ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF PAGES 69

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

1. DATE OF ORDER	
2. CONTRACT NO. *(If any)*	HSHQDC-06-D-00024
3. ORDER NO.	HSHQDC-07-J-00744
4. REQUISITION/REFERENCE NO.	RPNC-07-00122

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

7. TO: RICK FINN (b)(6)

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

6. SHIP TO:

a. NAME OF CONSIGNEE
BALLSTON PLAZA II

b. STREET ADDRESS
1110 N. GLEBE RD

c. CITY: ARLINGTON | d. STATE: VA | e. ZIP CODE:

f. SHIP VIA

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.

☒ 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 ☒ 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		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE *(Date)*	16. DISCOUNT TERMS
a. INSPECTION	b. ACCEPTANCE			
Destination	Destination			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)
	Tax ID Number: (b)(4) DUNS Number: 610320215+0000 This is a time-and-materials contract. All sub-CLINS amounts are not-to-exceed ceilings. Continued ...					

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.	17(h) TOTAL *(Cont. pages)*

21. MAIL INVOICE TO:

a. NAME	Department of Homeland Security	$3,750,860.00
b. STREET ADDRESS (or P.O. Box)	IAIP 245 Murray Lane, SW Building 410 Attn: Invoice Processing	
c. CITY: Washington	d. STATE: DC	e. ZIP CODE: 20528

17(i) GRAND TOTAL: $3,750,860.00

SEE BILLING INSTRUCTIONS ON REVERSE

22. UNITED STATES OF AMERICA
BY *(Signature)*

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

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (Rev. 3/2005)
Prescribed by GSA/FAR 48 CFR 53.213(e)

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-07-J-00744

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)

Project Title: "National Coordinating Center Communications Information Sharing and Analysis 24x7 Watch"

Work shall be conducted in accordance with the attached pricing schedule, contract clauses, and statement of work.

The contractor shall provide the types of labor at the corresponding unit price per hour in accordance with the terms and conditions of the award. The unit price per hour is inclusive of the hourly wage, plus any applicable overhead, general and administrative expenses, and profit.

Sub-CLINs 0001AF (Task 6: National Command and Coordination Capability) will not be executed at this time. When required, the task order will be modified to exercise an option for this sub-CLIN.

Tasks 1 and 4 will not be charged under this award until November 8, 2007.

Period of performance is a base period of fifty (50) weeks from date of award. Three additional one-year options may be exercised at the government discretion.

CAGE Code: 474R7
DUNS: 610320215
TIN: (b)(4)

Contract Specialist: Nancy R. Hoffman
(phone: (b)(6)
(e-mail

Contracting Officers Representative: John OConnor
(phone: (b)(6)
(e-mail:

Continued ...

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-07-J-00744

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 Prep. & Intel. Acquisition Division 245 Murray Lane, SW Building 410 Washington DC 20528 Period of Performance: 10/01/2007 to 09/14/2008					
0001AA	Task 1: Program and Task Order Management (b)(4) hrs.) Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS Accounting Info: NSEP000-000-M7-4080-03-000-01-08-0200-00-00-00-00-GE-0E 2576 RP7122 Funded: (b)(4)				(b)(4)	
0001AB	Task 2: Operations Support (b)(4) hrs.) Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS Accounting Info: NSEP000-000-M6-4080-01-000-01-08-0200-00-00-00-00-GE-0E 2576 RP7122 Funded: (b)(4) Accounting Info: NSEP000-000-M7-4080-05-000-01-08-0200-00-00-00-00-GE-0E 2576 RP7122 Funded: (b)(4) Accounting Info: NSEP000-000-M7-4080-03-000-01-08-0200-00-00-00-00-GE-0E 2576 RP7122 Funded: (b)(4)					
0001AC	Task 3: Information Processing and Communications Support (b)(4) hrs.) Product/Service Code: D316 Continued ...					

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-07-J-00744

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS Accounting Info: NSEP000-000-M7-4080-04-000-01-08-0200-00-00-00-00-GE-0E 2576 RP7122 Funded: (b)(4)					
0001AD	Task 4: Intelligence Support (b)(4) hrs.) Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS Accounting Info: NSEP000-000-M7-4080-03-000-01-08-0200-00-00-00-00-GE-0E 2576 RP7122 Funded: (b)(4)					
0001AE	Task 5: Homeland Infrastructure Threat & Risk Analysis Center (b)(4) hrs.) Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS Accounting Info: NSEP000-000-M7-4080-04-000-01-08-0200-00-00-00-00-GE-0E 2576 RP7122 Funded: (b)(4)				(b)(4)	
0001AF	Task 6: National Command & Coordination Capability (NCCC) Planning, Implementation Preparation, Federal Policy Assessment and Support (b)(4) hrs. - option) Amount: (b)(4) Option Line Item) 09/15/2008 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS Continued ...					

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-07-J-00744

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
0001AG	Task 7: Continuity Communications Architecture Support (b)(4) hrs.) Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS Accounting Info: NSEP000-000-M7-4080-02-000-01-08-0200-00-00-00-00-GE-0E 2576 RP7122 Funded: (b)(4)				(b)(4)	
0001AH	SOW Para. 5.1.1.2: Surge Support (est (b)(4) hrs.) Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS Accounting Info: NSEP000-000-M7-4080-01-010-01-08-0200-00-00-00-00-GE-0E 2576 RP7122 Funded (b)(4)					
0001AI	Travel (NTE Ceiling: $9,064.00) Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS Accounting Info: NSEP000-000-M7-4080-01-010-01-08-0200-00-00-00-00-GE-0E 2576 RP7122 Funded: $9,064.00				9,064.00	
0001AJ	Other Direct Costs (NTE Ceiling: $75,000.00) Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS Accounting Info: Continued ...				75,000.00	

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-07-J-00744

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	NSEP000-000-M7-4080-04-000-01-08-0200-00-00-00-00-GE-0E 2576 RP7122 Funded: $75,000.00					
0002AA	Task 1: Program Management and Task Order Management (b)(4) hrs.) Amount: (b)(4) Option Line Item) 09/15/2008 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0002AB	Task 2: Operations Support (b)(4) hrs.) Amount: (b)(4) Option Line Item) 09/15/2008 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0002AC	Task 3: Information Processing and Communicaitons Support (b)(4) hrs.) Amount: (b)(4) (Option Line Item) 09/15/2008 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS				(b)(4)	
0002AD	Task 4: Intelligence Support (b)(4) hrs.) Amount: (b)(4) Option Line Item) 09/15/2010 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0002AE	Task 5: Homeland Infrastructure Threat & Risk Analysis Center (b)(4) hrs.) Continued ...					

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-07-J-00744

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	Amount (b)(4) (Option Line Item) 09/15/2010 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0002AF	Task 6: National Command and Coordination Capability (NCCC) Planning, Implementation Preparation, Federal Policy Assessment and Support (b)(4) hrs.) Amount: (b)(4) Option Line Item) 09/15/2010 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0002AG	Task 7: Continuity Communications Architecture (CCA) Support (b)(4) rs.) Amount: (b)(4) Option Line Item) 09/15/2010 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS				(b)(4)	
0002AH	SOW Para. 5.1.1.2: Surge Support (b)(4) hrs. est.) Amount (b)(4) Option Line Item) 09/15/2007 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0002AI	Travel (NTE Ceiling of $10,000.00) Amount: $10,000.00(Option Line Item) 09/15/2008 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT Continued ...					

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-07-J-00744

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	SVCS					
0002AJ	Other Direct Costs (NTE Ceiling: $75,000.00) Amount: $75,000.00(Option Line Item) 09/15/2008 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0003AA	Task 1: Program and Task Order Management (b)(4) hrs.) Amount: (b)(4) Option Line Item) 09/15/2008 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0003AB	Task 2: Operations Support (b)(4) rs.) Amount: (b)(4) (Option Line Item) 09/15/2010 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS				(b)(4)	
0003AC	Task 3: Information Processing & Communications Support (b)(4) hrs.) Amount: (b)(4) Option Line Item) 09/15/2010 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0003AD	Task 4: Intelligence Support (b)(4) rs.) Amount: (b)(4) Option Line Item) 09/15/2010 Product/Service Code: D316 Product/Service Description: Continued ...					

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-07-J-00744

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0003AE	Task 5: Homeland Infrastructure Threat & Risk Analysis Center (b)(4) hrs.) Amount: (b)(4) (Option Line Item) 09/15/2010 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0003AF	Task 6: National Command & Coordination Capability (NCCC) Planning, Implementation Preparation, Federal Policy Assessment and Support (b)(4) Amount: (b)(4) (Option Line Item) 09/15/2010 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS				(b)(4)	
0003AG	Task 7: Continuity Communicaiotns Architecture Support (b)(4) hrs.) Amount: (b)(4) Option Line Item) 09/15/2010 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0003AH	SOW Para. 5.1.1.2: Surge Support Amount: (b)(4) (Option Line Item) 09/15/2010 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0003AI	Travel (NTE Ceiling: $10,000.00) Continued ...					

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-07-J-00744

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	Amount: $10,000.00(Option Line Item) 09/15/2010 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0003AJ	Other Direct Costs (NTE Ceiling: $75,000.00) Amount: $75,000.00(Option Line Item) 09/15/2010 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0004AA	Task 1: Program & Task Order Support (b)(4) rs.) Amount: (b)(4) Option Line Item) 09/15/2011 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS				(b)(4)	
0004AB	Task 2: Operations Support (b)(4) hrs.) Amount: (b)(4) Option Line Item) 09/15/2011 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0004AC	Task 3: Information Processing and Communications Support (b)(4) hrs.) Amount: (b)(4) Option Line Item) 09/15/2011 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0004AD	Task 4: Intelligence Support Continued ...					

