit to be published, or distribute for public consumption, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this contract, without the prior written consent of the Contracting Officer. An electronic or printed copy of any material proposed to be published or distributed shall be submitted to the Contracting Officer.

(End of clause)

HSAR 3052.242-72 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (DEC 2003)

(a) The Contracting Officer may designate Government personnel to act as the Contracting Officer's Technical Representative (COTR) to perform functions under the contract such as review or inspection and acceptance of supplies, services, including construction, and other functions of a technical nature. The Contracting Officer will provide a written notice of such designation to the Contractor within five working days after contract award or for construction, not less than five working days prior to giving the contractor the notice to proceed. The designation letter will set forth the authorities and limitations of the COTR under the contract.

(b) The Contracting Officer cannot authorize the COTR or any other representative to sign documents, such as contracts, contract modifications, etc., that require the signature of the Contracting Officer.

(End of clause)

VI. LOCAL CLAUSES

1. PERIOD OF PERFORMANCE.

The period of performance for this order shall commence upon date and the base period shall continue for eleven (11) months thereafter. If any or all of the contract options are exercised pursuant to the terms of the order, then the period of performance shall be extended in accordance with the schedule set forth below:

a) Base Period: Eleven (11) months from the date of Award

The timeframes listed above provide the overall period of performance for the task order. However, the price schedule delineates the specific periods of performance for each of the tasks identified in the statement of work.

2. TRAVEL.

a. Long-distance Travel. The contractor shall seek advance written approval from the contracting officer (CO) and contracting officer technical representative (COTR) prior to incurring any costs associated with travel. The request shall be forwarded from the contractor's contracts or procurement point of contact.

The contractor will be reimbursed for actual travel-related costs in accordance with the federal lodging and per diem allowances stated in the Federal Acquisition Regulation (FAR) 31.205-46 and the Federal Travel Regulation (FTR) governing the travel requirements conducted under this contract. The government will not reimburse transportation costs in excess of coach class commercially-scheduled air or reasonable ground transportation by the most expeditious route. Special FAR requirements exist for overseas travel.

Advance travel requests shall be submitted in sufficient time for the CO and COTR to grant prior approval, and

must identify: a) the name of the traveler(s); b) inclusive dates and destination (including itinerary); c) purpose of the trip; and d) include a complete cost breakdown.

When seeking reimbursement, the long-distance travel expenditures must be: a) other than local travel expenses within the local Washington DC metropolitan commuting area or the location of the contractor's personnel if their actual workplace is outside the Washington DC metropolitan area; b) allowable under the FTR, FAR and the terms and conditions of this contract; c) approved by the CO and COTR prior to travel expenditure; and d) allocable, allowable, reasonable, and necessary for performance under this contract.

Invoices, including travel expenses, must provide a detailed cost breakdown of the actual expenditures incurred. The contractor shall maintain the original or legible copy of receipts for all travel-related expenses, with copies provided along with the applicable invoice. The government reserves the right to request additional evidence of any invoiced travel-related expenses.

The contractor shall be reimbursed on an actual cost basis in accordance with the FAR and FTR allowances. The contractor shall request and be in receipt of advance approval from the CO and COTR prior to incurring any costs associated with long-distance travel.

b. Local Travel. Local travel costs will not be reimbursed under this task order except in the following limited situations:

Reimbursement for local travel costs will be authorized to support the following operations:

1. Site surveys, installation, operations, maintenance or upgrades involving National Cyber Protection System (NCPS).
2. NCPS technical interchange meetings and engineering support activities conducted with external Federal, State and Local, Academic entities.
3. Incident response to support collection of compromised digital media (hard drives, removable drives, computers, etc.), on site network damage assessments to determine the extent of a network compromise, and assistance to mitigate the affect of a compromise or other threat activity or vulnerability.
4. Participation in the Joint Agency Collaborative Knowledge Exchange (JACKE) program, to include courier duties for classified technical information.

Local travel costs are not authorized to support local meetings, conferences, or training.

3. SUBMISSION OF INVOICES.

Original invoices shall be sent to the address identified in block **21** of form **Optional Form 347**. The invoice must contain the (1) contract number or blanket purchase agreement as applicable, (2) order number, (3) applicable contract line item number(s). The invoice must comply with the payment clause in this award document to be considered a proper invoice.

The contractor shall also submit invoices to the following locations:

NPPDVendorInvoices@HQ.DHS.GOV

and to:

the Contracting Officer (CO) and Contracting Officer's Technical Representative (COTR).

4. ORGANIZATIONAL CONFLICTS OF INTEREST.

It is recognized by the parties hereto that the effort performed by the Contractor under this contract is of a nature that it may create a real or perceived organizational conflict of interest as contemplated under the FAR Subpart 9.5.

Purpose. The primary purpose of this clause is to ensure that:1) the contractor's objectivity and judgment are not biased because of its past, present, or currently planned interests (financial, contractual, organizational, or otherwise) which relate to work under this contract; 2) the contractor does not obtain an unfair competitive advantage by virtue of its access to non-public information regarding the government's program plans and actual or anticipated resources; and 3) by virtue of its access to proprietary information belonging to others, the contractor does not obtain any unfair competitive advantage.

Scope. The restrictions described herein shall apply to performance or participation by the contractor and any of its affiliates or their successors in interest (hereinafter collectively referred to as "contractor") in the activities covered by this clause as prime contractor, subcontractor, co-sponsor, joint venture, teaming partner, consultant, or in any similar capacity.

Maintenance of Objectivity. The contractor shall be ineligible to participate in any capacity in contracts, sub-contracts, or proposals thereunder which stem directly from the contractor's performance of work under this contract or are directly related to this contract. Furthermore, unless directed in writing by the contracting officer, the contractor shall not perform any services under this contract on any of its own products or services or the products or services of another firm if the contractor is, or has been substantially involved in their development or marketing. In addition, if the awardee under this contract advises the government on the preparation of statements of work, the contractor shall be ineligible to perform or participate in any capacity in any contractual effort which is based on the resulting efforts. Nothing in this subparagraph shall preclude the contractor from competing for follow-on contracts involving the same or similar services.

Access To and Use of Government Information. If the contractor, in the performance of this contract, obtains access to information such as plans, policies, reports, studies, financial plans, or data which has not been released or otherwise made available to the public, the contractor agrees that without prior written approval from the contracting officer, it shall not: a) use such information for any private purpose unless the information has been released or otherwise made available to the public; b) compete for or accept work based on such information for a period of six months after the completion of the contract, or until such information is released or otherwise made available to the public, whichever occurs first; c) submit an unsolicited proposal to the government which is based on such information until one year after such information is released or otherwise made available to the public; and d) release such information unless such information has previously been released or otherwise made available to the public by the government.

Access To and Protection of Proprietary Information The contractor agrees that, to the extent it receives or is given access to proprietary data, trade secrets, or other confidential or privileged technical, business, or financial information (hereinafter referred to as "proprietary data") under this contract, it shall treat such information in accordance with any restrictions imposed on such information. The contractor further agrees to enter into a written agreement for the protection of the proprietary data of other contractors and to exercise diligent effort to protect such proprietary data from unauthorized disclosure. In addition, the contractor shall obtain from each employee who has access to proprietary data under this contract, a written agreement which shall in substance provide that such employee shall not, during his/her employment by the contractor or thereafter, disclose to others or use for their benefit, proprietary data received in conjunction with the work under this contract.

Subcontracts. The contractor shall include this clause in consulting agreements and sub-contracts. The terms "contract," "contractor," and "contracting officer" will be appropriately modified to preserve the government's rights.

Representations and Disclosures

The contractor represents that it has disclosed to the contracting Officer, prior to award and subsequent to award, all facts relevant to the existence or real; pr perceived organizational conflicts of interest as that term is used in FAR Subpart 9.5.

The contractor agrees that if after award it discovers an organizational conflict of interest with respect to this contract, a prompt and full disclosure shall be made in writing to the contracting officer which shall include a plan of action the contractor has taken or proposes to take to avoid or mitigate such conflict(s).

Some techniques that may be utilized to identify, mitigate and avoid organizational conflicts of interests include, but are not limited to: 1) submission of a comprehensive OCI avoidance/mitigation plan that creates organizational, physical, and geographic firewalls; 2) utilization of non-disclosure statements; 3) disclosure of sensitive information to all competitors; 4) active management of organizational conflicts of interest during contract performance; 5) assigning work efforts to contractor team members that are not affected by the conflict; 6) declination of work efforts; and 7) re-organization, restructuring, or divestiture of corporate entities.

