AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT	1. CONTRACT ID CODE	PAGE OF PAGES 1 3

2. AMENDMENT/MODIFICATION NO.	3. EFF. DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
P00003	03/04/2007	(b) (2)	

6. ISSUED BY CODE (b) (2)

Department of Homeland Security
Customs and Border Protection
1300 Pennsylvania Ave NW
(b) (6)
Washington DC 20229

7. ADMINISTERED BY (If other than item 6) CODE

Dept of Homeland Security
Customs and Border Protection
Office of Procurement - (b) (6)
1300 Pennsylvania Ave. NW
Washington DC 20229

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and Zip Code)

THE BOEING COMPANY
(b) (6)

CODE 807414318 FACILITY CODE

9A. AMENDMENT OF SOLICITATION NO.

9B. DATED (SEE ITEM 11)

X 10A. MODIFICATION OF CONTRACT/ORDER NO. HSBP1006D01353

10B. DATED (SEE ITEM 13) 09/18/2006

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
X	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (Such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103 (b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor ☐ is not ☒ is required to sign this document and return 1 copies to issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this modification is to replace the Contract Security Classification Specification (DD 254); replace the SOW; revise clause G.2 of the contract; designate a new Contracting Officer; and correct contractor's DUNS number.

SEE CONTINUATION PAGE

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)	15C. DATE SIGNED
(b) (6) Contract Manager (b) (6)	3/16/08

16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	16C. DATE SIGNED
Maria Sands Contracting Officer (b) (6)	3/18/08

NSN 7540-01-152-8070
PREVIOUS EDITION UNUSABLE

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA FAR (48 CFR) 53.243

INFORMATION
FOR
AWARD/ORDER/IA HSBP1006D01353 , MODIFICATION P00003

SUMMARY OF CHANGES

1. The DD254 dated 20070220 is replaced by the DD254 dated 20080213 and is attached.

2. The Statement of Work (SOW) listed as Attachment 01 under Section J of the master contract is replaced by the attached revised SOW dated January 29, 2008.

3. The following clause has been changed from:

G.2 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE

a. The Contracting Officer's Technical Representative (COTR) for this contract is:

(b) (6)
1300 Pennsylvania Avenue, NW
Washington DC, 20229

(b) (6)

(b) (6) @dhs.gov

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]

TO:

G.2 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE

a. Contracting Officer's Technical Representatives will be assigned at the Task Order level.

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]

4. The Contracting Officers listed in Section G under this Contract is changed from:

Deborah L. Smith,
Ronald B. Rosenberg, and
Vernon Cooper

TO:

Jeffrey Gwilliam, Contracting Officer
U.S. Department of Homeland Security
U.S. Customs and Border Protection
Office of Finance
Secure Border Initiative Acquisition Office
1300 Pennsylvania Avenue, NW, (b) (6)
Telephone: (b) (6)
Fax: (b) (6)
Email: (b) (6) @dhs.gov

5. In P00002, Block 15A The Boeing Company, Arlington, VA DUNS number is incorrect. Block 15A is changed from:

The Boeing Company
(b) (6)

CODE 910425694

TO:

The Boeing Company
(b) (6)

CODE 807414318

ALL OTHER TERMS AND CONDITIONS OF THE CONTRACT REMAINS UNCHANGED.

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: **TOP SECRET**

b. LEVEL OF SAFEGUARDING REQUIRED: **SECRET**

2. THIS SPECIFICATION IS FOR: (X and complete as applicable)

X	a. PRIME CONTRACT NUMBER: **HSBP1006D01353**	
	b. SUBCONTRACT NUMBER	
	c. SOLICITATION OR OTHER NUMBER=	Due Date (YYYYMMDD)

3. THIS SPECIFICATION IS: (X and complete as applicable)

	a. ORIGINAL (Complete date in all cases)		Date (YYYYMMDD): 20070220
X	b. REVISED (Supersedes all previous specs)	Revision No.: 002	Date (YYYYMMDD): 20080213
	c. FINAL (Complete item 5 in all cases)		Date (YYYYMMDD):

4. IS THIS A FOLLOW-ON CONTRACT? [ ] YES [X] NO. If Yes, complete the following:

Classified material received or generated under _____ (Preceding Contract Number) is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? [ ] YES [X] NO. If Yes, complete the following:

In Response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____

6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)

a. NAME, ADDRESS, AND ZIP CODE	B. CAGE CODE	C. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
THE BOEING COMPANY **499 Boeing Blvd** **Huntsville, AL 35824**	**3A768**	**Defense Security Service (DSS)** **Bldg 3216 Little John Drive** **Huntsville, AL 35898**

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	B. CAGE CODE	C. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)

8. ACTUAL PERFORMANCE

	B. CAGE CODE	C. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
Department of Homeland Security (DHS) Washington, DC metropolitan area and the contractor facilities (SEE ITEM 13).		