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-07-J-00744

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	(b)(4) hrs.) Amount: (b)(4) Option Line Item) 09/15/2011 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0004AE	Task 5: Homeland Infrastructure Threat and Risk Analysis Center (b)(4) hrs.) Amount: (b)(4) ption Line Item) 09/15/2011 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0004AF	Task 6: NCCC Planning, implementation Preparation, Federal Policy Assessment, and Support (b)(4) rs.) Amount (b)(4) ption Line Item) 09/15/2011 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS				(b)(4)	
0004AG	Task 7: Continuity Communications Architecture Support (b)(4) hrs.) Amount: (b)(4) Option Line Item) 09/15/2011 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0004AH	SOW Para. 5.1.1.2: Surge Support (b)(4) hrs. est.) Amount: (b)(4) Option Line Item) 09/15/2011 Product/Service Code: D316 Product/Service Description: Continued ...					

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-07-J-00744

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
0004AI	Travel (NTE Ceiling: $10,000.00) Amount: $10,000.00(Option Line Item) 09/15/2011 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS				(b)(4)	
0004AJ	Other Direct Costs (NTE Ceiling: $75,000.00) Amount: $75,000.00(Option Line Item) 09/15/2011 Product/Service Code: D316 Product/Service Description: TELECOMMUNICATIONS NETWORK MANAGEMENT SVCS					
	The total amount of award: $21,818,762.00. The obligation for this award is shown in box 17(i).					

5. Labor Hours

Base Period		
Contract Line Item (CLIN)	**Description**	**Quantity & Unit**
0001AA	Task 1: Program & Task Order Management	(b)(4)
0001AB	Task 2: Operations Support	
0001AC	Task 3: Information Processing & Communications Support	
0001AD	Task 4: Intelligence Support	
0001AE	Task 5: Homeland Infrastructure Threat & Risk Analysis Center	
0001AF	Task 6: National Command and Coordination Capability (NCCC) Planning, Implementation Preparation, Federal Policy Assessment, and Support	
0001AG	Task 7: Continuity Communications Architecture (CCA) Support	
0001AH	Paragraph 5.1.1.2: Surge Support	
	Total Not-to-Exceed (NTE) Hours	

Option Period 1		
Contract Line Item (CLIN)	**Description**	**Quantity & Unit**
0002AA	Task 1: Program & Task Order Management	(b)(4)
0002AB	Task 2: Operations Support	
0002AC	Task 3: Information Processing & Communications Support	
0002AD	Task 4: Intelligence Support	
0002AE	Task 5: Homeland Infrastructure Threat & Risk Analysis Center	
0002AF	Task 6: National Command and Coordination Capability (NCCC) Planning, Implementation Preparation, Federal Policy Assessment, and Support	
0002AG	Task 7: Continuity Communications Architecture (CCA) Support	
0002AH	Paragraph 5.1.1.2: Surge Support	
	Total NTE Hours	

Option Period 2		
Contract Line Item (CLIN)	**Description**	
0003AA	Task 1: Program & Task Order Management	(b)(4)
0003AB	Task 2: Operations Support	
0003AC	Task 3: Information Processing & Communications Support	
0003AD	Task 4: Intelligence Support	
0003AE	Task 5: Homeland Infrastructure Threat & Risk Analysis Center	
0003AF	Task 6: National Command and Coordination Capability (NCCC) Planning, Implementation Preparation, Federal Policy Assessment, and Support	
0003AG	Task 7: Continuity Communicatio Architecture (CCA) Support	
0003AH	Paragraph 5.1.1.2: Surge Support	
	Total NTE Hours	

Option Period 3		
Contract Line Item (CLIN)	**Description**	**Quantity & Unit**
0004AA	Task 1: Program & Task Order Management	(b)(4)
0004AB	Task 2: Operations Support	
0004AC	Task 3: Information Processing & Communications Support	
0004AD	Task 4: Intelligence Support	
0004AE	Task 5: Homeland Infrastructure Threat & Risk Analysis Center	
0004AF	Task 6: National Command and Coordination Capability (NCCC) Planning, Implementation Preparation, Federal Policy Assessment, and Support	
0004AG	Task 7: Continuity Communication Architecture (CCA) Support	
0004AH	Paragraph 5.1.1.2: Surge Support	
	Total NTE Hours	

6. Other Direct Costs

Base Year			
Contract Line Item (CLIN)	**Description**	**Quantity & Unit**	**Estimated Amount**
0001AI	Travel	One Lot	NTE $9,064.00
0001AJ	Other Direct Costs (ODC)	One Lot	NTE $75,000.00
Total		One Lot	$84,064.00

Option Period 1			
Contract Line Item (CLIN)	**Description**	**Quantity & Unit**	**Estimated Amount**
0002AI	Travel	One Lot	NTE $10,000.00
0002AJ	Other Direct Costs	One Lot	NTE $75,000.00
Total			$85,000.00

Option Period 2			
Contract Line Item (CLIN)	**Description**	**Quantity & Unit**	**Estimated Amount**
0003AI	Travel	One Lot	NTE $10,000.00
0003AJ	Other Direct Costs	One Lot	NTE $75,000.00
Total			$85,000.00

Option Period 3			
Contract Line Item (CLIN)	**Description**	**Quantity & Unit**	**Estimated Amount**
0004AI	Travel	One Lot	NTE $10,000.00
0004AJ	Other Direct Costs	One Lot	NTE $75,000.00
Total			$85,000.00

7. Hourly Rates

Labor Category	Base Period	Option Period 1	Option Period 2	Option Period 3
(b)(4)				

The applicable clauses from the contractor's EAGLE Contract No. HSHQDC-06-D-00024 are in full force and effect for the life of the contract.

I. FEDERAL ACQUISITION REGULATION (FAR) CLAUSES

52.204-9 Personal Identity Verification of Contractor Personnel.

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.

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 (7) days.

(End of clause)

FAR 52.217-9 Option to Extend the Term of the Contract.

OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within seven (7) days; provided that the Government gives the Contractor a

preliminary written notice of its intent to extend at least seven (7) days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed three (3) years and fifty (50) months.

(End of clause)

52.227-14 Rights in Data—General.

RIGHTS IN DATA—GENERAL (JUNE 1987)

(a) *Definitions*. "Computer software," as used in this clause, means computer programs, computer data bases, and documentation thereof.

"Data," as used in this clause, 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," as used in this clause, means data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, as well as data identifying source, size, configuration, mating, and attachment characteristics, functional characteristics, and performance requirements; except that for computer software it means data identifying source, functional characteristics, and performance requirements but specifically excludes the source code, algorithm, process, formulae, and flow charts of the software.

"Limited rights," as used in this clause, means the rights of the Government in limited rights data as set forth in the Limited Rights Notice of paragraph (g)(2) if included in this clause.

"Limited rights data," as used in this clause, 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 thereof.

"Restricted computer software," as used in this clause, means computer software developed at private expense and that is a trade secret; is commercial or financial and is confidential or privileged; or is published copyrighted computer software, including minor modifications of such 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)(3) 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," as used in this clause, means data (other than computer software) which are of a scientific or technical nature.

"Unlimited rights," as used in this clause, means the right 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 regarding copyright, 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) 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;

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

(iii) Substantiate 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) Establish claim to copyright subsisting in data first produced in the performance of this contract to the extent provided in paragraph (c)(1) of this clause.

(c) Copyright—

(1) *Data first produced in the performance of this contract.* Unless provided otherwise in paragraph (d) of this clause, the Contractor may establish, without prior

approval of the Contracting Officer, claim to copyright subsisting 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 establish claim to copyright subsisting in all other data first produced in the performance of this contract. When claim to copyright is made, the Contractor shall affix the applicable copyright notices of 17 U.S.C. 401 or 402 and acknowledgment of Government sponsorship (including contract number) to the data when such data are delivered to the Government, as well as when the data are published or deposited for registration as a published work in the U.S. Copyright Office. 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 in 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 by or on behalf of the Government.

(2) *Data not first produced in the performance of this contract.* The Contractor shall not, without 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 and which contains the copyright notice of 17 U.S.C. 401 or 402, unless the Contractor identifies such data and 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; *provided*, however, that if such data are computer software the Government shall acquire a copyright license as set forth in paragraph (g)(3) of this clause if included in this contract or as otherwise may be provided in a collateral agreement incorporated in or made part of this contract.

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

(d) Release, publication and use of data.

(1) 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 to the extent such data may be subject to the Federal export control or national security laws or regulations, or unless otherwise provided in this paragraph of this clause or expressly set forth in this contract.

(2) The Contractor agrees that to the extent it receives or is given access to data necessary for the performance of this contract which contain restrictive markings, the Contractor shall treat the data in accordance with such markings unless otherwise specifically authorized 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)(2) or (g)(3) of this clause and use of such is not authorized by this clause, or if such 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, the following procedures shall apply prior to canceling or ignoring the markings.

(i) The Contracting Officer shall make written inquiry to the Contractor affording the Contractor 30 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 30-day period (or a longer time not exceeding 90 days 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 subdivision (e)(1)(i) of this clause, the Contracting Officer shall 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 shall 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 shall furnish the Contractor a written determination, which determination shall 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 shall continue to abide by the markings under this subdivision (e)(1)(iii) until final resolution of the matter either by the Contracting Officer's determination becoming final (in which instance the Government shall 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) This paragraph (e) does not apply if this contract is for a major system or for support of a major system by a civilian agency other than NASA and the U.S. Coast Guard agency subject to the provisions of Title III of the Federal Property and Administrative Services Act of 1949.

(4) 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 this paragraph (e) from bringing a claim under the Contract Disputes Act, including pursuant to the Disputes clause of this contract, as applicable, 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 either the limited rights or restricted rights notice as authorized by paragraph (g) of this clause, or the copyright notice required by paragraph (c) of this clause, shall be deemed to have been furnished with unlimited rights, and the Government assumes no liability for the disclosure, use, or reproduction of such data. However, to the extent the 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 for good cause shown) after delivery of such data, permission to have notices placed on qualifying data at the Contractor's expense, and 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 use of the proposed notice is authorized; and

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

(2) The Contracting Officer may also (i) permit correction at the Contractor's expense of incorrect notices if the Contractor identifies the data on which correction of the notice is to be made, 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) When data other than that listed in subdivisions (b)(1)(i), (ii), and (iii) of this clause are specified to be delivered under this contract and qualify as either limited rights data or restricted computer software, if the Contractor desires to continue protection of such data, the Contractor shall withhold such data and not furnish them to the

Government under this contract. As a condition to this withholding, the Contractor shall identify the data being withheld and furnish form, fit, and function data in lieu thereof. Limited rights data that are formatted as a computer data base for delivery to the Government are to be treated as limited rights data and not restricted computer software.