Remedies and Waiver

For breach of any of the above restrictions or for nondisclosure or misrepresentation of any relevant facts required to be disclosed concerning this contract, the government may terminate this contract for default, disqualify the contractor from subsequent related contractual efforts, and pursue such other remedies as may be permitted by law or regulation. If, however, in compliance with this clause, the contractor discovers and promptly reports an organizational conflict of interest (or the potential therefore), subsequent to contract award, the contracting officer may terminate this contract for convenience of the government if such termination is deemed to be in the best interest of the government.

The parties recognize that this clause has potential effects which will survive the performance of this contract and that it is impossible to foresee each circumstance to which it might be applied in the future. Accordingly, the Contractor may, at any time, seek a waiver from the Contracting Officer by submitting a full written description of the requested waiver and the reasons in support thereof. If it is determined to be in the best interests of the Government, the Contracting Officer will grant such a waiver.

Compliance with FAR Subpart 9.5 and HSAR 3009.5 regarding perceived or real organizational conflicts of interest (OCI) is required. If an OCI exists, a mitigation plan shall be prepared and forwarded to the contracting officer for resolution.

5. RESOURCE ALLOCATION.

The contractor shall notify the COTR and Contracting Officer when it anticipates that there will be overages or underages in a given CLIN or sub-CLIN. The Contracting Officer may execute a within-scope modification to shift resources (level of effort) and/or capacity amongst CLINs or sub-CLINs. Upon such modification, the contractor is authorized to use available resources (level of effort) and/or capacity across CLINs or sub-CLINs as necessary during the performance period. Written approval from the Contracting Officer and/or task order modification is required prior to utilizing the flexibility granted under this clause.

6. INDIRECT RATES

Any indirect rates applied to travel or other direct costs shall be in accordance with the rates approved by the Defense Contract Audit Agency (DCAA) and consistent with the contractor's normal accounting practices.

7. CONTRACTING OFFICERS - TECHNICAL REPRESENTATIVE

The Contracting Officer may designate a Technical Representative (COTR) to assist in monitoring the work under this contract. The COTR is responsible for the technical administration of the contract and technical liaison with the Contractor. The COTR IS NOT authorized to change the scope of work or specifications as stated in the contract and in any Task Order, to make any commitments or otherwise obligate the Government or authorize any changes which affect the contract price, delivery schedule, period of performance, or other terms or conditions.

The Contracting Officer is the only individual who can legally commit or obligate the Government for the expenditure of public funds. The technical administration of this contract shall not be construed to authorize the revision of the terms and conditions of this contract and any Task Orders issued. The Contracting Officer shall authorize any such revision in writing.

ATTACHMENT C

SECURITY REQUIREMENTS REVIEW CHECKLIST
FOR
CLASSIFIED CONTRACTS/ORDERS

DEPARTMENT OF HOMELAND SECURITY

Office of Procurement Operations

SECURITY REQUIREMENTS REVIEW CHECKLIST FOR CLASSIFIED CONTRACTS/ORDERS

*Program Office should email the completed **Checklist (Section A-C)** and the password-protected proposed **Statement of Work/ Statement of Objectives/Performance Work Statement (appropriately labeled "SOURCE SELECTION INFORMATION, See FAR 2.101 and 3.104")** to DD254AdministrativeSecurity@dhs.gov*

Section A – Procurement Information			
Name of Program Office supported by these services:			
Program Office POC for this procurement:			
Program POC Telephone:		Program POC email:	
Requisition Number:			
Type of Procurement: ☐ Inter-Agency Agreement (IAA) ☐ Blanket Purchase Agreement (BPA) Identify Servicing Agency: ☐ Contract ☐ Other			
☐ Yes	☐ No	New Solicitation	Solicitation Number (if known):
☐ Yes	☐ No	Replacement of existing procurement	
☐ Yes	☐ No	Task on existing contract/BPA	Contract/BPA Number:
		COTR/Task Manager Name:	
		COTR/Task Manager Telephone:	
Section B – Information and Systems Access			
☐ Yes	☐ No	Contractor will require access to National Security Information (NSI) in the performance of their scope of work. NSI access is required at level: ☐ Secret ☐ Top Secret	
☐ Yes	☐ No	Contractor will require access to Sensitive but Unclassified Information.	
☐ Yes	☐ No	Contractor will require DHS information technology (IT) systems access.	
☐ Yes	☐ No	Services will be performed at a DHS facility.	
☐ Yes	☐ No	Services may be performed at a contractor-owned and operated facility.	
☐ Yes	☐ No	Contractor will require DHS building access **only**.	
Section C – Contractor Information			
Estimated number of contractor staff to work on the task order/contract _____			
Section D – Office of Security, Industrial Security Program Branch Review			
Date Review completed:			
Print name of Reviewer/ Security Specialist:			
Signature of Reviewer/ Security Specialist:			
☐ Yes	☐ No	Security clearance required for contractor personnel. (If YES, FAR 52.204-2 required in solicitation and contract/order.)	
☐ Yes	☐ No	Requires access to unclassified DHS information technology (IT) resources (If YES, HSAR clause 3052.204-70 required in solicitation and contract/order)	
☐ Yes	☐ No	Requires access to DHS unclassified facilities, IT resources, & sensitive but unclassified information (If YES, HSAR clause 3052.204-71 required in solicitation and contract/order)	
☐ Yes	☐ No	Requires access to DHS IT resources If YES, HSAR clause 3052.204-71 ALT 1 required in solicitation and contract/order If NO, HSAR clause 3052.204-71 ALT 2 required in solicitation and contract/order	
☐ Yes	☐ No	DD Form 254 (Contract Security Classification Specification) required [See POP 302 and Office of Security, Administrative Security Division, Industrial Security Programs]	

DEPARTMENT OF HOMELAND SECURITY

NATIONAL CYBER SECURITY DIVISION
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

INTEGRATION AND SUPPORT SERVICES STATEMENT OF WORK

April 21, 2009
Version 1.0

Table of Contents

1.0 REQUIRING ORGANIZATION 1
2.0 OBJECTIVE 1
3.0 BACKGROUND 1
3.1 Department of Homeland Security 1
4.0 SCOPE 2
4.1 DHS Enterprise Architecture Compliance 2
4.2 NCPP Enterprise Architecture Compliance 3
5.0 APPLICABLE DOCUMENTS 3
6.0 TECHNICAL REQUIREMENTS/TASKS 4
6.1 Task Order Management 4
6.2 24 X 7 Incident Handling Team Support 6
6.3 Malicious Code Support 9
6.4 Strategic Analysis Services 10
6.5 Situational Awareness (EINSTEIN) 12
6.6 Information Support Services 15
6.7 Transition Planning Services 17
7.0 Workspace Services 18
8.0 SURGE SUPPORT 18
9.0 DELIVERABLES 18
9.1 Format of Deliverables 18
9.2 Acceptance and Rejection Procedures of Draft and Final Deliverables 19
9.3 Deliverable/Delivery Schedule 19
10.0 PERIOD OF PERFORMANCE 21
11.0 PLACE OF PERFORMANCE 21
12.0 Travel Requirements 22
13.0 OTHER DIRECT COSTS 22
14.0 GOVERNMENT FURNISHED INFORMATION AND EQUIPMENT 22
14.1 Government Furnished Information (GFI) 22
14.2 Government Furnished Equipment (GFE) 23
15.0 OTHER PERTINENT INFORMATION OR SPECIAL CONSIDERATIONS 23
15.1 Identification of Potential Conflicts of Interest (COI) 23
15.2 Identification of Non-Disclosure Requirements 23

15.3 FAR 52.227-14, Rights in Data – General 23
16.0 ENHANCED SKILLS TRAINING 24
17.0 PERSONNEL QUALIFICATIONS 24
18.0 ACCESSIBILITY REQUIREMENTS 24
18.1 Applicable Standards 24
18.2 Exceptions 25
19.0 SECURITY REQUIREMENTS 26
19.1 General 26
19.2 Contractor Personnel 27
19.3 Termination 27
19.4 Suitability Determination 28
19.5 Background Investigations 28
19.6 Alternative Citizenship Requirements for Non-IT Contracts 29
19.7 Information Technology Security Clearance 29
19.8 Information Technology Security Training and Oversight 29
19.9 References 30
20.0 INVOICES 30
21.0 ACRONYMS 31

1.0 REQUIRING ORGANIZATION

Department of Homeland Security
National Cyber Security Division
245 Murray Lane
Building 410
Mailstop 8500
Washington, D. C. 20528-8500

2.0 OBJECTIVE

The objective of this Integration and Support Services (ISS) Task Order (TO) is to provide information technology (IT) services to support the Department of Homeland Security (DHS) National Cyber Security Division (NCSD).

3.0 BACKGROUND

3.1 Department of Homeland Security

NCSD functions under DHS and currently supports and interfaces with other functions of DHS.