9. GENERAL IDENTIFICATION OF THE PROCUREMENT

(U) Provide technical support and management support including research, development, design, test, and evaluation of components subsystems and systems to secure the US borders for DHS CBP.

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X
b. RESTRICTED DATA		X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X	
d. FORMERLY RESTRICTED DATA		X	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		X
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY		X
(1) Sensitive Compartmented Information (SCI)	X		f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
(2) Non-SCI	X		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	X	
f. SPECIAL ACCESS INFORMATION		X	h. REQUIRE A COMSEC ACCOUNT	X	
g. NATO INFORMATION		X	I. HAVE TEMPEST REQUIREMENTS		X
h. FOREIGN GOVERNMENT INFORMATION		X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		X
I. LIMITED DISSEMINATION INFORMATION		X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X
j. FOR OFFICIAL USE ONLY INFORMATION	X		I. OTHER (Specify) See Block #13.		X
k. OTHER (Specify)		X			

DD Form 254, DEC 1999

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release

[ ] Direct [X] Through (Specify): **NONE AUTHORIZED**

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review. In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. Security Guidance. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Reference Item 10a & 11h: Contractor is authorized to use U.S. Government cryptographic equipment. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level. Further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior approval of the contracting activity." Contractor shall contact the DHS COMSEC Control Office of Record (COR), at Commercial (540) 542-3848, to receive current COMSEC guidance. "Contractor shall verify that a COMSEC clearance was approved and established by DHS, by contacting the DHS COMSEC Control Office of Records, Scott Oglesby at Commercial 540-542-3848, Contractor shall request COMSEC guidance and verify that a copy of the CANISPOM was requested on their behalf from NSA".

Reference 10e. (1)(2), SCI/Non-SCI: All contractor personnel assigned to this contract shall possess security clearances issued by the Defense Security Service (DSS) commensurate with the level of required access to classified information that is directly in support of this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor-generated Confidential clearances are not eligible for access to classified information released or generated under this contract. Contractor personnel who are specifically designated as requiring access to Sensitive Compartmented Information (SCI) must be eligible under the provisions of DCID 6/4 without exception. Personnel will be submitted for access by their DHS manager and verified by their Contract Technical Representative. If approved for access, they will receive an indoctrination briefing by DHS security staff prior to being granted access to SCI. All personnel security reporting requirements of DCID 6/4 will be made directly to the DHS SSO. Prior to leaving this contract, personnel will be scheduled for debriefing with the DHS SSO or by calling (202) 282-8643. ***Safeguarding level is for non-SCI only. Access to SCI will be at DHS facilities only.*** For the purposes of this contract, the contractor is not authorized to process and/or store SCI information at contractor locations.

14. ADDITIONAL SECURITY REQUIREMENTS. **Requirements** identify the pertinent contracted clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.) [ ] Yes [X] No

15. INSPECTIONS. **Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 If additional space is needed.)** [X] Yes [ ] No

"DHS (b) (6) VES THE "NEED-TO-KNOW" AT THE SCI LEVEL"

"**Clearances:** Access to Intelligence information requires a final US Government clearance. **Subcontracting:** Subcontracting requires prior approval of the GCA. **Briefings:** Special briefings and procedures are required. DSS does not conduct inspections for Sensitive Compartmented Information (SCI), but must inspect non-SCI intelligence material the contractor possesses.

16. CERTIFICATION AND SIGNATURE. **Security requirements stated herein are complete and adequate for safeguarding the classified Information to be released or generated under this classified effort. All questions shall be referred to the official named below.**

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE (Include Area Code)
(b) (6)	Program Manager Industrial Security	(b) (6)

d. ADDRESS (Include Zip Code)	17. REQUIRED DISTRIBUTION	
Department of Homeland Security 301, 7th & D Street S.W. Washington D.C. 20528	[X]	a. CONTRACTOR
	[ ]	b. SUBCONTRACTOR
	[X]	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE (b) (6)	[ ]	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	[X]	e. ADMINISTRATIVE CONTRACTING OFFICER
	[X]	f. OTHERS AS NECESSARY