(2) [Reserved]

(3) [Reserved]

(h) *Subcontracting.* The Contractor has the responsibility to 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 such rights, the Contractor shall promptly bring such refusal to the attention of the Contracting Officer and not proceed with subcontract award without further authorization.

(i) *Relationship to patents.* 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 (June 1987).

(g)(2) 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 withholdable. If delivery of such data is so required, the Contractor may affix the following "Limited Rights Notice" to the data and the Government will thereafter treat the data, subject to the provisions of paragraphs (e) and (f) of this clause, in accordance with such Notice:

LIMITED RIGHTS NOTICE (JUNE 1987)

(a) These data are submitted with limited rights under Government Contract No. _____ (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*(d)(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 clause)

FAR 52.232-7 Payments under Time-and-Materials and Labor-Hour Contracts.

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.

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)

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

HSAR 3052.204-70 Security Requirements for Unclassified Information Technology Resources.

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 ["insert number of days"] 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.

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)

Implementing Instructions for Compliance with HSAR clause 3052.204-71, "Contractor Employee Access"

1. GENERAL

Department of Homeland Security Acquisition Regulation (HSAR) clause 3052.204-71 requires that contractor personnel requiring unescorted access to government facilities, access to sensitive information, or access to government information technology (IT) resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract.

Department of Homeland Security (DHS) policy requires a favorably adjudicated background investigation prior to commencing work on this contract for all contractor personnel who require recurring access to government facilities or access to sensitive information, or access to government IT resources.

Contractor employees will be given a suitability determination unless this requirement is waived under Departmental procedures. Requirements for suitability determination are defined in paragraph 3.0.

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 to 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, it shall abide by the requirements set forth by the agency.

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.

2. CONTRACTOR PERSONNEL

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". 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)"

2.2 CONTINUED ELIGIBILITY

The Contracting 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.

2.3 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 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.

3.0 SUITABILITY DETERMINATION

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 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.

Contract 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.

4.0 BACKGROUND INVESTIGATIONS

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.

Be advised that unless an applicant requiring access to sensitive information has resided in the US for three of the past five years, the Government may not be able to complete a satisfactory background investigation.

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.

4.1 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.

5.0 INFORMATION TECHOLOGY SECURITY CLEARANCE

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).

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.

6.0 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.

7.0 REFERENCES

7.1 DHS Office of Security

DHS, Office of Security
Personnel Security Staff
Attn: Yolanda Alleyne
Washington DC 20528
Telephone: (b)(6)

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.

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: (b)(6) **Program Manaager.**

(End of clause)

HSAR 3052.242-72 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE.

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)

III. LOCAL CLAUSES

1. PERIOD OF PERFORMANCE.

The period of performance for this order shall commence upon date and the base period shall continue for fifty (50) weeks 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: Fifty Weeks from Date of Award.
b) Option Period I: One Year.
c) Option Period II: One Year.
d) Option Period III: One Year.

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.

b. Local Travel. Local travel will not be reimbursed within a fifty (50) mile radius of the individual's assigned worksite. Local travel may include frequent trips to the National

Communications System, other Department of Homeland Security facilities, and local meeting or conference venues.

If the contractor locates personnel outside the Washington D.C. metropolitan area, the worksite shall be considered to be the Washington D.C. metropolitan area. Travel expenses to and/or from the Washington D.C. metropolitan area will not be reimbursed, unless otherwise authorized.

3. SUBMISSION OF INVOICES.

Original invoices shall be sent electronically to the assigned contract specialist identified on the cover page of the order. The invoice must contain the 1) contract number; 2) task order number; and 3) applicable contract line item numbers (CLINs).

The invoice must comply with the payment clause in the award document in order to be considered a proper invoice. One copy of the invoice shall be forwarded to the Contracting Officer's Representative (COR) for coordination. It will then be forward by the COR to the contract specialist for approval to make payment.

The contractor is authorized to submit monthly invoice on a whole-month basis. Invoices shall include time sheets, and receipts for actual travel and other direct costs (ODCs) expenses.

4. ORGANIZATIONAL CONFLICTS OF INTEREST.

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. FUNDING FLEXIBILITY.

The contractor is not restricted to the price delineated for the contract line item numbers (CLINs) or sub-CLINs in the price schedule in those instances where CLINs or sub-CLINs share the same accounting information. The contractor is authorized to use the available funding across CLINs or sub-CLINs with the same accounting information as necessary during the performance period as long as the aggregate ceiling price for the CLINs or sub-CLINs is not exceeded. However, the contractor is not authorized to exceed the ceiling price of this order.

6. **Non-Personal Services**

(a) The Government and the Contractor understand and agree that the technical, analytic and liaison support services delivered by the Contractor to the Government are non-personal services. The parties also recognize and agree that no employer-employee or master-servant relationship exists or will exist between the Government and the Contractor. The Contractor and the Contractor's employees are not employees of the

Federal Government and are not eligible for entitlement and benefits given federal employees.

(b) Contractor personnel under this contract shall not (i) be placed in a position where there is an appearance that they are employed by a Federal Officer, or are under the supervision, direction, or evaluation of a Federal Officer, or (ii) be placed in a position of command, supervision, administration or control over Government personnel.

STATEMENT OF WORK (SOW)
NCC 24x7 Watch

September 28, 2007

1. **Order Title.** NCC Communications Information Sharing and Analysis Center 24x7 Watch

2. **Background.** Provide a 24 x 7 National Coordinating Center (NCC) Watch and Analysis Operation to provide technical, analytical, and liaison support services for the NCC, the NCC Communications Information Sharing and Analysis Center (NCC Communications ISAC), and Department of Homeland Security. NCC Watch objectives include:

- Be an honest and impartial information broker
- Facilitate voluntary collaboration among NCC partners to support both Government and industry information sharing requirements
- Foster working liaisons with external sources/liaison partners
- "Add value"—e.g., provide information and originate assessments not available elsewhere; watch all sources, compile information and act as a filter; and perform high quality analysis
- Ensure protection of information and rights of data owner
- Maintain, administer, and enhance IT systems supporting NCC Watch operations
- Assist the NCS in executing its roles and responsibilities under Executive Order (E.O.) 12472 for planning, developing, and implementing enhancements to the national telecommunications infrastructure.

2.1 Department of Homeland Security (DHS). NCS is in the Cyber Security and Communications Division of the National Protection and Programs Directorate (NPPD) and provides support and interface with other functions of DHS, in particular the Preparedness Directorate and the National Operating Center (NOC) formerly Homeland Security Operations Center (HSOC).

2.2 NCS. The National Communications System (NCS) is a federation of 23 Federal Departments and Agencies responsible for ensuring that reliable, interoperable, and secure telecommunications are available to fulfill national security and emergency preparedness (NS/EP)[1] requirements under all conditions. NCS has been successful in establishing and enhancing interagency cooperation and a partnership with the telecommunications industry since 1962. The Office of the Manager, NCS (OMNCS) serves as the administrative arm to the Manager, NCS and is responsible for the day-to-day operational and programmatic activities, under the direction of the Deputy Manager.

2.3 OMNCS CIP Division. The OMNCS Critical Infrastructure Protection (CIP) Division manages core Telecommunications CIP activities and the daily operations of the NCC and the NCC Communications ISAC. Telecom CIP consists of risk management actions that are

[1] NS/EP: "Capabilities required to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population , damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States." (Telecomm Glossary 2000)

intended to prevent a threat from attempting to, or succeeding at, destroying or incapacitating the telecommunications infrastructure. The CIP Division supplies a senior staff member as NCC Manager. The NCC Manager is responsible for NCC operations, liaison with NCC industry and agency partners, oversight of the NCC Operations, the ISAC function, and chairs the NCC meetings. The CIP Division also provides the coordination for the National Security Telecommunications Advisory Committee (NSTAC) and Government Network Security and Information Exchange (NSIE).

2.4 NCC. The National Coordinating Center (NCC) is a joint industry-government collaborative organization whose mission is to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications[2] services or facilities under all conditions, crises, or emergencies. The NCC was established in 1984 based on a recommendation to the President by the NSTAC. The Manager, NCC is a senior government staff member with the CIP Division of the OMNCS. The NCC Operations Chief in support of the Manager, NCC is responsible for day-to-day activities of the NCC Watch including, maintaining situational awareness, reporting, triage of information, and assessment. The NCC, in support of the NCS as the lead for Emergency Support Function 2 – Communications of the National Response Plan (NRP), is the operations focal point for NCS response activities.

2.4.1 NCC Government Members. Government agency representation in the NCC includes those NCS member agencies that provide delegates to the NCS or that are regular participants in the NCC activities. Current agency members include the Departments of State, Defense, Commerce; the General Service Administration; the Federal Communications Commission; the Federal Emergency Management Agency, the Federal Reserve Board, and the National Security Agency.

2.4.2 NCC Industry Members. Industry representation in the NCC and/or Telecom ISAC includes Americom, AT&T, APCO, Avici Systems, Boeing, , Cellular Telecommunications & Internet Association, Cincinnati Bell, Cisco Systems, COMPTEL, Computer Sciences Corporation, EDS, Globalstar, Intelsat, Internap, Intrado, Juniper, Level3 Communications, Lockheed Martin, Lucent Technologies, McLeodUSA, Motorola, NewSkies, Nortel Networks, Northrop Grumman, Qwest Communications, Raytheon, Savvis, Science Applications International Corporation, Sprint, Telecommunications Industry Association, the United States Telecom Association, VeriSign, Verizon Business Solutions (former MCI), Verizon Communications, and Verizon Wireless. This group continues to expand to encompass new entrants offering telecommunications services, products, and equipment that can assist the NCC in executing its NS/EP telecommunications mission.