3.1.1 DHS Under Secretary for National Protection and Program Directorate

The mission of the DHS Under Secretary for National Protection and Program Directorate (NPPD) is to identify and assess current and future threats to the homeland, map those threats against vulnerabilities, issue timely warnings, and take preventive and protective action. Two key areas of support include Intelligence Analysis and Alerts and Critical Infrastructure Protection. The goal of the Intelligence Analysis and Alerts function is to produce actionable intelligence, i.e., information that can lead to stopping or apprehending terrorists, improve the government's ability to disrupt and prevent terrorist acts, and to provide useful warning to the private sector and our population. NPPD fuses and analyzes information from multiple sources pertaining to terrorist threats and partners with intelligence-generating agencies, such as the National Security Agency (NSA), the Central Intelligence Agency (CIA), and the Federal Bureau of Investigation (FBI). DHS threat analysis and warning functions support the President and other national decision-makers. DHS coordinates with Federal, State, and local agencies and with the private sector. The Critical Infrastructure Protection function deals with protecting the nation's critical infrastructure as a shared responsibility of Federal, State, and local government, and in active partnership with the private sector, which owns approximately 85 percent of the nation's critical infrastructure. The Preparedness Directorate (PREP) has the responsibility for

coordinating the national effort to secure the nation's infrastructure and providing the primary Federal contact for coordinating protection activities, including vulnerability assessments, strategic planning efforts, and exercises.

3.1.2 National Cyber Security Division

The NCSD was created on 6 June 2003 as a part of the DHS, PREP. The NCSD has been charged with coordinating the implementation of the strategy outlined in the National Strategy to Secure Cyber Space, and is partnering with private and public organizations to develop long-term solutions to address the considerable challenges inherent in securing cyberspace.

The NCSD of the DHS consists of five major components: the United States Computer Emergency Readiness Team (US-CERT), Federal Network Security, Network Security Deployment, Global Cyber Security Management, and Critical Infrastructure Cyber Protection and Awareness. The NCSD was established to serve as the federal government's cornerstone for cyber security coordination and preparedness, including implementation of the National Strategy to Secure Cyberspace.

This acquisition is for the ISS for the US-CERT. The US-CERT is the operational arm of the NCSD. US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local government, industry and international partners. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public.

4.0 SCOPE

The scope of this Statement of Work (SOW) includes all integration and systems engineering services necessary to support both the United States Computer Emergency Readiness Team (US-CERT) and the Network Security Deployment (NSD) branches of NCSD. This includes Task Order Management, Systems Integration and Development, Systems Operations and Maintenance, System Engineering Management, and Program Support, 24x7 Incident Handling Team Support, Malicious Code (Malcode) Support, Strategic Analysis Services, Situational Awareness; and Information Support Services. The Government may issue additional tasks under this TO.

4.1 DHS Enterprise Architecture Compliance

Contractors shall comply with DHS Enterprise Architecture requirements when the task order involves tasks to design, develop, or maintain an IT system for a DHS Headquarters or Component program. All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures as they relate to this Statement of Work and associated TOs. Specifically, the Contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware or software shall be compliant with the HLS EA Technology Reference Model (TRM) Standards and Products Profile.
- All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model.

4.2 NCPP Enterprise Architecture Compliance

Contractors shall comply with NCSD/National Cybersecurity & Protection Program (NCPP) Enterprise Architecture requirements when the task order involves tasks to plan, design, develop, implement and maintain National Cybersecurity and Protection System (NCPS) solutions for an NCPP, US-CERT, or their component programs. All solutions and services shall meet NCPP Enterprise Architecture polices, standards, and procedures as they relate to this Statement of Work and associated TOs. Specifically the Contractor shall comply with the following NCPP Enterprise Architecture (NCPP EA) requirements:

- All developed solutions and requirements shall be compliant with the NCPP EA.
- All hardware or software shall be compliant with the NCPP EA Operations Technology Reference Model (OTRM) standards and products profile.
- All data assets, information exchanges and data standards, weather adopted or developed, shall be submitted to the NCPP's System Engineering and Integration (SE&I) Group for review and insertion in the SE&I Data Reference Model

5.0 APPLICABLE DOCUMENTS

1. DOD 5220.22M, National Industrial Security Program Operating Manual
2. DHS MD 4300 Pub, Homeland Security Information Technology Security Program Publication
3. DHS MD 4010.2 Pub, Section 508 Program Management Office and Electronic and Information Technology Accessibility
4. DHS MD 4010.2 Appendix A, Software Applications and Operating Systems
5. DHS MD 4010.2 Appendix B, Web-based Intranet and Internet information and applications
6. DHS MD 4010.2 Appendix C, Telecommunications Products
7. DHS MD 4010.2 Appendix D, Video and Multimedia Products
8. DHS MD 4010.2 Appendix E, Self contained, Closed Products
9. DHS MD 4010.2 Appendix F, Desktop and Portable Computers
10. DHS MD 4010.2 Appendix G, Functional Performance Criteria
11. DHS MD 4010.2 Appendix H, Information, Documentation and Support
12. Homeland Security Critical Information Act of 2002
13. Government Accountability Office (GAO), Testimony Before the House Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity

14. Computer Security Incident Handling Guide
15. Comprehensive National Cybersecurity Initiative Homeland Security Presidential Directive (HSPD) 23/National Security Presidential Directive (NSPD) 54

6.0 TECHNICAL REQUIREMENTS/TASKS

This SOW contains the requirements for multiple tasks that will be awarded upon task order award. The technical requirements, tasks, and deliverables for each task are detailed in the subsections that follow. A consolidated list of deliverables for this SOW is included in Section 9.3 of this SOW, entitled Deliverable/Delivery Schedule. The following is a list and description of each of the tasks and optional tasks for this task order:

6.1 Task Order Management

The Contractor shall serve as a single point of contact and provide task order management for all tasks. This includes development of a Program Management Plan, supporting disciplines and regulatory compliance, performing centralized program management support, and conducting and participating in Program Management Reviews (PMRs). The Contractor shall develop and implement a transition plan for all tasks under this task order. In addition, the Contractor shall assist NSD in responding to questions and requests from other DHS and external organizations. The Contractor shall also perform Continuity of Operations (COOP) and Disaster Recovery (DR) activities as directed by the Government.

6.1.1 Program and Project Management

The Contractor shall develop a Program Management Plan following task order award. The Program Management Plan shall include the statement of objectives; technical approaches; an organizational chart identifying relationships, authorities, responsibilities, and contact information for each individual; the master schedule; a time phased budget schedule; and a description of the management controls that the Contractor shall employ to meet the performance, cost, and schedule requirements of the task order. The Program Management Plan shall also contain a Risk Management Plan that describes the approach that will be used to actively manage risk on the program. The initial Program Management Plan is due 45 days after task order award with a revised Program Management Plan due 30 days following award of Optional Task(s). The Contractor shall provide an updated Program Management Plan annually and shall provide partial updates as mission requirements dictate.

Deliverable: Program Management Plan

6.1.2 Task Order Management

The Contractor shall be responsible for the daily activities required for successful execution of all tasks. The Contractor shall oversee the task order by using vehicles such as status reporting,

quality assurance monitoring, and security management reviews. The Contractor shall prepare and present a Monthly Status Report every 30 days. The Monthly Status Report shall include, but is not limited to, the previous month's progress; the current month's planned progress; issues and recommendations; schedule performance; estimated costs versus actual costs; and program risks, risk mitigation plans, and risk mitigation actions taken.

Deliverable: Monthly Status Report

6.1.3 Support Disciplines and Regulatory Compliance

The Contractor shall employ productivity and management control methods including, but not limited to, Quality Assurance (QA), Configuration Management (CM), and Risk Management. The Contractor shall support NSD with all aspects of DHS AD102 compliance. Additionally, work may involve Federal Information Processing Standards (FIPS), and Federal Laws and Regulations that affect information systems operations. Examples are the Privacy Act of 1974, the Computer Security Act of 1987, and the Financial Systems Integration Office (FSIO) systems requirements. Performance in this area shall entail multiple technical and functional disciplines.

6.1.4 Task Management Support

The Contractor shall provide and perform general administrative, clerical, and other related functions necessary to provide task management of the tasks associated with this task order.

6.1.5 Program Management Reviews

The Contractor shall prepare and present a PMR to the Government on a quarterly basis. The PMR reviews shall address each awarded Task and shall provide detailed performance, schedule, and cost information for the previous quarter. Additionally, each PMR shall address the current quarter's performance and schedule requirements. The PMR review slides shall include, but are not limited to, prior quarter performance, schedule, and cost data; current quarter performance, schedule, and cost data; accomplishments; issues and recommendations; and risks identified and mitigation actions taken.