8. ACTUAL PERFORMANCE		
a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
McDonnell Douglas Corporation The Boeing Company (b) (6)	18355	Defense Security Service (b) (2) One Pacific Plaza 777 Center Avenue, (b) (6) Huntington Beach, CA 92647
a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
The Boeing Company (b) (6)	1J649	Defense Security Service (b) (2) 1340 Braddock Place, (b) (6) Alexandria, VA 22314
a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE(Name, Address, and Zip Code)
Boeing Service Company (b) (6)	54669	Defense Security Service (b) (2) 5800 E. Campus Circle Drive, (b) (6) Irving, TX 75063
a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE(Name, Address, and Zip Code)
The Boeing Company (b) (6)	2D627	Defense Security Service (b) (2) Industrial Security Field Office 10040 N. 25th Avenue, (b) (6) Phoenix, AZ 85021-1647
a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE(Name, Address, and Zip Code)
Autometric Incorporated (b) (6)	2R708	Defense Security Service (b) (2) 1340 Braddock Place, (b) (6) Alexandria, VA 22314
a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE(Name, Address, and Zip Code)
The Boeing Company (b) (6)	33472	Defense Security Service (b) (2) 1250 Oakmead Parkway, (b) (6) Sunnyvale, CA 94085-4030
a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE(Name, Address, and Zip Code)
McDonnell Douglas Helicopter Company DBA: The Boeing Company (b) (6)	8V613	Defense Security Service (b) (2) Industrial Security Field Office 10040 N. 25th Avenue, (b) (6) Phoenix, AX 85021
a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE(Name, Address, and Zip Code)
The Boeing Company (b) (6)	1WX73	Defense Security Service (b) (2) 1340 Braddock Place, (b) (6) Alexandria, VA 22314
a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE(Name, Address, and Zip Code)
Boeing Service Company (b) (6)	3L1K7	Defense Security Service (b) (2) 5540 N. Academy Blvd., (b) (6) Colorado Springs, CO 80918
a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE(Name, Address, and Zip Code)
The Boeing Company (b) (6)	0BCT4	Defense Security Service (b) (2) 5540 N. Academy Blvd., (b) (6) Colorado Springs, CO 80918

DD254 BLOCK #13. CONTINUATION SHEET

The Boeing Company [redacted] **CAGE CODE: 3A768**
Contract #HSBP1006D01353

Reference 10e. (1)(2), SCI/Non-SCI (CONTINUATION):

a. All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).

b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.

c. All Contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access.

d. Inquiries pertaining to classification guidance on SCI will be directed to the Special Security Officer (SSO).

e. SCI furnished in support of this contract remains the property of the Department of Homeland Security (DHS), agency, or component originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the Contract Officer.

f. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

Reference10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD 11042.1) "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated Jan 6, 2005. DHS contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on handling DHS FOUO shall contact DHS OS ASD at [redacted]."

Reference Item 11c: The contractor shall use **(DHS SCG CBP-001 "SBI" Secure Border Initiative)** for classification of information associated with this effort. Additionally, the contractor shall derivatively classify newly created information associated with this effort based on the classification guidance provided through existing classified sources. All classified information shall be marked in accordance with the NISPOM. The ISOO Pamphlet on "Marking Classified National Security Information" dated March 25, 2003, may be used as a guide on the proper marking of classified information. Questions relating to Marking Classified National Security Information can be addressed to DHS Office of Security Administrative Security Division, at telephone [redacted].

Reference Item 11g: The contractor is authorized the use of Defense Technical Information Center (DTIC) Services as required. A DD Form 1540 and 2345 must be submitted for registration with DTIC. The contracting activity must certify need-to-know. See NISPOM Chapter 11, Section 2.

January 29, 2008

CONCEPT OF OPERATIONS INDEFINITE DELIVERY INDEFINITE QUANTITY (IDIQ)
REVISED STATEMENT OF WORK (SOW)

-- ATTACHMENT 01 -

Department of Homeland Security (DHS)/ U.S. Customs and Border Protection (CBP) Secure Border Initiative (SBInet)

Concept of Operations Indefinite DeliveryIndefinite Quantity (IDIQ)Statement of Work (SOW)
Table of Contents

1 Vision of the Secure Border Initiative (SBI)net Program....1
2 Purpose....1
3 Background....1
4 Scope of Work....2
5 SBInet Program Objectives....3
6 Technical and Management Requirements....3