2.5 NCC Communications ISAC. The NCC Communications Information Sharing and Analysis Center (NCC Communications ISAC) is a function under the NCC. The NCC Communications ISAC builds on the history of cooperation and established trust relationships among the NCC members, and is also a coordinating body. Although the concept of the ISAC was introduced by Presidential Decision Directive 63, the NCC has been a central hub for sharing critical national security/emergency preparedness (NS/EP) telecommunications information among Government and industry since 1984. The mission of the NCC Communications ISAC is

to support Executive Order 12472 and national Critical Infrastructure Protection goals; to facilitate voluntary collaboration and information sharing among its membership and its liaison partners; to gather information on vulnerabilities, threats, intrusions, and anomalies from multiple sources and perform analysis with the goal of averting or mitigating impact upon the telecommunications infrastructure.[2] Information is sanitized and disseminated in accordance with information sharing agreements established for that purpose by the Comm ISAC members. Although the bulk of the ISAC effort is directed towards virtual telecommunication infrastructure issues, the scope of the mission is all hazards.

2.6 NSIE. The National Security Information Exchange (NSIE) process was started by NSTAC and the Manager, NCS, in 1991. Its purpose is to exchange information, at a technical working level, among companies and between government and industry on issues involving penetration or manipulation of software and databases associated with the control and operation of the Public Network (PN) which could affect NS/EP telecommunications. The NSIE consists of two forums—the NSTAC NSIE, providing the industry perspective, and the Government NSIE. The two bodies meet together bi-monthly to exchange information and experiences on telecommunications and information network vulnerabilities, risks, trends, and mitigations. Due to the sensitivity of information discussed, all members and their parent company/agency sign non-disclosure agreements[3]. Many of the NSIE member companies are also NCC members. Due to the high level of trust placed in the NSIE by the NCC members, much of the information disseminated from the NCC Communications ISAC is also shared with the NSIE representatives. The NCC Comm ISAC Watch provides message dissemination and alerts to the NSIE membership as requested.

2.7 JTF-GNO. The Department of Defense Joint Task Force – Global Network Operations (JTF-GNO) is the umbrella for the DoD Computer Emergency Response Team (DoD-CERT) and the former the Defense Information Systems Agency (DISA) Global Network Operations and Security Center (GNOSC) and is located at DISA Headquarters.[4] Their constituency includes combatant commanders and their Components, Services and Service components, Defense Agencies, the Joint Staff, and Office of the Secretary of Defense. Although their individual missions are different, all three together are focused on protecting the interconnected set of information systems and networks that comprise the Defense Information Infrastructure (DII). The DoD-CERT serves as technical advisors to the JTF, concentrating on computer network defense sensor analysis, strategic impact analysis and response, malicious code analysis and countermeasures, and vulnerability identifications and management. The DoD organizations are liaison partners with the NCC and NCC Communications ISAC.

---

[2] Telecommunications Infrastructure—The framework of interdependent telecommunication networks and systems, including both physical and software components, by which the telecommunications industry conducts the transmission, emission, or reception of signs, signals, writing, images, and sounds, or intelligence of any nature, by wire, radio, optical, or other electromagnetic systems.

[3] Individuals are members in the NSIEs, in contrast to the case with the NCC, where the companies and agencies are members.

[4] This is currently in the same building as the NCS Headquarters.

3. Scope.

The objective of this SOW is to procure support services to maintain the on-going 24x7 National Coordinating Center (NCC) Communications Infrastructure Information Sharing and Analysis Center Watch and Assessment Operation (short title "NCC Communications ISAC Watch,"), and related support to the parent organization, the Department of Homeland Security. The task order will include a base period of fifty (50) week after date of award, with an additional three one-year option periods. This support will support NCC emergency response, planning, and preparation efforts for all hazards including man-made and natural.

This action will provide support to the NCC watch and assessment operation and shall include, but is not limited to, the following disciplines:
Program Manager
Watch Coordinator
Watch Officer
System developer/administrator
Technical Lead
Intelligence Analyst
Surge and Specialized Support (SME, administrative, policy, process, training)

The NCC Communications ISAC Watch will provide technical, analytical, and liaison support services for the NCC, in particular for the NCC Communications Information Sharing and Analysis Center Communications Information Sharing and Analysis Center (NCC Communications ISAC) function that supports both Executive Order (E.O.) 12472 and the critical infrastructure protection goals of Presidential Decision Directive 63 and Homeland Security Presidential Directive-7 (HSPD-7). Support shall be provided in the areas of information assurance analysis, document development, requirements development, to include recommendations for effective use and requirements for the watch and analysis operation, liaison with other public and private sector organizations, information system support, and other administrative support as required. Support shall assist the NCC to execute its responsibilities under EO.12472 to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services and facilities under all conditions of crisis and emergency.

Results and deliverables will maintain operations and enhance and evolve the concept of operations and procedures for the 24x7 NCC Communications ISAC Watch and Assessment Operation.

4. Applicable Documents.

Executive Order (E.O.) 12472 – established the NCC and sets NS/EP goals
Section 706 of the Communications Act of 1934 –defines role of the Office of Science and Technology Policy to control, coordinate, and direct the Nation's telecommunications facilities systems and services which the NCS and its operational component the NCC supports
Presidential Decision Directive 63 (PDD-63) – defines critical infrastructure goals

Homeland Security Presidential Directive-7 (HSPD-7) – defines critical infrastructure including telecommunications for which the NCS is the sector specific agency
National Response Plan (NRP) with focus on ESF-2 Annex – NCS is the lead for ESF-2 and the NCC is focus for operational activities of the NCS
DHS 4300A Sensitive System Handbook – defines IT policy required for DHS certification and accreditation
DHS 4300B National Security Systems Handbook - defines IT policy required for DHS certification and accreditation

DHS 4010.2 Electronic and Information Technology Accessibility - defines IT policy required for DHS certification and accreditation
National Security Presidential Directive (NSPD) 51 and Homeland Security Presidential Directive (HSPD) 20 - establishes a comprehensive national policy on the continuity of Federal Government structures
NCS Directive 3-10 sets the minimum requirements for continuity communications capabilities for the Federal Executive Branch – these requirements are directly applicable to NCC operations

The Contractor shall comply with the appropriate DHS/DoD-approved architectures, programs, standards and guidelines, such as National Information Assurance Certification and Accreditation Process (NIACAP), Department of Homeland Security security guidance, and Defense Information Infrastructure (DII) Strategic Technical Information Guide (STIG).

5. Specific Tasks.

- **Task Area 1: Program and Task Order (TO) Management**
- **Task Area 2: Operations Support**
- **Task Area 3: Information Processing and Communication Support**
- **Task Area 4: Intelligence Support**
- **Task Area 5: Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) Communications Specialist**
- **Task Area 6: National Command and Coordination Capability (NCCC) Planning, Implementation Preparation, Federal Policy Assessment, and Support**
- **Task Area 7: - Continuity Communications Architecture (CCA) Support**

5.1 Task 1 – Program and Task Order Management.

The Contractor shall provide a Program Manager position responsible for the planning, direction, coordination, and control necessary to manage and accomplish all work contained in this SOW. Specifically, the Contractor shall provision all necessary support services and staffing, including surge support and subject matter experts (as needed), to provide a 24 x 7 operation in support of the NCC, to include management and enhancement of the information sharing, sanitization, and dissemination process; NCC partner liaison; analysis, technical liaison efforts, and other technical and analytical support. Provide the technical (task order level) and functional activities at the Contract Level needed for the Program Management of this SOW.

Duties include productivity and management methods and production of the Management Plan describing the technical approach, organizational resources and management controls to be employed to meet the cost, performance and schedule requirements. Provide a weekly summary of activities and a quarterly status report monitoring the quality assurance, progress/status reporting, and program reviews applied to the TO. Provide Quarterly Program Management Review presentations covering budget expenditure, Watch activities, message traffic summary, visitors, and recommendations going forward.

5.1.1 The Management Plan shall address the following schedule and staffing categories.

5.1.1.1 Schedule - Contractor shall, as a minimum, support the following schedule:

MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SUNDAY	SATURDAY
7am Watch turnover	7am Watch turnover	7am Watch turnover	7am Watch turnover	7am Watch turnover	600am Watch turnover	600am Watch turnover
9am IT-ISAC call	9am IT-ISAC call	9am IT-ISAC call	9am IT-ISAC call	9am IT-ISAC call	11am Watch call	11am Watch call
11am Watch call	930am Physical security call	11am Watch call	11am Watch call	10am Call with Canada	630pm Watch turnover	630pm Watch turnover
3pm Watch turnover	11am Watch call	3pm Watch turnover	3pm Watch turnover	11am Watch call		
11pm Watch turnover	3pm watch turnover	11pm Watch turnover	11pm Watch turnover	3pm Watch turnover		
	11pm Watch turnover			11pm Watch turnover		

5.1.1.2 Staffing: Contractor shall support the following minimum Watch staffing. In addition, the Contractor shall provide the ability to surge with additional watch officers in the case of a major incident or event. Staffing levels below encompass the minimum level of support required for Tasks 1, 2, 3, & 4.