Deliverable: PMR Slides

6.1.6 Security

The Contractor Program Manager assigned to this task order shall have an active Top Secret (TS)/Sensitive Compartmented Information (SCI) Clearance. All personnel assigned to this task shall be clearable through the TS/SCI level.

6.2 24 X 7 Incident Handling Team Support

The Contractor shall manage and operate an information security incident handling capability on a 24 hour per day/7 days per week basis; perform incident handling; perform incident and security event reporting; and provide surge support for both planned and unplanned contingencies. The Contractor shall provide and manage a complete, comprehensive team of highly qualified technical personnel necessary to perform the work described in this Task. It is anticipated that the Contractor will provide personnel experienced in, but not limited to, current technologies in information systems and network administration; computer security; intrusion detection systems; malcode and anti-virus support; relational database administration, querying, and report generation; and integration of standard office automation tools.

6.2.1 Manage and Operate the 24x7 Incident Handling Capability

The Contractor shall staff, manage, and operate the Incident Handling Capability 24 hours per day, seven days per week. The Contractor shall staff the 24x7 Incident Handling Capability with a minimum of two personnel specializing in incident handling at all times.

6.2.2 Track, Handle, and Report

The Contractor will track, handle, and report all security events and computer incidents in accordance with government procedures. This includes, but is not limited to, both Level 1 and Level 2 computer incidents. To efficiently facilitate and expedite the tracking, handling, and reporting of all security events and computer incidents, the Contractor shall coordinate with relevant organizations, which include, but are not limited to, U.S. government agencies; state and local governments; critical infrastructure owners and operators; and international governments.

6.2.3 Perform Tracking Using the Government Tracking System

The Contractor shall perform tracking of all reported security events and incidents using the government tracking system. In addition, the Contractor shall document the resolution of each security event or incident using the government tracking system.

6.2.4 Escalation

The Contractor shall perform escalation of warranted security events and incidents in accordance with government procedures.

6.2.5 Assist in Restoration Efforts

For each security event or incident requiring restorative services, the Contractor shall assist in restoration efforts by providing technical guidance; coordinating recovery efforts; archiving relevant information; and reporting status information to government personnel.

6.2.6 Follow Government Resolution and Escalation Procedures

Whenever incidents or security events require resolution, the Contractor shall follow Government resolution and escalation procedures. Whenever possible, problem resolution will occur within the Incident Handling Team. In situations where this is not possible, the Contractor shall escalate the request in accordance with Government procedures.

6.2.7 Identify Patterns in Reported Compromises

For all incidents reported, the Contractor shall identify patterns in reported compromises and identify additional compromises as part of the same incident. The Contractor shall document all information associated with a particular incident. Using a government provided format, the Contractor shall draft and submit complaint letters to the Government for approval. Following government approval, the Contractor shall transmit finalized complaint letters to various organizations for action.

Deliverables: Draft and Final Complaint Letters

6.2.8 Monitor Other Agency Internet Infrastructures

The Contractor shall monitor the general health and welfare of other federal government agencies' internet infrastructures. To perform this, the Contractor shall perform monitoring of both the systems and networks of federal government agencies. The Contractor shall use government provided tools and use sensor data to correlate events and conduct trend analyses of anomalous events identified through monitoring. This includes, but is not limited to, determining port and protocol events and internet traffic anomalies.

6.2.9 Perform Other Duties as Necessary

The Contractor shall perform other duties as necessary to efficiently and effectively manage and operate the Incident Handling Capability on a 24 hours a day, seven days a week basis. Other duties include, but are not limited to, arranging shift schedules, distributing tasks, and organizing teams.

6.2.10 Reduce Risk and Facilitate Continuous Improvement

To reduce risk and facilitate continuous improvement, the Contractor shall identify all processes involved in the management and operation of 24x7 Incident Handling Capability. The Contractor shall submit this list to the Government for approval. Once approved, the Contractor shall document all processes on the list involved in the management and operation of the 24x7 Incident Handling Capability in accordance with a government provided format. This includes, but is not limited to, triage, incident handling, analysis and trend reporting, monitoring networks and systems, anti-virus support responses, re-direction to applicable security resources, security

vulnerability information dissemination, and incident reporting. The government will have 60 days to review and comment on the draft processes. The Contractor shall submit final Incident Handling Capability processes to the Government 270 days after task order award.

Deliverables: Incident Handling Capability Process List, Draft Incident Handling Capability Processes, Final Incident Handling Capability Processes.

6.2.11 Report on Security Incidents (Daily and Weekly Basis)

The Contractor shall report on security incidents and events on a daily and weekly basis in accordance with government procedures. On a daily basis, the Contractor shall prepare operational status slides using a government provided format. On a weekly basis, the Contractor shall prepare assessments, reports, and weekly trends of incident and security events using a government provided format. Following Government approval, the Contractor shall then disseminate these reports across the federal, state and local governments, and U.S. critical infrastructures. During off-peak hours, the Contractor shall prepare additional status reports, assessments, and reports and, following Government approval, disseminate these to facilitate coordination and dissemination of information to other federal, state, and local governments and U.S. critical infrastructures.

Deliverables: Operational Status Slides, Assessments, Status Reports, Trends of Incident and Security Events

6.2.12 Provide Planned and Unplanned Contingency Support

In the event of a contingency, the Contractor shall provide contingency support on both a planned and unplanned basis to support an increased workload. Contingency support will be for both major planned exercises and actual crisis operations. For exercise support, the Contractor shall provide additional assistance as directed by the government. For actual contingency operations, staffing requirements may increase dramatically during a contingency, typically lasting for less than a three-week period. To minimize disruption of existing tasks, during the contingency, the Contractor shall provide additional personnel, with active clearances, for the duration of any contingency. In the event of unplanned contingency operations, as directed by the government, the Contractor shall present a staff augmentation plan to the Government Contracting Officer (CO) for approval. In the plan, the Contractor shall highlight any additional funding requirements above the current task authorization.

Deliverables: Contingency Staff Augmentation Plan (as required)

6.2.13 Security

All personnel assigned to 24 X 7 Incident Handling Team Support task shall possess an active TS clearance and be clearable through the TS/SCI level.

6.3 Malicious Code Support

The Contractor shall manage and operate the US-CERT Malicious Code Laboratory. The Contractor shall develop procedures to analyze and categorize malcode; perform detailed analysis and characterization of malcode; produce reports on trends in malcode; develop and implement processes to keep US-CERT and others abreast of malcode developments; maintain a working inventory of tools and processes; and organize and maintain a collection of malcode in a safe environment separate from operational systems.

The Contractor shall provide and manage a complete, comprehensive team of highly qualified technical personnel necessary to perform the work described in this Task. The Contractor shall assign personnel to this Task proficient in topics of interest related to malcode including, but not limited to, automatic detection and characterization; reactive countermeasures; proactive defenses; threat assessment; damage assessment; reverse engineering; and roBOT NETworks (BOTNETs). In addition, the Contractor shall provide personnel experienced in, but not limited to, current technologies in information systems and network administration; computer security; intrusion detection systems; malcode and anti-virus support; and relational database administration, querying, and report generation.

6.3.1 Manage and Operate the Malicious Code Laboratory

The Contractor shall operate the US-CERT Malicious Code Laboratory. The Contractor shall establish procedures to analyze and categorize software code for malicious intent. The Contractor shall operate the Malicious Code Laboratory, including the design of the analytical tools and the analysis of malcode in both static and dynamic (run-time) environments.

Deliverables: Analytical Procedures

6.3.2 Analyze and Categorize Malicious Code

The Contractor shall analyze and categorize malcode. At a minimum, the analysis and categorization shall consider obfuscation and armoring techniques, vulnerability exploits, distribution and propagation techniques, potential damage, and impacted operating environments. The Contractor shall work within the government and commercial community of expertise to plan appropriate action in response to specific instances of malcode. The Contractor shall coordinate with the IT security community to determine the extent of potential damage, work with the community to identify the appropriate responses, and issue warning products.

Deliverables: Analytical Reports

6.3.3 Perform Detailed Analysis and Characterization

The Contractor shall perform detailed analysis and characterization of malcode to adequately identify or corroborate specific dangers and threats to critical infrastructure.

Deliverables: Analytical Reports

6.3.4 Track Trends and Develop and Implement Processes

The Contractor shall track trends in malcode development and develop and implement processes to keep US CERT personnel and others current on malcode developments and trends. The Contractor shall write, produce, and distribute timely information papers covering topics of concern in malcode.

Deliverables: Malcode Trend Reports

6.3.5 Maintain a Working Inventory of Tools and Processes

The Contractor shall maintain a working inventory of tools and processes for the identification and analysis of code for malicious intent. The Contractor shall operate and maintain tools in a working environment as necessary for analysis. The Contractor shall establish and maintain effective working relationships with other government and industry organizations concerned with the investigation of malcode to keep abreast of new tools and processes used by other organizations.