6.1 Mission Engineering Task Area....3
6.1.1Systems Analysis and Architecture (1.1.9.2)....4

6.1.1.1 Modeling and Simulation (1.1.9.2.1, 1.2.2.4)....4

6.1.1.2 Concept of Operations (1.1.9.2.2)....4

6.1.1.3 Trade Studies (1.1.9.2.3)....4

6.1.2 Operations & Maintenance Planning (1.1.9.4)....5

6.1.3 Program Operational Metrics (1.1.1.2)....5

6.2 Technology Development Task Area....5

6.3 Prime Mission Product Task Area....5

6.3.1 Field Agent Systems....5

6.3.2 Surveillance and Detection Systems....5

6.3.2.1 Fixed Surveillance and Detection Systems....5

6.3.2.2 Airborne Sensors....6

6.3.2.3 Marine Sensor Systems (1.2.4.2)....6

6.3.2.4 Sensor Processing....6

6.3.2.5 Inspection Systems....6

6.3.3 Command Control and Communications Systems....6

6.3.3.1 Common Operating Picture....6
6.3.3.1.1C2 Software (1.2.3.2)....6
6.3.3.1.2C2 Integration (1.2.3.3)....6

6.3.3.2 Case Processing Systems....7

6.3.3.3 Intelligence Systems and Applications....7

6.3.3.4 Wireless Communications....7

6.3.3.5 Information Technology (IT) Infrastructure....7

6.3.4 Mobile Response Platforms....8

6.4 Facilities and Infrastructure Task Area....8

6.4.1 Tactical Infrastructure....8

6.4.2 Facilities....8

6.4.2.1 SBInet Facilities....8

6.4.2.1.1 Land-Use Regulatory Activities (1.1.6, 1.2.1.9)....8

6.4.3 Environmental (1.1.6, 1.2.1.9)....9

6.5 Systems Engineering Task Area....9

6.5.1 Engineering Management (1.2.2.1)....9

6.5.2 Architecture (1.2.2.3)....10

6.5.3 Life-Cycle Cost/Affordability (1.1.9.1.1)....10

6.5.4 Configuration and Data Management (1.1.9.1.2, 1.2.1.3)....10

6.5.5 Requirements Management (1.1.9.1.3)....10

6.5.6 Requirements, Interfaces, and Verification (1.2.2.2)....10

6.5.7 Product Design (1.2.2.5)....10

6.5.8 Software Management (1.1.9.1.4, 1.2.2.8)....11

6.5.9 Risk Management (1.1.4, 1.2.1.7)....11

6.5.10 Specialty Engineering (1.2.2.6)....12

6.5.11 Product/Process Improvement (1.1.9.1.5)....12

6.6 Test and Evaluation Task Area (1.1.9.3)....12

6.6.1 ITV Planning (1.1.9.3.1)....12

6.6.2 Integration Lab (1.1.9.3.2) 13

6.6.3 Test and Evaluation (1.2.2.7) 13

6.6.4 Integration (1.2.2.9) 13

6.6.5 System Acceptance Testing (SAT) (1.2.9.2) 13

6.7 Training Task Area (1.3.1) 13

6.8 Integrated Logistics Support Task Area 13

6.8.1 Asset Management (1.2.1.4) 14

6.8.2 Hardware Maintenance (1.3.2) 14

6.8.3 Software Maintenance (1.3.4) 14

6.8.4 Spares and Inventory (1.3.3) 14

6.9 Deployment and Installation Task Area (1.2.9.1) 14

6.10 Operations Support Task Area 14

6.10.1 Operations Support (1.3.6) 14

6.10.2 Customer Support (Help Desk) (1.3.5) 14

6.10.3 Information Technology (IT) Systems Support (1.3.7) 14

6.11 Program Management Task Area 15

6.11.1 Program Management Office (1.1.1) 15

6.11.1.1 Program Manager/Deputy/Chief Engineer (1.1.1.1) 15

6.11.1.2 Program Coordination and Administrative Support (1.1.1.2) 15

6.11.2 Project (Task Order) Office 15

6.11.2.1 Project Manager (1.2.1.1) 15

6.11.2.2 Project Coordination and Administrative Support (1.2.1.2) 15

6.11.3 Business Management (1.1.2) 15

6.11.3.1 Cost and Schedule Management (EVMS) (1.1.2.1, 1.2.1.5.1) 16

6.11.3.2 Contracts Management (1.1.2.2, 1.2.1.5.2) 16

6.11.3.3 Task Order Preparation (1.1.2.3) 16

6.11.4 Supplier Management and Procurement (1.1.3, 1.2.1.6) 16

6.11.5 Security (1.1.8, 1.2.1.11) 17
7 Assumptions and Constraints 18

7.1 Assumptions 18

7.2 Constraints 20
8 Schedule of Deliverables 22

The vision of SBInet is to provide an integrated defense-in-depth that will support the interdiction of illegal immigration and internal and external threats operating in or moving through the international borders with Canada and Mexico. SBInet will support a border security awareness capability that:

Reduces the United States of America's (USA) vulnerability to terrorism and protects national interests while enhancing Customs and Border Protection's (CBP) border security and control missions.

Supports CBP's strategic, operational, and tactical decision-makers.

Provides CBP with the optimum mix of personnel, technology, infrastructure, and response platforms to detect, identify, classify, and respond to illegal breaches of the international borders with Canada and Mexico and thereby bring the situations to the appropriate law enforcement resolution.

Provides the decision support information to support a common operational picture (COP) and an accurate assessment of the operational environment.

Provides members of the border enforcement community with the information necessary to support homeland security strategies and plans for unity of effort.

2 Purpose

The purpose of this document is to serve as an omnibus statement of work under which task orders and delivery orders may be issued and cross-referenced.

When coupled with the work breakdown structure this document is a framework for defining the technical objectives of the Contractor's SBInet program. The statement of work (SOW) is the document that describes what products are to be delivered and what services are to be performed by the Contractor. This document is intended to define and describe the actual work to be performed at the Task Area level as opposed to definitive task statements. Definitive task statements will be defined separately in individual task orders issued under this contract.

3 Background

The Department of Homeland Security (DHS), Secure Border Initiative (SBI) is a comprehensive approach to immigration enforcement. The SBI focuses broadly on two major enforcement themes: controlling the border and immigration enforcement within the USA. Border control means gaining full control of the USA borders so illegal immigration as well as security breaches can be prevented. Enforcement inside the USA means locating and removing aliens who are present in the USA in violation of USA laws. This pillar is tied to the President's proposal for a temporary worker program, which will make broader and more aggressive enforcement practical.

In developing the SBI, DHS is taking an integrated systems approach to the problem. The entire immigration enforcement system requires review, beginning with the gathering of immigration-specific intelligence and the detection of illegal border crossings, followed by apprehension, processing, transportation, and detection of the alien, and ending with the alien's removal from the USA. Adding agents at the border is insufficient unless they can be given the technology they need and the USA detains and removes the aliens they catch. A systematic approach will deploy all of these tools in stages, allowing each stage to build on the success of earlier stages.

CBP, SBInet

The SBInet unified border control strategy encompasses both the northern and southern land borders including the Great Lakes, and the interdiction of cross-border violations between the ports and at the official ports of entry (POEs). This strategy will funnel traffic to the USA through POEs where DHS has a greater level of control. The border environment is extremely complex, encompassing rural, urban, and remote areas as well as extreme climate variations and terrain.

Therefore, SBInet as a border control tool must be flexible and capable of being implemented in a manner that best suits these needs and requirements. Control of the border requires that four key

elements be met. These four elements are:

1 Detect an entry when it occurs;
2 Identify what the entry is;
3 Classify its level of threat (who the entrant is, what the entrant is doing, how many, etc.) (Note: this element must be met prior to the point of interdiction/encounter by law enforcement personnel.);
4 Respond effectively and efficiently to the entry, and bring the situation to the appropriate law enforcement resolution. Note: The appropriate law enforcement resolution does not end with the apprehension / interdiction. It must include the ability to efficiently transport from the point of interdiction to processing, and the ability to access appropriate databases during processing to gather and share information about and relating to the person in custody or under investigation.

Border control is achieved in a given area when CBP is able to consistently meet all four of the above elements in that area.

Managing, securing, and controlling the border requires determining the optimum mix of personnel, technology, infrastructure, and response platforms to achieve maximum tactical and strategic advantage in each unique border environment. Risk-based deployment and implementation of the solution; along with a new regime of complementary policies, processes and/or enhanced processes, regulations, and legislation; will further enhance tactical advantage.

CBP recognizes that existing capabilities to secure the border are limited in the current threat environment. The capabilities and capacity do not incorporate the optimal mix of personnel, processes, technologies, infrastructure, and response platforms to support the desired operational environment. Finally, the required capabilities have not been integrated into a "system-of-systems," and do not provide a clear COP.