Monday – Friday Day shift 0600-1600
- 1 Watch Coordinator
- 2 Watch Officers
- 1 System administrator (on-call when off duty)
- 1 Tech /Analysis Lead (on-call when off duty)
- 1 Intelligence officer (M-F 8hr/day)
- 1 Program Manager (on-call when off duty)

Monday – Friday Swing shift 1400-2400
2 Watch Officers

Monday – Friday Night shift 2200-0800
2 Watch Officers

Saturday – Sunday Day 0530 – 1830
1 Watch Coordinator
2 Watch Officers

Saturday – Sunday Night 1730 - 0630
2 Watch Officers

Watch Coordinator: The Watch Coordinator shall have strong management skills and a strong background in IT Security. The Watch Coordinator is responsible for overseeing the day-to-day activities at the Watch in accordance with the Standard Operating Procedures (SOPs) or as directed by the NCC Manager or NCC Operations Lead. The Watch Coordinator shall act as the primary point of contact for interfacing with the government and industry partners. The Watch Coordinator shall be responsible for product quality control and maintaining required staffing levels.. The Watch Coordinator is primarily a day shift role with on-call responsibility as needed. Duties include oversight prioritization, and de-confliction of the activities of the Watch and Assessment Operation and the watch officers, as well as to provide additional liaison support through interface with telecommunications and information/communications industry representatives and liaison partners of the NCC or NCC Communications ISAC. The Watch Coordinator role is not a "supervisory" position, rather it is a role to ensure continuity and best application of skills of the watch operations, and to guide and perform focused technical research.

- The person filling this role will frequently attend meetings and discussions, interface with industry or outside agencies, while leaving the watch officers free to continue their monitoring, analysis, and on-going liaisons.
- Depending on the situation, the Watch Coordinator may temporarily swap positions with a given watch officer whose skills may be more germane to apply to a particular issue or meeting.
- The Watch Coordinator is NOT intended to replace the intercommunication function expected of all the watch officers, but his/her role will allow watch operations to continue uninterrupted.
- The Watch Coordinator will also focus Watch research and liaison efforts on specific areas in response to current or evolving situations.

Watch Officers: Watch officers must have an Information Technology (IT) security background with a broad expertise in research, analysis, and writing skills and be able to perform triage on questions, issues, or events involving the nation's critical communications infrastructure. Officers will be responsible for monitoring the NCC accounts, in accordance with their security

clearance for communications infrastructure-related information, interfacing with sector representatives, responding to initial requests from the sectors or other parts of DHS, and performing initial research into answers, issues, or events prior to turning the action over to NCC Government leads. Watch Officers may occasionally serve as Watch Captains if required.

Tech/Analysis Lead: Tech/Analysis Lead must have management skills to direct activities and possess a strong IT security background. The Tech lead shall have broad expertise in research, analysis and technical writing skills and be able to perform triage on questions, issues, or events involving the nation's Critical Communications Infrastructures. In addition to the duties described for Watch Officers, the Tech/Analysis Lead must be able to manage and distribute the workload to ensure that the required reporting requirements are met and must provide overall operational guidance to the Watch Officers for analysis and technical research. The Tech/Analysis Lead may be recalled to duty as situations required analysis.

System Administrator: The system administrator is responsible for day-to-day administration and maintenance of NCC systems at all operating locations including the NCC and COOP facilities. The system administrator shall perform system upgrades of hardware and software, network configuration, user support, create and maintain system documentation, ensure certification and accreditation of NCC systems.

Program Manager: The Program Manager shall provide programmatic oversight and is responsible to task management, tracking expenditures, documentation and maintenance of procedures, overall staffing including surge and specialized consultants, policy development, training, liaison with NCC management, NCC Comm-ISAC industry partners, and NCC government partners. Program Manager will also assist NCC Management with defining short and long terms goals, relationships, and NCC infrastructure.

Intelligence Analyst: The Intelligence Analyst shall have a broad expertise in intelligence collection, handling, and processing. The intelligence analyst shall assist in the definition of collection requirements, assessing threats to the communications sector, address vulnerabilities and consequences, and recommend countermeasures. The Intelligence analysis Lead may be recalled to duty as situations require. The intelligence analyst shall possess Top Secret (Sensitive Compartmented Information (SCI)) credentials to represent the NCS. Work will performed at a location in the National Capital Region as defined by the Government.

Surge Support: As determined by the Government, additional support may be required to effectively manage and execute the emergency response mission of the NCS during NS/EP events. This additional surge support shall be proposed by the Contractor as a mandatory option to be negotiated, when required, for the specific NS/EP response requirement. Types of support may include subject matter experts, administrative, technical support, and security specialists.

5.1.2 Weekly Informal Logs and Activity Assessments.

The Contractor watch officer personnel shall maintain, back up, and provide to OMNCS designated personnel Contractor watch-officer informal logs of shift activities plus weekly informal activity summaries, watch assessments, and recommendations for priorities, changes, or activities for the following week.

5.1.3 NCC Watch Quarterly Program Management Review.

The Contractor shall provide a quarterly NCC Watch and Analysis Operation Operational Assessment, including concise details of activities performed by the watch officers, assessments of incidents/events, and status of liaisons with other organizations, issues, lessons learned and recommendations for changes in procedures or priorities of tasks for the next period. Based on ongoing experiences of the NCC Watch and Analysis Operation, and in collaboration with the OMNCS CIP Division, the Contractor shall provide a quarterly NCC Watch Program Management Review (PMR). The Contractor shall work with the CIP Division staff to incrementally draft and organize information to define and prioritize NCC Watch and Analysis operations. The quarterly assessment should concentrate on contract status, funding profile, visitors to the Watch, chronology of Watch activities by event and topic, and forward looking improvement (relationships, tools, and technology) and issues.

5.2 Task 2 – Operations Support.

Provide the 24 x 7 technical, analytical, and liaison capabilities to support the National Coordinating Center (NCC), in particular the NCC Communications Information Sharing and Analysis Center (NCC Communications ISAC) operations. This includes managing the information sharing process, performing analysis, researching technical issues, coordinating and liaising, and related functions. Managing the information sharing process involves many specific functions, such as monitoring phones, monitoring and maintaining email on various unclassified and classified accounts, monitoring various systems and tools to extract information on impending events or threats, conferencing with other watch centers, coordinating with industry representatives, liaison partners, data providers, and other functional elements of the Department of Homeland Security, sanitizing data and coordinating approval from information owners for release and dissemination; and disseminating information and soliciting feedback A corollary function to management of the information sharing process are analysis efforts. The core business of the NCC Watch is to be the operational arm of the NCC, however, it is also responsible for triage of a number of other NCC functions such as Telecommunications Service Priority (TSP) and Government Emergency Telecommunications Service (GETS). Detailed guidance will be provided to the Contractor through NCC Standard Operating Procedures (SOPs) and supplemental Watch Internal Procedures to expand upon the information in the following paragraphs.

The Contractor shall assist the NCC with the goals of

- Maintaining the OMNCS as a leader in the telecommunications arena by demonstrating technical and operational capabilities for information collection, sharing, and analysis.

- Representing Communications CIP objectives and equities in the national CIP arena by collaborating with other stakeholders and influencing decision makers (e.g., Research and Development, standards, and policy).
- Demonstrating the value of sharing information through provision of Government information to industry. (Sanitization of classified and/or sensitive information will be required.)
- Improving protection of all infrastructures and demonstrating the value of cross infrastructure analysis by taking a leadership role in the ISAC community.
- Ensuring viability of the telecommunications infrastructure by continuing the leadership role in telecommunications CIP restoration planning, response, and recovery in an all-hazards environment.

through the execution of the following tasks:

- Coordinating policy, procedures, and issues with representatives of NCC and NCC Communications ISAC member companies and agencies
- Developing and coordinating procedures that will allow Government and industry to voluntarily report outages, anomalies, events, and intrusions that have NS/EP implications
- Drafting, coordinating, and implementing Standard Operating Procedures (SOPs) to carry out detailed ISAC functions
- Acting as liaisons with external organizations, for the purpose of establishing on-going relationships and information flow between them and the NCC Communications ISAC.
- Gathering, researching, and coordinating information related to potential impact on the virtual and physical telecommunications infrastructure/information networks, and contributing to analysis efforts where feasible.
- Drafting, coordinating, and obtaining approval for release of threat, vulnerability, information network attack, or other telecommunications-related information to NCC Communications ISAC member representatives.
- Monitoring the NCC Communications ISAC support tools and email accounts, inputting data, drafting alert notifications, and coordinating issues with NCC Communications ISAC member representatives
- Developing internal telecommunication infrastructure security strategies
- Developing warnings, advisories, and other urgent notifications to NCC Communications ISAC members, and other ISACs and liaison partners as appropriate, of a widespread attack, imminent attack, threat or anomaly
- Facilitating processing and sharing of all-source information, including classified and sensitive information
- Maintaining awareness of trends in the identification of intrusions, signs/symptoms of potential intrusions, outages, or widespread anomalous conditions.
- Drafting and coordinating requirements for automated support tools such as databases, correlation and analysis tools, notification tools
- Recommending alternatives to meet mission requirements.

5.2.1 Monitor NCC Communications ISAC Email Accounts.

Monitor various unclassified email accounts, SIPRNET (Secret level) email account, JWICS (top secret), and any other email accounts established to support the NCC and/or NCC Communications ISAC. Watch officers will be responsible to analyze email bulletins and other information from multiple sources, compare contents, and recommend handling response to NCC management and execute NCC management direction. Detailed guidance on managing, generating, and disseminating email will be provided in the NCC Standard Operating Procedures (SOPs) and Watch Internal Procedures. The following examples are illustrative, but not all-inclusive.

a. The following named-sources provide regular bulletins or alerts that may be openly re-distributed to NCC and NCC Communications ISAC members: DOE CIAC, CERT (Carnegie Mellon), NCSD's US-CERT (some products), and SANS Institute.

b. The following are some additional sources that may provide information on an ad-hoc basis. Information from these sources requires sanitization and specific approval for release to named recipients before dissemination, and most likely has limits on re-distribution:

- NCC Communications ISAC members: Inputs require sanitization, coordination with originator, and specific approval for release, as described in NCC SOPs and Watch Internal Procedures supplementing the SOPs.
- Joint Task Force- Global Network Operations (JTF-GNO)/ Dept of Defense Computer Emergency Response Team (DoD-CERT)
- US Computer Emergency Response Team (US-CERT)
- National Security Incident Response Center (NSIRC)
- Federal Emergency Management Agency (FEMA): Some products require sanitization and specific approval for release.
- DHS HITRAC (Homeland Infrastructure Threat and Risk Analysis Center)
- Other ISACs operational centers
- Other industry or government technical inputs

c. General tasks and procedure for distributing emails that do not require sanitizing, the following are exemplary and greater detail will be provided by NCC management personnel:

- Forward to the NCC Communications ISAC email list the first bulletin received from a known source on a particular topic (e.g., specific new cyber vulnerability).
- After forwarding, study the bulletin and research the links and background information provided in the bulletin, and consult other available sources (e.g. web sites, available experts). Consult with liaison partners, such as US-CERT, DoD-CERT, JTF, and other watch centers, other ISACs, for related information on this event, threat level, and extent of current or estimated damage.
- If a second bulletin on what appears to be the same topic, but from a different source, arrives, analyze the second bulletin for differences in content from the first bulletin.