Deliverables: Analytical Tools Inventory and Analytical Processes Inventory

6.3.6 Organize and Maintain a Collection of Malicious Software

The Contractor shall organize and maintain a collection of malicious software (malware) in a safe environment that is maintained separate from operational systems.

Deliverable: Malware Inventory

6.3.7 Security

All personnel assigned to the Malicious Code Support task shall be clearable through the TS/SCI level.

6.4 Strategic Analysis Services

The Contractor shall perform strategic analysis of incidents and analysis of sophisticated cyber attack patterns over extended periods of time. The Contractor shall conduct detailed technical analysis of incidents; computer autopsies and forensics; participate in working groups; and conduct and participate in technical briefings. The Contractor shall provide technical analysis; data fusion; data trend monitoring; emergency response team services; community of interest analysis cell services; reverse engineering services; network analysis tools evaluation and integration services; and operational metrics support services.

6.4.1 Technical Analysis

The Contractor shall conduct detailed technical assessments of emerging policy, technical plans, program documents, and on-going analysis projects. The Contractor shall conduct system analysis of, as examples, a technical review involving the contents of a compromised system; reverse engineering unusual files and data; or, the identification and documentation of the tactics, techniques, and procedures used by an attacker to gain unauthorized system access. The Contractor shall conduct technical reviews of data originating from or reflecting status of ongoing intrusions and document the findings of apparent activities involved and any intrusive or damaging traffic leading to or from the compromised host.

Deliverable: US-CERT Technical Report

6.4.2 Data Fusion

The Contractor shall support data fusion from various data inputs to include reported intrusions, sensor inputs, network status, open source, and law enforcement and intelligence inputs. The Contractor shall also provide incident handling support for incident detection, analysis, and coordination and response.

Deliverable: Incident Handling and Analysis Report

6.4.3 Data Trend Monitoring

The Contractor shall monitor data trends from intrusion detection systems and traffic analysis tools. The result of this monitoring will be an analysis of potential compromises and emerging threats. Information concerning potential compromises, emerging threats, and traffic patterns shall be identified and documented in Federal Information Notices (FINs) and Critical Infrastructure Information Notices (CIINs). Contractor prepared FINs and CIINs shall provide both technical and non-technical information for wide dissemination purposes.

Deliverables: FINs, CIINs

6.4.4 Emergency Response Team Services

Contractor personnel shall participate in rapid emergency response team deployments for on-site support requirements. The Contractor shall identify and maintain a roster of personnel to support this requirement. Generally, the government will provide a minimum of 12 hours notification prior to deployment. Deployment may be to areas in the process of disaster recovery and may be for extended periods of time.

Deliverable: Deployment Personnel Roster

6.4.5 Community of Interest Analysis Cell Services

Contractor personnel shall be teamed into community of interest analysis cells. Personnel shall maintain consistent dialogue with community of interest organizations. Personnel may be required to attend conferences and on-site orientation. Contractor personnel assigned as Strategic Analysts shall serve as a liaison and advocate for their respective cells by: 1) ensuring strategic analysis products produced by the US-CERT are distributed throughout the cells; 2) detecting trends throughout their cells; and 3) providing a thorough and comprehensive analysis on the state of their respective cell including creating detailed reports and briefings. Analysis cells will include, but are not limited to, organizations within the federal government, state/local government, and critical infrastructure and international counterparts.

6.4.6 Reverse Engineering Services

The Contractor shall be tasked with reverse engineering of malware code, tool evaluations, and analysis as a result of proliferation of new techniques and tools. The Contractor shall be tasked to analyze software code applications, scripts, and processes using the resources of the US-CERT Malicious Code Laboratory to evaluate and assess the technical operations. The Contractor shall prepare Reverse Engineering Reports and Reverse Engineering Briefings as required.

Deliverables: Reverse Engineering Report, Reverse Engineering Briefing

6.4.7 Network Analysis Tools Evaluation and Integration Services

The Contractor shall participate in the identification, evaluation, and integration of existing and future network analysis tools to be used by US-CERT Operations.

6.4.8 Operational Metrics Support Services

The Contractor shall develop, maintain, and automate operational metrics in support of US-CERT. The metrics shall include both internal and external metrics to assess operational performance and effectiveness.

6.4.9 Security

All personnel assigned to the Strategic Analysis Services task shall possess an active TS/SCI clearance.

6.5 Situational Awareness (EINSTEIN)

The Contractor shall incrementally provide a global situational awareness capability; support the development and evolution of current and future data collection and collaboration technologies;

support the development of network sensor requirements specifications and operations architecture; perform verification, validation, and delivery of enhanced capabilities; and provide production support necessary to incorporate new capabilities and systems into DHS operational environments.

The Contractor shall provide and manage a team of highly skilled personnel, experienced in, but not limited to information assurance, systems programming, systems administration, infrastructure engineering, network security, analysis, situational awareness, test and evaluation, and new and emerging technologies in the areas of data collection and collaboration, network sensors, and global situational awareness.

NPPD plans to migrate the EINSTEIN production environment from the Pensacola Naval Air Station to a DHS Enterprise Data Center. The Contractor shall assist with migration planning and execution when requested by the COTR. The Contractor shall continue to meet the requirements of this SOW regardless of the location of the EINSTEIN production environment at no additional costs.

6.5.1 Global Situational Awareness Capability

The Contractor shall analyze, design, develop, deploy, and incrementally enhance the information assurance collection management system and the tools required to provide a Global Situational Awareness (GSA) capability to DHS, NCSD, and US-CERT. The Contractor shall plan, develop, and implement a system that will provide information "collectors" and collaboration tools for the delivery of information to DHS, NCSD, US-CERT, and participating customers. Additionally, the Contractor shall produce a consolidated situational view capability, to reside at a US-CERT site, with the ability to allow views of definable subsets of data. The Contractor shall support information requirements development, submission, and coordination through the US-CERT approval and validation process. In addition, the Contractor shall coordinate with the all DHS, NCSD, and US-CERT approved sectors, agencies, components, and disciplines regarding the deployment and operation of situational awareness capabilities. The Contractor shall document and deliver the requirements, design, code, user, and version description documentation to the Government. Following Government review, the Contractor shall update all documentation developed under this task.

6.5.2 Development of Data Collection and Collaboration Technologies

The Contractor shall elicit and develop the requirements (including operational requirements) needed by the DHS, NCSD, and US-CERT to support the development and migration of current and future high-speed, passive Data Collection and Collaboration Technologies (DC&C). The Contractor shall develop, document, and integrate these technologies with pre-existing programs and interfaces, to the maximum extent possible, to minimize requirements changes with current and future customers. Following Government review, the Contractor shall update all documentation developed under this task.

6.5.3 Network Sensor Requirements Specification and Operations Architecture

In conjunction with the Product Development Support effort, the Contractor shall develop the requirements specifications and operations architecture needed by the product engineers to support the integration, throughput, and security requirements of current and future Network Sensor (NS) technologies or other sensors into existing DHS and other agency infrastructures. The Contractor shall monitor the operations architecture to identify and subsequently develop any required enhancements to improve interface capabilities with the DHS management system. The requirements specification, operations architecture, and developed enhancements shall encompass the health, welfare, and security of the "sensors" and other deployed systems as well as an identification of coverage areas (e.g. the Internet Protocol (IP) address range the sensor is watching compared with the total IP space owned and leased by a particular office/agency) and decomposed into community of interests defined by the government. Following Government review, the Contractor shall update all documentation developed under this Task.

6.5.4 Verification, Validation, and Delivery of Enhanced Capabilities

Prior to delivery of any enhanced capability or system to the operational environment, the Contractor shall thoroughly verify, test, and validate any enhanced capability or system developed under this task. The Contractor shall deliver and install all equipment in up to, and including, four geographically dispersed operational environments.

6.5.5 Production Support for the Operational Environment

The Contractor shall support all facets of integrating new systems and capabilities into the operational environment in up to, and including, four geographically dispersed sites. This includes, but is not limited to, installation, on-going maintenance, occurrence and event investigation, and root cause analysis for both production systems and peripheral equipment. The Contractor shall perform root cause analysis to identify systemic problems, implement corrective actions, and identify future improvements to operations. The Contractor shall document lessons learned on a quarterly basis. The Contractor shall minimize downtime by providing personnel on an on-call basis, 24 hours per day, seven days per week. The Contractor shall provide full DR and COOP support for all systems and capabilities delivered under this task.

6.5.6 Security

All personnel assigned to the Situational Awareness (EINSTEIN) task shall be clearable through the TS/SCI level.