- Prepare a second email for the Telecom ISAC email list. The email should point out the results of the analysis above (i.e., if the info is the same, but simply from another corroborating source, indicate so). If there are differences – highlight (e.g., "two new web links provided for related information, but the other information is the same as previous bulletin from Source x", or "this bulletin has more updated information on Topic abc than the previous bulletin from source x").
- Perform the same process of analysis, comparison, and consulting other experts for additional bulletins received on that same topic.
- Do not forward non-ISAC type information from these same sources (e.g. SANS course information) or US-CERT email directing federal agency compliance with patch updates.

d. General tasks for emails that require sanitizing (e.g. NCC Communications ISAC member inputs by email or phone). If current standard operating procedures do not clearly address the given situation, coordinate with the on-call Government NCC operations staff person prior to distribution of any notifications from sanitized sources.

- Same tasks as listed in paragraph c. above, and
- Coordinate with the originator for specific wording, elements to eliminate, headers and caveats to add, and authorized recipients and re-distribution. Ensure that the source's name, and any other identifying information, such as target IP addresses, email addresses, filenames, etc. are sanitized.
- For inputs by phone, provide the originator a draft of the proposed wording.
- The non-sanitized version and originating material will be maintained by the Watch via email archives, document archives, and station log at the appropriate level of classification.

5.2.2 Maintain Recipient E-mail Groups. In accordance with NCC SOPs and Watch Internal Procedures, maintain, create, and verify various email groups of authorized recipients.

5.2.3 Monitor other NCC Communications ISAC and Critical Infrastructure Support Systems and Tools.

a. Monitor all available NCC Communications ISAC support tools, monitoring systems, and automated information sources and takes appropriate action. Main areas to track are:

- incoming reports or message forum postings from NCC Communications ISAC members
- incoming reports, message, and calls from DHS and other Government partners
- monitor reports, message traffic, and notices pertaining to Emergency Support Function 2 (ESF2)
- changes or anomalous trends in Internet status, or "health" based on available sources
- significant new information on current exploits, vulnerabilities, threats, etc.

b. The following are the current and evolving NCS and DHS systems, sources, or capabilities where these efforts will focus:

- Useful information assurance websites, mostly open source; other classified sources as provided by the government
- Ad hoc exploit data, possibly to include source code, provided by government and industry liaison partners, or other sources
- Homeland Security Information Network (HSIN)
- Infrastructure Mapping Tool (IMT)
- IMAPDATA
- Network Outage Reporting System (NORS)
- Renesys
- Verisign Global Top-Level Domain (GTLD)
- Genscape
- Other systems, as available, supporting the research and analysis tasks of the Watch

c. Monitor and review analysis data provided to the NCC and NCC Communications ISAC by internal and external sources. External data may be intelligence of threats or vulnerabilities to the communications infrastructure. Data may also be reports of pending of occurring natural disasters impacting the communications and require collaborative analysis by industry and Government partners. Further, external data may include information regarding current exploit code events, along with raw binary executables being provided to a combined industry and government group for collaborative efforts in analysis.

- Use available sources to process, analyze, and correlate additional information relating to an incident, natural disaster, new anomaly, reported threat such as a virus or worm, or trouble tickets or messages posted to in NCS email. Analysis may require collaboration with members (when activated) of the Analysis Response Team (ART) which is a combination of government and Contractor support responsible for assessment of threats to communications infrastructure.
- Collaborate, where possible, with liaison partners' technical representatives to analyze and develop mitigation strategies to counter pending or current threats to the telecommunications infrastructure/information networks.
- If appropriate, research, draft, and coordinate NCC Communications ISAC bulletins or alert notifications or ESF2 Situation Reports for distribution to NCC Communications ISAC members and other authorized recipients.
- Based on available information, update the NCC Communications ISAC Situational Awareness Overview, a short bullet summary/display of current status (located in the NCC Operations Center).
- If Watch procedures are unclear, or the situation is sensitive, provide background information and recommendation for action to the on-call NCC government staff for decision.

5.2.4 Recommend Immediate Actions. Based on information provided by external sources through email or other means, and/or Telecom ISAC member inputs, analysis and coordination, recommend appropriate action for the NCC and Telecom ISAC.

- Make recommendation to on-call Government NCC operations staff and provide the on-call person with all pertinent background information.
- Coordinate with other parties as needed for approval to release their information to NCC Communications ISAC members, to include re-distribution within NCC Communications ISAC member companies/agencies to personnel with a need-to-know.
- Coordinate with originators of all information for approval for release of information to the NCC Communications ISAC members and re-distribution within their companies/agencies.
- Perform telephone/email contact as needed to alert NCC Communications ISAC member representatives of urgent notifications.
- Monitor automated alerting mechanisms (if installed) to verify that they are performing their functions correctly.
- Set up conference bridges as needed to discuss ongoing issues.

5.2.5 Maintain On-going Interface with NCC Communications ISAC Liaison Partners and Other Entities. In most cases, initial relationships will be established by the Government NCC operations staff, while the maintenance and enhancement of those relationships with the operational and technical contacts will be a responsibility of the NCC Watch.

- As much as permitted by the NCSD, JTF-GNO, and others, keep up-to-date on their ongoing communication/information system issues and threats, current operations, in particular where these issues may represent national trends that could affect NCC and NCC Communications ISAC members' infrastructures.
- Maintain interface with watch centers and designated points of contact within other entities such as other functional elements of the Department of Homeland Security, National Cyber Security Division's (NCSD) United States Computer Emergency Readiness Team (US-CERT), the National Infrastructure Coordination Center (NICC), the National Security Incident Response Center (NSIRC), and other watch centers, as appropriate.
- Maintain interface with other ISAC operational centers as specified in the Inter-ISAC Information Exchange Procedures.
- Maintain interface with NCC agency and NCC Communications ISAC industry representatives
- Maintain interface with other liaison partners, technical interchange and information sharing forums.

5.2.6 Protection of Materials. The Contractor shall be responsible for organization and maintenance of all NCC Watch documentation and support information and shall ensure that all materials including classified documents are appropriately backed up and secured in facilities and containers provided by OMNCS. The Contractor shall be responsible for protection of sensitive materials located at the Contractor's facility.

5.2.7 Perform NCC Triage. Perform triage and serve as 24 x 7 NCS and NCC Point-of-Contact focal point. Although its main focus is on virtual telecommunication issues and operation of the NCC Communications ISAC, the NCC Watch has responsibility to perform a triage function for other NCC functions, and to provide the after-hours point of contact for NCS. The following are the general tasks in this area:

- Perform a general "triage" function for calls or emails coming to the NCC Operations Center. Triage involves putting the caller in direct contact with the appropriate government point of contact to handle the caller's issue.
- Coordinate issues and contact the on-call Government NCC operations staff person, Emergency Operations Team (EOT) chief, or other appropriate NCS personnel, as needed. This may also include initial triage of inquiries regarding Telecommunications Service Priority (TSP) when the TSP point of contact is unreachable.
- Outside normal duty hours, answer all calls forwarded from the main NCC number, 703-607-4900. This number is also the 24-hour OMNCS contact.
- If on-duty Contractor personnel have SCI access, provide access to the OMNCS SCIF for pre-designated, authorized, and appropriately cleared government personnel, in accordance with the access list and procedures to be provided by OMNCS CIP Division, and activate/de-activate the video teleconference system.
- Use systems and tools provided in the NCC Operations Center to conduct emergency alerting of key personnel or initiation of changes in response levels or threat levels. The Contractor shall only be responsible for the correct use of these alerting tools.

5.2 Task 3 -Information Processing and Communication Support.

The Contractor shall assist in the oversight of the operational information systems in direct support of the NCC Watch, as directed and necessitated by NCC Management. Oversight is necessary to ensure that all appropriate software, and hardware are implemented to support the tools and utilities use by the NCC Watch.

5.3.1 The Contractor shall provide system administration of NCC networks and equipment at the NCC and alternate locations to ensure that the appropriate configuration, software and hardware are installed and operating correctly. The Contractor duties including assist in managing the process of maintaining networks, hardware, upgrading software, adding software, applying patches, documenting, and performing back-up and recovery operations. By managing the maintenance process, the Contractor will ensure that updates are performed correctly and in a timely fashion.

5.3.2 All operational information systems at all NCC operations and COOP locations will be accredited under the policies and processes specified in accordance with DHS policy and guidance. Provide technical and non-technical professional expertise to address life cycle security from inception of the program through accreditation, and obsolescence. Perform IA Information Technology assessments of proposed and existing DHS systems to include assessing and verifying information systems including trusted systems; identifying and assessing security

requirements and deficiencies in applications, systems, local and wide area networks (LANs and WANs) and commercial switching, transmission and signaling networks. Provide technical support to conduct Certification and Accreditation (C&A) using the Federal Information Security Management Act (FISMA) and DHS Certification and Accreditation. The Contractor shall conduct reviews and providing recommendations for resolution of inconsistencies within existing DHS C&A policies and procedures; monitor the implementation of, and compliance with, C&A standards within DHS. System configurations and accreditations will be documented in a government furnished database. Typical documentation for DHS C&A includes Contingency Plans, System Security Policies, Risk Assessments, Privacy Information Assessment, Privacy Threat Analysis, and Operating Procedures, and Program Objectives and Milestones.

5.3.3 Support the movement and relocation of the NCC infrastructure to DHS facilities at 1110 North Glebe Road, Ballston, VA. The Contractor shall participate in coordination meetings; document NCC relocation requirements; survey the new environment including physical and technical infrastructure; and make recommendations on how to maintain operations during transition. The Contractor shall develop a migration plan that addresses the establishment of the new location and acceptance test the fitness of this environment including feedback on the readiness to support NCC operations. The Contractor shall assist in addressing and mitigating any issues preventing this facility from assuming operations. The Contractor shall assist in the relocation of NCC resources including equipment, material, and documents. The Contractor shall assist with closeout of the Courthouse Road facility including movement of equipment, forwarding and closeout of email accounts, termination of connectivity, and working with NCS to satisfy Navy and Defense Information Sharing Agency (DISA) closeout requirements.

5.4 Task 4 - Intelligence Support.

The Contractor shall assist in the review, development, and dissemination of intelligence products to NCC community and the communications sector through interaction with private and public partners. The Contractor shall be responsible for maintaining and tracking material in accordance with prescribed security guidelines. The Contractor shall assist the NCC in forming and maintaining extensive liaison with local, national, and international contacts with the intelligence and law enforcement communities. The Contractor shall prepare position papers, briefings, and finished intelligence reports (basic-descriptive, current-reportorial, or speculative-estimate) for NCC, NCS, and DHS management. The Contractor shall assist in the development of sanitized and tear line material to facilitate information sharing.

5.5 Task 5 - Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) Communications Specialist.

HITRAC is the DHS fusion center for the production of sector specific threat and certain types of high-level risk analysis products. HITRAC is intended to foster a working relationship with intelligence professionals and sector security experts with the intent of producing analytic products enabling more complete and holistic understanding of the risks to U.S. Critical Infrastructure and Key Resources (CI/KR). The Contractor shall provide one full-time equivalent

communications security specialist with Top Secret (SCI) credentials to represent the NCS. Work will performed at a location in the National Capital Region as defined by the Government.

In support of this work, the Contractor shall:

- Review intelligence products providing CI/KR threats, vulnerabilities, consequences of attack, and protective measures.
- Assist in the production of standardized infrastructure-specific threat analysis on all U.S. CI/KR sectors which will support the NIPP and compliment other DHS risk-based efforts.
- Assist in the development and dissemination of intelligence products to DHS and the communications sector through interaction with private and public industry and capturing their requirements.

This HITRAC support shall be included in the award as a priced option to be executed, when required, for execution of specific intelligence review and threat assessment.

5.6 Task 6 – National Command and Coordination Capability (NCCC) Planning, Implementation Preparation, Federal Policy Assessment, and Support.

The Contractor shall propose as a mandatory option, when required by the Government, for planning efforts for implementation of the National Command and Coordination Capability (NCCC). The NCCC is the means to provide the President with the ability to respond deliberately and appropriately to any crisis. It includes responsive, reliable, survivable, and robust processes and systems to command, control, and coordinates operations among Federal, State, Tribal, Insular, and local governments, as well as private organizations, foreign governments, and international entities, as required. The NCCC efforts include the delivery of policy recommendations, operational concepts and technology solutions designed to provide shared collaboration/situational awareness, decision planning and execution, as well as other command, and coordination capabilities at all levels of government in all hazards. Significant support is required of the Departments and Agencies (D/As) for the successful development and implementation of the NCCC.

The Contractor will specifically be involved with:

- Reviewing the strategy, directives, and initiatives currently addressing the processes, procedures and systems that affect situational awareness, collaboration and information sharing, planning and decision-making capabilities
- Examining organizational and jurisdictional concerns.
- Supporting the identification of new capabilities and interoperability requirements
- Preparing/coordinating document deliverables and providing document configuration management
- Review, adjustment, and execution of the NCCC Implementation Plan

- Review and report on the Federal Policy Framework assessing statutory, policy, and procedural issues and barriers in legislation, directives, and national initiatives. Assessment will identify concept of operations, identification of roles and responsibilities, and highlight gaps and shortfalls.
- Providing program support in related tasking such as meeting coordination, drafting of memoranda, administrative support, drafting of presentations, etc. Support also includes development of tasks and management of implementation.

This NCCC support shall be included in the award as a priced option to be executed, when required, for planning and implementation.

5.7 Task 7 - Continuity Communications Architecture (CCA) Support.

In 2004, the National Communications System (NCS) Committee of Principals (COP) tasked the Continuity Communications Working Group (CCWG) with creating a method for studying the current state of telecommunications capabilities across the Federal Executive Branch (FEB). The goal of this effort was to ensure that each FEB Department and Agency (D/A) had the necessary communications/Information Technology (IT) systems capabilities to execute Mission Essential Functions (MEF) under all circumstances, at both their headquarters and alternate operating locations.

Several framework documents were created that proposed an architecture based on submissions of each D/A to the Office of Management and Budget. The methodology rationale was that each D/A could track communications expenditures in their budgets, which in turn could then be linked to their Priority Mission Essential Functions (PMEF), and thus eliminate more invasive data-collection techniques.

In the following year, a different approach was employed to:

- Continue the NCS tasking to complete the architecture mission;
- Normalize PMEFs and provide agency pass-back;
- Map communications requirements against PMEFs;
- Develop Enterprise Architecture and Transition Plans; and
- Assist D/As to procure communications systems to meet architecture framework.

The data-collection effort included creating a database management tool, and methodology for data analysis, as well as several site visits with each participating D/A to collect, update and validate all data they will have provided. The goal of this effort was the ability to generate multiple reports that highlight gaps and overlaps in communications capabilities that currently exist across the FEB and to provide a means to create a mitigation strategy to remove gaps and eliminate overlaps.

In May 2007, National Security Presidential Directive (NSPD) 51 and Homeland Security Presidential Directive (HSPD) 20 established a comprehensive national policy on the continuity

of Federal Government structures. In specific, paragraph 16 (h) states that the Secretary of Homeland Security shall "As Executive Agent of the National Communications System, develop, implement, and maintain comprehensive continuity communications architecture." Additionally, paragraph 16 (d) states "Conduct quarterly and annual assessments of continuity communications capabilities in consultation with an official designated by the Chief of Staff to the President."

In July 2007, NCS Directive 3-10 was published. This directive sets the minimum requirements for continuity communications capabilities for the FEB. With these authorities in place, the following tasking will be addressed to meet the requirements set forth in NSPD 51/HSPD 20 and NCS Directive 3-10.

(1) Supporting the development of baseline continuity communications architecture.
(2) Determining the adequacy of current communications and IT systems/applications capacity for the FEB and understanding future growth/modernization plans.
(3) Supporting PMEF development and mapping D/As PMEFs to the infrastructure to ensure continuity of National Essential Functions under all conditions.
(4) Coordinating minimum communications compliance.
    a. Developing processes, procedures and policy.
    b. Supporting testing for compliance.
    c. Creating plans for testing, exercise and evaluation, and outreach support to the community of interest.
(5) Ensuring Continuity Communications Architecture intersects and is compatible with existing/emerging programs such as the National Command and Coordination Capability and Emergency Communications.
(6) Supporting the coordination of and finalization of the draft NCSM 3-10-1, *Minimum Requirements for Continuity Communications Capabilities Users Manual*, and providing subsequent manual production requirements/updates as directed.
    a. Collaborating with GSA to identify minimum communications product candidates available through GSA as well as identifying sources for non-GSA available products
    b. Developing a minimum communications product catalogue for selection reference.
    c. Establishing NCS and GSA web pages for the community of interest.
(7) Attending meetings with government clients and interagency conferences in support of CCA development.
(8) Providing technical, analytical, and logistical support as needed to manage and facilitate all processes and procedures associated with CCA.
    a. Researching, creating and reviewing documents, providing analyses, subject matter expertise, synthesizing procedures, protocols, and other capabilities that would further the CCA effort.
    b. Providing strategic planning and transitional support as required.

This CCA support shall be included in the award as a priced option to be executed, when required, establishing a baseline, collection of requirements, providing technical and analytic support, and planning and implementation.

6. Deliverable/Delivery Schedule:

Days = calendar days unless otherwise specified
TM = Task Monitor
ATM = Alternate Task Monitor

SOW Task#	Deliverable Title	Due Date	Copies	Distribution	Frequency and Remarks
5.1 5.1.1	Management Plan	10 days after award	1 each	TM, ATM	
5.1 5.1.2	Weekly Informal Summary	Weekly	1 each	TM, ATM	Government will review within 3 workdays
5.1 5.1.3	NCC Watch Quarterly Program Management Review (PMR)	Every 90, 180, 270, 360 days after award	1 each	TM, ATM	Subsequent quarterly assessments will concentrate on the period since the last quarterly report.
5.1.1.2	Surge staffing	As required		TM, ATM	Will be negotiated at time of need
5.2	NCC procedures maintenance and creation	As required	TBD	TM, ATM	Identify updates and recommendations for procedure enhancement in quarterly PMR
5.2	Threat, vulnerability research, notice and alerts creation	As required	TBD	TM, ATM	Format will vary from email to position papers to presentations
5.2.3.c	Analysis reports and presentations, and situation reporting	As required	TBD	TM, ATM	Direction and format provided by Gov't at time of need
5.3.2	System Accreditation documentation maintenance and creation	Minimum yearly review and update of existing documents; Create as required	1 each	TM, ATM	Types of documentation required include System Security Policy, test and validation reports, privacy
5.4	Intelligence review and	As required	1 each	TM, ATM	Will be negotiated at time of need

	creation of notices, reports, and briefings				
5.5	HITRAC specialist				Will be negotiated at time of need
5.6	National Crisis Coordination Center				Will be negotiated at time of need
5.7	Continuity Communications Architecture (CCA) support				Will be negotiated at time of need

*Standard Distribution

- 1 copy of the transmittal letter and the deliverable to the Primary TM and Alternate TMs

The Contractor shall provide all final document deliverables in soft copy and hard copy as specified below. Daily, weekly, interim, informal deliverables, and working-copy products required for on-going general support may be provided by email or disk, as arranged. The Government may impose a maximum page limit on all deliverables, if it chooses.