6.5.7 Deliverables

The contractor shall develop or provide input to the following acquisition and system engineering documents. The delivery schedule will be mutually agreed to by the government and the contractor as required to enable the government to meet the requirements of DHS Acquisition Directive 102-01.

Deliverables: Analysis of Alternatives, Capability Development Plan, Data Architecture Document, Data Management Plan, Deployment Plan, Developmental Test Plan, Integrated Logistics Support Plan, Lifecycle Cost Estimate, Lessons Learned Document, Logical Design Document, Project Management Plan, Site Prep Plan, System Design Document, and Version Description Document

6.6 Information Support Services

The Contractor shall support development, implementation, and maintenance of information services, products, and reports and shall develop and maintain operating procedures; produce daily reports of computer security events and incident statistics; prepare quarterly Federal Information Security Management Act (FISMA) reports of computer security events and incident statistics; review and update documentation; and provide exercise support services. The Contractor shall also support developing and disseminating processes for daily, quarterly, and annual reports via the US-CERT portal and the US-CERT internet site.

6.6.1 Operating Procedures

The Contractor shall support the development, refinement, and standardization of operating procedures between the US-CERT, DHS, federal government Information Sharing Analysis Centers (ISAC), and international partners. Performance shall include visits to both U.S. government and foreign government Computer Security Incident Response Centers (CSIRC)/CERT and participation in unclassified and classified teleconferences, Video Teleconferences (VTC), and other meetings related to this task.

Deliverables: CSIRC/CERT Visit Report

6.6.2 Computer Security Events/Incident Statistics

The Contractor shall prepare daily reports of computer security events/incident statistics including, but not limited to:

- a breakout of incidents;
- federal agencies, state/local governments, and critical infrastructures affected; and
- the status of ongoing activities.

The information contained in the reports shall include, but is not limited to:

- incident trends;
- analysis of traffic patterns;
- vulnerability statistics; and
- malcode trends and outbreaks.

Deliverables: Computer Security Event/Incident Statistics Report

6.6.3 Federal Information Security Management Act Report

The Contractor shall prepare quarterly FISMA reports of computer security events and incident statistics including a breakout of incidents affecting federal agencies and sub agencies for each unique government agency and analysis of the activities during the past quarter. The information contained in the reports shall include, but is not limited to:

- incident trends;
- analysis of traffic patterns;
- vulnerability statistics; and
- malcode trends and outbreaks.

Deliverables: FISMA Report

6.6.4 Review and Update Services

The Contractor shall be responsible for review and update of documentation, including, but not limited to:

- Standard Operating Procedures (SOP);
- internal operational processes;
- manuals; and
- other US-CERT documentation.

The Contractor shall gather necessary information from US-CERT personnel, other DHS employees, and relevant references. The Contractor shall create and arrange system files and folders that contain US-CERT documentation. The Contractor shall develop, write, format, and edit technical and non-technical information for reports, manuals, procedures, processes, briefs, and other forms of documentation.

Deliverables: SOPs Updates, Internal Operational Processes Updates, Manual Updates, Other US-CERT Documentation Updates

6.6.5 Exercise Support Services

Exercise Support falls under the Plans Policy Coordination Program which also entails the International Support function.

The Contractor shall represent the US-CERT in various exercise scenarios, and, as directed by the Government, will act on behalf of the US-CERT. Contractor personnel supporting this requirement shall be highly knowledgeable and experienced in Security Operations Center functions and responsibilities. Travel involved for Exercise Support shall involve primarily Continental US (CONUS) travel, but may also include Outside Continental US (OCONUS) travel. The duration of most exercises is approximately three days but may be longer depending on level of participation and type of exercise. Contractor personnel supporting this requirement may be required to support the Initial Planning Phases and Final Planning Conferences. The Contractor shall maintain and manage a staff, whose knowledge and skills include, but is not limited to, writing; review and editing technical documents for flow, errors, logic, and overall consistency with other related documents; ability to prioritize, multi-task, and work with teams to meet deadlines; document project plans and timelines; knowledge of Critical Infrastructure and interdependencies and cyber security vulnerabilities and solutions; background in Network Security Operations, and development of exercise scenarios, plans, and policies.

Currently, the International Support function consists primarily of planning and policy development. The intent of the program is to provide outreach support to the various international CSIRCs in support of US-CERT operations. The Contractor shall develop information sharing protocols in accordance with current Federal guidelines. Some OCONUS travel may be required in support of this effort to meet with International CSIRC organizations to develop information sharing protocols.

The Contractor shall prepare periodic briefings and after action plans and reports. Planning exercises with other agencies may involve integration into each organization's operational tactics, techniques, procedures, and personnel. In conjunction with other organizations, the Contractor shall provide technical and organizational skills to respond to realistic computer defense scenarios for exercises.

Deliverables: Periodic Briefings, After Action Plans and Reports

6.6.6 Security

All personnel assigned to the Information Support Services task shall be clearable through the TS/SCI level.

6.7 Transition Planning Services

The Contractor shall develop, document and monitor the execution of a transition plan that may be used to transition tasks and materials to a new Contractor, or to the Government. The plan will incorporate an inventory of all services and materials developed that will be required to fully perform the services provided under this contract. The plan will include a schedule of briefings, including dates and time and resources allotted, that will be required to fully transition all materials developed to the follow-on Contractor, and will provide the names of individuals that will be responsible for fully briefing their follow-on counterparts. The plan is to ensure that the follow-on Contractor, or the Government, will be provided sufficient information and be fully

briefed prior to the current expiration date of the contract, to provide adequate time for the new Contractor to have their personnel completely familiar with the requirements and in place on the turnover date. The Contractor shall plan for a 30 day(s) transition period. The plan shall provide the contact information for contractor individuals who will be assigned to the transition team and identify their roles in the transition.

The Contractor shall participate in transition meetings with the program manager and project staff, and representatives of the successor Contractor. The purpose of these meetings is to review project materials and take preparatory steps to ensure an effective transition in Contractor support. The transition plan is due to the Government 60 days prior to the expiration date of the contract.

Deliverable: Transition Plan

7.0 WORKSPACE SERVICES

The Contractor shall provide the necessary services to support Network Security Deployment Integrated Project Teams (IPT), Working Groups, and Review Teams necessary to conduct NCPS development and deployment.

8.0 SURGE SUPPORT

As determined necessary and approved by the Government, the Contractor shall provide additional support. The Contractor shall seek Government approval in advance of incurring any costs associated with surge support. Government approval shall be authorized by the Contracting Officer. The Contractor may be required to work more than 8 hours during a business day, or when operational conditions require continuous staffing 24 hours per day, 7 days per week to support operations during emergency conditions throughout the CONUS, as specified by the Government. The Contractor shall provide knowledgeable, skilled, cleared personnel to augment the Government staff. The Government will define the work to be performed, working hours, security requirements, and duration of assignment.

9.0 DELIVERABLES

The Contractor shall ensure the accuracy, functionality, completeness, professional quality, and overall compliance with government guidelines and requirements of all deliverables. Working copy products may be provided by email or disk as arranged with the Government Task Lead.

9.1 Format of Deliverables

Final documentation deliverables shall be provided in hard and soft copy using Microsoft (MS) Office products as specified below. Daily, weekly, interim, informal deliverables, and working-copy products may be provided by email or disk.

- Final soft copy: Developed using the current DHS version of Microsoft Word, Power Point, and/or other standard application software and provided on a CD-ROM disk. If more than one deliverable is provided at the same time, deliverables may be included on the same disk.
- Final hard copy: Typewritten on 8-1/2"x11" white paper. The Contractor shall not use spiral binding or other binding that interferes with photocopying.

9.2 Acceptance and Rejection Procedures of Draft and Final Deliverables

- **Acceptance .** The COTR and/or the alternate COTR will review all draft and final deliverables to ensure accuracy, functionality, completeness, professional quality, and overall compliance with the guidelines/requirements of the task. The Contractor shall ensure the accuracy and completeness of all deliverables in accordance with referenced policy, regulations, laws, and directives. Reports and presentations shall be concise and clearly written. Errors, misleading or unclear statements, incomplete or irrelevant information, and/or excessive rhetoric, repetition, and "padding", or excessive length if a page limit is imposed, shall be considered deficiencies and will be subject to correction by the Contractor at no additional cost to the Government. Unless otherwise indicated in the task descriptions, the Government will require 20 workdays to review and comment on deliverables. If the deliverable does not meet the noted criteria, the Government will return it to the Contractor for revision.