- Soft copy (three each deliverable): Developed using the current DISANet version of Microsoft Word, PowerPoint and/or other DISA standard application software. Provided on a 3" high-density floppy disk (if space permits) or CD-ROM. If more than one deliverable is provided at the same time, deliverables may be included on the same disk or CD-ROM.
- Hard copy (one each deliverable): Typewritten on 8½" x 11" white paper, single-spaced, 12 pitch "Times New Roman" font, printed double-sided, and format at the discretion of the Contractor. The Contractor shall not use spiral binding or other binding that interferes with photocopying.

7. Government-Furnished Equipment (GFE)/Government-Furnished Information (GFI).

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

- Work space, with one each unclassified DISANET workstation and telephone for the watch officers and Watch Coordinator
- Containers for storage of documentation and references
- Access to DHS A, B, C LANs
- Access to a photocopier
- Access to printers (B/W and Color)
- Access to a scanner
- Access to a STU III/STE telephone
- Access to secure fax

- Access to a SIPRNET workstation (as required)
- Access to a internet gateway
- Access to a JWICS workstation for those with SCI access

GFI. The Government will furnish information to assist the Contractor in completing the tasks. This will include, but not be limited to, copies of all relevant documentation pertaining to the NCC and NCC Communications ISAC, NCC and OMNCS personnel contact information, and OMNCS and DISA procedures. It will also include data sources as available to the NCC and NCC Communications ISAC.

8. Place of Performance.

Work performed under this task order will be performed at a Government site currently on a military installation in Arlington, VA and a DHS facility in Arlington. The NCC Operations Center will be the main place of performance. As appropriate and agreed to by the NCC and the Contractor, contract personnel may be located to other desks to represent and support NCC operations, potential positions include but are not limited to JTF-GNO, the National Infrastructure Coordinating Center (NICC) currently located at the Transportation Security Administration's (TSA) Transportation Security Operations Center (TSOC) in Herndon, VA, the JTF-GNO located in Arlington, VA, the National Operating Center (NOC) in Washington, DC. In order to establish and maintain an integrated watch operation, all NCC Communications ISAC watch officers must vary their place of duty among all locations on a regular basis (where clearance permits). All watch officers, plus the Watch Coordinator will require access to all locations where NCC watch operations are located.

If the NCS contingency plan is activated, and the functions of the NCC and NCC Communications ISAC are required to re-locate, the place of performance will be at the OMNCS alternate sites: (primary) Mt Weather, near Berryville, VA, and Culpepper, VA. Specialized surge support may include a place of performance in the downtown Washington D.C. area.

NCCC and CCA work will largely be conducted at contractor facilities with frequent engagement at Government facilities primarily in the Washington National Capital Region.

9. Period of Performance.
This action is for a base period of fifty (50) weeks with three successive one-year option periods. Award is estimated for the end of September 2007 affording a transition period of 30 days.

10. Security.

a. Clearances.

For the period of performance covered by this SOW, the Contractor must provide personnel cleared at the Top Secret Sensitive Compartmented Information (TS/SCI) level. For Contractor personnel who have current Special Background Investigations (SBI) from non-DOD government organizations, the government will allow those personnel to perform work on the

NCC Watch for a limited amount of time at a Top Secret collateral level while their SCI clearances are being converted to the DoD/DHS system. The Contractor will coordinate cases when circumstances require a waiver of the TS/SCI clearance requirement. The clearance waiver option can only be exercised with written approval by the Task Monitor (TM).

The Government will provide cleared Contractor personnel access to appropriate DISA/OMNCS or DHS facilities. The Government will provide the Contractor escorted entry to controlled areas that are controlled beyond the level of access required by this task. All Contractor personnel should be capable of obtaining a TOP SECRET clearance with SCI access in accordance with DCID 6/4. All Contractor personnel shall wear badges or nameplates that identify the company or Contractor for which they work while performing any work related activity on Government facilities.

Contractor personnel used as administrative surge support as described in Place of Performance and Skill Sets Required are not required to have SCI access, but they must have final Secret clearances. Security shall be in accordance with the Contract Security Specifications contained in the DD Form 254.

11. Inspection and Acceptance.

a. Acceptance Criteria.

The Task Monitor (TM) and/or Alternate Task Monitor (ATM) will review all draft and final deliverables to ensure accuracy, functionality, completeness, professional quality, and overall compliance within the guidelines/requirements of the delivery order. 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, 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.

b. 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 updated/corrected version 10 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.

12. Other Pertinent Information or Special Considerations.

a. Identification of Possible Follow-on Work. Options as identified.

b. Identification of Non-Disclosure Requirements. Some material will contain proprietary, sensitive, or classified data from various public or private sources. All Contractor personnel performing work for the NCC Watch and Analysis Operation must sign non-disclosure agreements. The Contractor shall require all sub-contractors to sign corporate and individual non-disclosure agreements.

c. Intellectual Property Rights. All specified draft and final deliverables become the property of NCS. The details of any and all security countermeasures that the Contractor may develop under this contract, including software, will become the property of NCS.

d. Staffing.

Duty Shift. The Contractor shall perform work for 24 hours per day, 7 days per week, with specific shift hours to be agreed upon in advance, and to include provision for overlap between shifts to allow a sufficient time for turnover, and to include a reasonable number of surge support and specialized technical support hours.

Skill Sets Required.

The Contractor shall provide watch officer candidates with strong IT security backgrounds, and Watch Coordinator personnel with both management skills and strong IT security skills. There may be a mix of skill sets to include functional analysts, system administration, program management, and administration in order to best meet the needs of the NCC and NCC Communications ISAC. The Contractor shall obtain agreement from the government on a case-by-case basis prior to any deviation from staffing. As a baseline, all positions shall be trained to act as Watch Officers and must have the skills necessary to fulfill this duty.

If the level of activity for incident response involves significant increase in administrative effort as part of the Watch support services role in (for example, collecting, formatting, and providing information; document preparation), other labor categories may be used to assist the Watch personnel as surge support. This will allow the senior information assurance analysts/functional analysts/security engineers to focus on the core tasks requiring their skills. Acceptable labor categories are Intermediate Systems Operator, Editor/Analyst, Technical Specialist II, and Quality Assurance/Configuration Analyst I. The Contractor shall obtain agreement from the Government on a case-by-case basis regarding the use of these labor categories.

f. Travel.

Long-distance Travel. Long-distance travel may be required to other government or industry locations CONUS to participate in:

- quarterly NSIE meetings (one person)
- special project technical meetings
- other travel as indicated by the TM/ATM

Traveling Ceiling.
$9,064 for Base Period
$10,000 each for Option Periods 1, 2, & 3

The TM/ATM will review for approval all travel orders under this task order prior to the travel taking place. The Contractor shall provide sufficient advance notice and include the names of the travelers, dates and destination, purpose, and a breakdown of the estimated travel costs.

g. Other Direct Costs (ODCs). Where equipment or software is necessary to support watch operations including, but not limited to, the cyber health and early warning tools and assessment and the government is not able to provide the equipment or software in a timely manner, the Contractor shall furnish the missing items. The Contractor shall, with Government concurrence, shall train, test and demonstrate tools and capabilities to enhance NCC Watch operations. The Contractor may list known ODC requirements as options in its proposal, e.g. equipment and recurring costs. The Contractor shall include in its main proposal annual costs for a T-1 Internet connection at the primary site. The Contractor shall expect to incur no more than the ceiling amounts stated below:

ODC Ceiling.
$75,000 for the Base Period
$75,000 each for Option Periods 1, 2, 3

h. Enhanced Skills Training. In the event the Contractor would like to attend training that would provide benefit to the work being performed under this task order, the Contractor may request the TM approve attendance on a case-by-case basis. In the event the TM approves, the Contractor will be responsible for paying all tuition, per diem and travel costs, but may bill the labor hours to attend to this task order.

i. Non Disclosure of Protected Critical Infrastructure Information.

The parties agree to implement an interim rule promulgating new regulations at Title 6 Code of Federal Regulations Section 29.8 (c) to govern procedures for handling critical infrastructure information. The regulations detailed in the interim rule, which was effective upon publication pursuant to Section 808 of the Congressional Review Act, were promulgated pursuant to Title II, Section 214 of the Homeland Security Act of 2002, known as the "Critical Infrastructure Information Act of 2002" (CII Act).

The Contractor shall not request, obtain, maintain or use Protected CII without a prior written certification from the Protected CII Program Manager or a Protected CII Officer that conforms to the requirements of Section 29.8(c) of the regulations in the Interim Rule.

The Contractor shall comply with all requirements of the Protected CII (PCII) Program set out in the CII Act, in the implementing regulations published in the Interim Rule, and in the PCII Procedures Manual as they may be amended from time to time, and shall safeguard Protected CII in accordance with the procedures contained therein.

The Contractor shall ensure that each of its employees, consultants, and subcontractors who work on the PCII Program have executed Non-Disclosure Agreements (NDAs) in a form prescribed by the PCII Program Manager. The Contractor shall ensure that each of its employees, consultants and subcontractors has executed a NDA and agrees that none of its employees, consultants or sub-contractors will be given access to Protected CII without having previously executed a NDA.

j DHS Enterprise Architecture Compliance.

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures as it relates to this Statement of Work and associated Task Orders. 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.

13. Accessibility Requirements (Section 508).

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) 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 equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All 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 GOTS and 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.

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, applies to all telecommunications products including end-user interfaces such as telephones and non end-user interfaces such as switches, circuits, etc. 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, including but not limited to training deliverables, 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.

36 CFR 1194.31 – Functional Performance Criteria applies to all EIT deliverables regardless of delivery method. All EIT deliverable 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. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may 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 apply.

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.