- **Rejection Procedures.** A rejected deliverable will be handled in the following manner:

  - After notification that the deliverable did not meet the acceptance criteria, the Contractor shall resubmit an updated/corrected version 15 workdays after receipt of Government comments.
  - Upon re-submission by the Contractor, the Government will reapply the same acceptance criteria. If the deliverable does not meet the acceptance criteria a second time, the Government might consider the Contractor as having deficient performance with respect to the subject task.

9.3 Deliverable/Delivery Schedule

Task	Description	Deliverable Description	Due
6.1	**Task Order Management Services**	Program Management Plan	45 Days; 30 Days Following Award of New Task Order
		Monthly Status Report	Monthly
		Program Management Review (PMR) Slides	Quarterly

Task	Description	Deliverable Description	Due
6.2	**24 X 7 Incident Handling Team Support**	Draft Complaint Letters	As required
		Final Complaint Letters	As required
		Incident Handling Capability Process List	60 Days
		Draft Incident Handling Capability Processes	180 Days
		Final Incident Handling Capability Processes	270 Days
		Operational Status Slides	Daily
		Assessments	Weekly
		Status Reports	Weekly
		Trends of Incident and Security Events	Weekly
		Contingency Staff Augmentation Plan	As required
6.3	**Malicious Code Support**	Analytical Procedures	120 Days
		Analytical Reports	As required
		Malcode Trend Reports	As required
		Analytical Tools Inventory	Quarterly
		Analytical Processes Inventory	180 Days
		Malware Inventory	Quarterly
6.4	**Strategic Analysis Services**	US-CERT Technical Report	As required
		Incident Handling and Analysis Report	As required
		Federal Information Notices (FINs)	As required
		Critical Infrastructure Information Notices (CIINs)	As required
		Deployment Personnel Roster	As required
		Reverse Engineering Report	As required
		Reverse Engineering Briefing	As required
6.5	**EINSTEIN**	Analysis of Alternatives	As required
		Capability Development Plan	As required
		Data Architecture Document	As required
		Data Management Plan	As required
		Deployment Plan	As required
		Developmental Test Plan	As required
		Integrated Logistics Support Plan	As required
		Lesson Learned Document	Monthly
		Lifecycle Cost Estimate	As required
		Logical Design Document	As required

Task	Description	Deliverable Description	Due
		Project Management Plan	As required
		Site Prep Plan	As required
		System Design Document	As required
		Version Description Document	As required
6.6	**Information Support Services**	CSIRC/CERT Visit Report	15 Days following CSIRC/CERT Visit
		Computer Security Event	Daily
		Incident Statistics Report	
		FISMA Report	Quarterly
		SOP Updates	Quarterly
		Internal Operational Processes Updates	Quarterly
		Manual Updates	Quarterly
		Other US-CERT Documentation Updates	Quarterly
		Periodic Briefings	As required
		After Action Plans and Reports	As required
6.7	**Transition Planning Services**	Transition Plan	60 days prior to expiration of this task order

10.0 PERIOD OF PERFORMANCE

The period of performance for this effort is eleven (11) months from the date of award.

11.0 PLACE OF PERFORMANCE

The principal place of performance is the Department of Homeland Security's NCSD facility at 1110 N. Glebe Road, Arlington, VA 22201. In the interim, as DHS renovates their facilities, contractors working may be asked to work from contractors' facilities when adequate workspace is not available at the government site.

The Contractor shall maintain an office within a 25 mile radius of Washington, D.C. Some of the work performed under this task order will require CONUS travel. A portion of the work performed under this task order will require OCONUS travel.

Relocation to alternate work sites shall be performed as emergencies and preparedness activities dictate.

12.0 TRAVEL REQUIREMENTS

The Contractor shall perform all travel required to perform this task order and shall be reimbursed for all actual costs incurred for the required travel in accordance with the Federal Travel Regulation (FTR). Each planned trip must be approved by the Contracting Officer Technical representative (COTR) in advance.

13.0 OTHER DIRECT COSTS

The Contractor shall seek Government approval in advance of incurring any costs associated with Other Direct Costs (ODCs). Government approval is provided by the head of the program office, the CO, and the COTR. The Contractor shall provide estimated costs, including any quotes, with its approval request. Allowable and reasonable costs incurred by the Contractor for ODCs will be reimbursed. The Contractor shall not charge the Government for any associated fees or profit over the actual costs incurred for ODCs.

Allowable ODCs that are necessary and directly support task order work include, but are not limited to, computer products including laptops, printers, monitors, and task order applicable software; materials for meetings; reproduction, graphics, and conference/seminar fees; recruiting, trade journal, broadcasts, and Internet advertising; exhibits and marketing/communications products; and conference booth fees.

Where equipment or software is necessary to support the cyber operations and the Government is not able to provide the equipment or software in a timely manner, the Contractor shall furnish the necessary items.

The Contractor shall provide receipts to the Government for each ODC incurred.

14.0 GOVERNMENT FURNISHED INFORMATION AND EQUIPMENT

The Government shall provide the Contractor with the following Government Furnished Information and Equipment as specified below.

14.1 Government Furnished Information (GFI)

The Government will furnish the Contractor with the following information in support of this task order:

1) DOD 5220.22M National Industrial Security Program Operating Manual, current publication
2) Contractors Quality Assurance Procedures, current publication
3) Critical Information Act of 2002, current publication
4) DHS Enterprise Architecture Guide (when available)
5) DHS/NCSD/US-CERT will provide the Contractor with appropriate access to information to accomplish the assigned tasks. All Government supplied information will

remain proprietary to the Government. Additionally, vendor proprietary information supplied as a result of any resulting task order may require the execution of Non-Disclosure Agreements between the Contractor and respective vendor.

6) Purchase, Licensing, and Maintenance Agreements for MOE Support (Optional Task).

14.2 Government Furnished Equipment (GFE)

The Government will furnish the Contractor with the following equipment access in support of this task order:

0) Work space, with at least one workstation and telephone for individuals assigned full time at the 1110 N. Glebe Road, Ballston, VA facility
1) Containers for storage of documentation and references
2) Access to a photocopier
3) Access to printers (Black and White and Color)
4) Access to a scanner
5) Access to the Information Sharing and Analysis System (ISAS) and other applicable tools
6) Tools required for the identification, handling, tracking, and reporting of security events and incidents for 24x7 Incident Handling
7) Tools required for the identification, tracking, analysis, and reporting of malicious code for Malcode Support
8) Tools required for support and maintenance for MOE Support (Optional Task).

15.0 OTHER PERTINENT INFORMATION OR SPECIAL CONSIDERATIONS

15.1 Identification of Potential Conflicts of Interest (COI)

There have been no COI identified.

15.2 Identification of Non-Disclosure Requirements

Some material will contain proprietary, sensitive, or classified data from various public or private sources. The Contractor shall require all Subcontractors to sign corporate and individual non-disclosure agreements.

15.3 FAR 52.227-14, Rights in Data – General

This section is incorporated by reference. All specified draft and final deliverables become the property of US-CERT. To the extent provided by clause 52.227-14, the details of any and all security countermeasures that the Contractor may develop under this task order, including

software, will become the property of US-CERT.

16.0 ENHANCED SKILLS TRAINING

In the event a Contractor submits a request to attend training that provides direct benefit to the work being performed by that Contractor under their specific task, the Contractor may request the Government Program Manager approve attendance on a case-by-case basis. In the event the Government Program Manager does not approve funds for the Contractor tuition, per diem, and/or travel costs, but approves the training, the Contractor may submit a request to bill the Government for the labor hours to attend training. All requests of this nature are reviewed by the Government Program Manager and approved/disapproved on a case-by-case basis.

17.0 PERSONNEL QUALIFICATIONS

The Contractor shall be responsible for employing technically qualified personnel to perform the work specified in this SOW. The Contractor shall maintain the personnel, organization, and administrative control necessary to ensure that the work delivered meets the Government's specifications and requirements. The work history of each Contractor employee must contain experience directly related to work he/she is required to perform under this task order.

The Government reserves the right, during the life of this order, to request work histories on any Contractor employee for the purpose of verifying compliance with the above requirements.

Specific Personnel Qualifications Requirements – Personnel required to perform the services set forth herein shall meet the minimum qualifications for the respective labor categories identified in the Contractor's Enterprise Acquisition Gateway for Leading-Edge Solutions (EAGLE) task order.

18.0 ACCESSIBILITY REQUIREMENTS

Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998, requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to and use of information and services that is comparable to the access and use available to non-disabled Federal employees and members of the public.

18.1 Applicable Standards

All Electronic Information Technology (EIT) deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable standards have been identified:

- 36 CFR 1194.21 – Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to Government Off The Shelf (GOTS) and Commercial Off The Shelf (COTS) software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22. This standard does not apply for the programming within Malicious Code Support unless a user interface results from the task. For instance, an executable "update" or "patch" requiring user input shall apply this standard.

- 36 CFR 1194.22 – Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX), then "1194.21 Software" standards also apply to fulfill functional performance criteria.

- 36 CFR 1194.23 – Telecommunications Products. This applies to all telecommunications products including end-user interfaces such as telephones and non end-user interfaces such as switches or circuits that are procured, developed, or used by the Federal Government.

- 36 CFR 1194.24 – Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available. Specifically, any training procured or developed under this work statement that utilizes video or multimedia.

- 36 CFR 1194.31 – Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverables shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

- 36 CFR 1194.41 – Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required "1194.31 Functional Performance Criteria", they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum.

18.2 Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein shall be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified

the following exceptions that may be applied:

- 36 CFR 1194.2(b) – (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some, but not all of the standards, the agency must procure the product that best meets the standards.

  When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires approval from the DHS Office on Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

- 36 CFR 1194.3(b) – Incidental to Contract, all EIT that is exclusively owned and used by the Contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service, or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those Contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

- 36 CFR 1194.3(f) – Back Office, applies to any EIT item that will be located in spaces frequented only by service personnel for maintenance, repair, or occasional monitoring of equipment. This exception does not include remote user interfaces that are accessible outside the enclosed "space".

19.0 SECURITY REQUIREMENTS

Any work performed at 1110 North Glebe Road is subject to DHS security requirements.

19.1 General

For proposal and source selection purposes, the Contractor will be required to have personnel cleared at the TS/SCI Clearance level.

Contractor's request for visit authorization shall be submitted in accordance with the 1110 Glebe Road, Ballston, Virginia Visitor's Policy. Upon request, a copy of this policy will be provided.

19.1.1 Additional Information for Classified Contracts

Performance of this contract requires the Contractor to gain access to classified National Security Information (includes documents and material). Classified information is Government information which requires protection in accordance with Executive Order 12958, National Security Information (NSI) as amended and supplemental directives.

The Contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, an attachment in the contract, and the National Industrial Security Program Operating Manual (NISPOM) for protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service. If the Contractor is required to have access to classified information at a DHS or other Government Facility, is shall abide by the requirements set forth by the agency.

19.1.2 General Requirement

The Contractor shall ensure these instructions are expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this contract.

19.2 Contractor Personnel

19.2.1 Employment Eligibility

To comply with the requirements HSAR Clause 3052.204-71, and Department policy, the Contractor must complete the following forms for applicable personnel who will be performing work under this contract as indicated:

- Standard Form (SF) 85P, "Questionnaire for Public Trust Positions"
- FD-258 fingerprint cards
- DHS Form 11000-6, "Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement" is required of all applicable Contractor personnel.
- DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act (FCRA)"

19.2.2 Continued Eligibility

The Contra ting Officer may require the Contractor to prohibit individuals from working on contracts if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence or security concerns.

19.3 Termination

The DHS Security Office shall be notified of all terminations/resignations within five (5) days of

occurrence. The Contractor shall return to the Contracting Officer's Technical Representative (COTR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to e returned, a report shall be submitted to the COTRE, referencing the pass or card number, name of individual to whom it was issued and the last known location and disposition of the pass or card.

19.4 Suitability Determination

DHS may, as it deems appropriate, authorize and make a favorable Entry On Duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to facilities or information at any time during the term of the task order. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Security Office.

Contractor employees waiting for an EOD decision may begin work on the contract provided they do not access sensitive Government information. Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by a Government employee. This limited access is to allow Contractors to attend briefings, non-recurring meetings, and begin transition work.

19.5 Background Investigations

Contractor employees (to include applicants, temporary, part-time, and replacement employees) under this task order needing access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the task order. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through DHS Security Office. Prospective Contractor employees shall submit the following completed forms to the Security Office through the COTR no less than 30 days before the starting date of the task order or 30 days prior to Entry On Duty of any employees whether a replacement, addition, subcontractor employee, or vendor:

- Standard Form (SF) 85P, "Questionnaire for Public Trust Positions"
- FD-258 fingerprint cards (2 copies)
- DHS Form 11000-6, "Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement"
- DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act (FCRA)"

Only complete packages will be accepted by the DHS Security Office. Specific instructions on submission of packages will be provided upon award of the contract.

Be advised that unless an applicant requiring access to sensitive information has resided in the United States for three of the past five years, the Government may not be able to complete a satisfactory background investigation. In such cases, DHS retains the right to deem an applicant as ineligible due to insufficient background information.

Non-US citizens shall not be authorized to access or assist in the development, operations, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

1. The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;
2. There must be a compelling reason for using this individual as opposed to a U.S. citizen; and,
3. The waiver must be in the best interest of the Government

19.6 Alternative Citizenship Requirements for Non-IT Contracts

For non-Classified or non-IT contracts, the above citizenship provision shall be replaced with the citizenship provision below:
Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-55 1). Any exceptions must be approved by the Department's Chief Security Officer or designee.

19.7 Information Technology Security Clearance

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in DHS IT Security Program Publication DHS MD 4300.Pub. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

19.8 Information Technology Security Training and Oversight

Before receiving access to IT resources under this contract the individual must receive a security

briefing which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS

19.9 References

19.9.1 DHS Office of Security

DHS, Office of Security
Personnel Security Staff
Attn: Christal Fulton
Washington DC 20528
Telephone [redacted] (b)(6)

20.0 INVOICES

Contractor shall invoice monthly and provide detail for Labor charges, Other Direct Costs, and Skills Training. This detail will consist of billing separated in the following categories: Task Order Management, Situational Awareness (EINSTEIN), Incident Handling Support, Strategic Analysis Services, Malicious Code Support, and Information Support Services. Additional instructions for billing/invoices will be requested by NCSD as required for reporting related to OMB 300 Capital Investments.

The Contractor shall submit invoices on a monthly basis in hard and soft copies to the following locations:

U.S. Department of Homeland Security
ATTN: Preparedness, Finance Branch, Randall Miller (7th and D St)
245 Murray Lane, SW, Building 410
Washington, DC 20528

U.S. Department of Homeland Security
ATTN: Office of Procurement Operations/Mary Caldwell/7th & D Street,
Room [redacted] (b)(6)
245 Murray Lane, SW, Building 410
Washington, DC 20528
E-mail: [redacted] (b)(6)

21.0 ACRONYMS

BOTNET	roBOT NETwork
CDRL	Contract Data Requirements List
CD-ROM	Compact Disk – Read Only Memory
CERT	Computer Emergency Readiness Team
CFR	Code of Federal Regulations
CIA	Central Intelligence Agency
CII	Critical Infrastructure Information
CIIN	Critical Infrastructure Information Notice
CM	Configuration Management
CO	Contracting Officer
COI	Conflict of Interest
CONUS	Continental United States
COOP	Continuity of Operations Plan
COTR	Contracting Officer Technical Representative
COTS	Commercial Off The Shelf
CSIRC	Computer Security Incident Response Center
DC	District of Columbia
DC&C	Data Collection and Collaboration
DHS	Department of Homeland Security
DOD	Department of Defense
DR	Disaster Recovery
EAGLE	Enterprise Acquisition Gateway for Leading-Edge Solutions
EDMO	Enterprise Data Management Office
EIT	Electronic Information Technology
EOD	Entry On Duty
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FIN	Federal Information Notice
FINS	Former Immigration and Naturalization Service
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FTR	Federal Travel Regulation
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GOTS	Government Off The Shelf
GSA	Global Situational Awareness
HLS EA	Homeland Security Enterprise Architecture
IP	Internet Protocol
ISAC	Information Sharing Analysis Center
ISAS	Information Sharing and Analysis System
ISS	Integration and Support Services

ISSO	Information System Security Officer
IT	Information Technology
JFMIP	Joint Financial Management Improvement Program
LPR	Lawful Permanent Resident
Malcode	Malicious Code
Malware	Malicious Software
MOE	Mission Operating Environment
MS	Microsoft
NCS	National Communications System
NCSD	National Cyber Security Division
NDA	Non-Disclosure Agreement
NISPOM	National Industrial Security Program Operating Manual
NOC	National Operations Center
NS	Network Sensor
NSA	National Security Agency
OAST	Office on Accessible Systems and Technology
OCONUS	Outside Continental United States
ODC	Other Direct Cost
PCII	Protected Critical Infrastructure Information
PMR	Program Management Review
PREP	Preparedness
QA	Quality Assurance
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SOP	Standard Operating Procedure
SOW	Statement of Work
TRM	Technology Reference Model
TS	Top Secret
US	United States
US-CERT	United States Computer Emergency Readiness Team
VA	Virginia
VTC	Video Teleconference
WBS	Work Breakdown Structure
XML	eXtensible Markup Language