The CBP SBInet component of SBI applies that comprehensive approach to securing the land borders at and between the POEs. The initial focus of SBInet will be between the POEs. Further, there is a requirement to build a COP of the border environment, within a command center environment, which will provide commonality within DHS components, and interoperability with stakeholders who are external to DHS. SBInet is the most comprehensive effort in the nation's history to gain control of the nearly 6,000 miles of international land border.

SBInet requires a comprehensive and aggressive strategy that will deploy the optimum mix of personnel, processes, technology, and infrastructure in a manner that will significantly reduce the probability of illegal entries and successful cross-border violations into the USA and maintain control of the border.

Scope of Work

The scope of this indefinite delivery, indefinite quantity (IDIQ) contract is the full range of services, products, and management required to accomplish the SBInet program objectives. This includes solutions based on the optimum mix of personnel, processes, infrastructure, technology, and response platforms that address all components of border security, and deploying the solutions to move from the current border strategy to one where the defined border areas are effectively secured. Advances in technology and other components of the solution must be accommodated to support continuous improvement in achieving SBInet program objectives.

The IDIQ contract will be for a three-year base period with three one-year options. The geographic coverage includes the northern and southern land borders of the USA, including the Great Lakes. The geographic coverage may be expanded to other USA border areas beyond those defined above.

The SBInet IDIQ contract will allow for performance-based task and delivery orders. Orders may be fixed price and cost type, as appropriate to the requirement. Applicable contract clauses and

provisions will be incorporated by reference into individual orders. Incentive provisions will be an important aspect of orders to ensure alignment of Government and Contractor goals and objectives. CBP expects that order incentive provisions will include plans to control performance, cost, and schedule

through monetary and non-monetary incentives and disincentives. CBP will develop a collaborative partnership between CBP, the Contractor, other stakeholders, and government Contractors. The SBInet Contractor's solution shall align with the goals and objectives of DHS and CBP. Within the context of the CBP/Contractor partnership, CBP does not use the term "partner" and "partnership" in the legal sense. Instead the CBP/Contractor partnership will reflect an open, collaborative, and customer-oriented relationship in which the Contractor and CBP will work together to achieve the program objectives and attain border control.

5 SBInet Program Objectives

To support the objectives of the SBInet Program, the Contractor will:

1. Develop a highly reliable, available, maintainable, and cost effective solution(s) to manage, control, and secure the border using the optimal mix of proven current and next-generation technology, infrastructure, personnel, response capabilities, and processes that will:

□ a. Detect an entry when it occurs;
□ b. Identify what the entry is;
□ c. Classify its level of threat (who it is, what the entrant is doing, how many, etc.) (Note: this element must be met prior to the point of interdiction/encounter by law enforcement personnel);
□ d. Respond effectively and efficiently to the entry and bring the situation to the appropriate law enforcement resolution.

1 Develop a near-real-time COP of the border environment, which provides commonality within DHS components and interoperability with other federal, state, local, and tribal partners outside of DHS. The COP must provide a mechanism that communicates comprehensive situational awareness, including information incorporating intelligence-driven operations capabilities at all operational levels and locations.
2 Throughout the term of the contract demonstrate continuous improvement in performance and reliability, and reduction in total operating cost.
3 Align its interests, motivation, and behaviors and that of its team members and subcontractors with those of the Government.
4 Maintain the highest level of service consistent with cost effectiveness. Provide and document audit and oversight activities that facilitate external reviews and assessments to prove that DHS is receiving superior supplies and services at fair and reasonable prices.
5 Establish a flexible, transparent, and responsive performance management information system that provides insightful, accurate, and timely information on both program status as well as performance reporting against mission measures and metrics.
6 Develop a solution that supports DHS compliance with Government standards and identified constraints.
7 Promote productive relationships with small business subcontractors and team members under the small business program as detailed in FAR Part 19 and in accordance with CBP goals and objectives.

6 Technical and Management Requirements

The technical and management activities supported under this contract include the Task Areas described below. The Contractor shall perform all activities in the following Task Areas through orders issued against this contract. The Contractor shall ensure that the work defined in these activities is integrated at the program level. Paragraph reference numbers in parentheses have been included to provide traceability to the Contractor's original proposal WBS.

6.1 Mission Engineering Task Area

The Mission Engineering task area includes the Modeling and Simulation activities supporting Systems analysis and Architecture definition, refining the SBInet Concept of Operations, Trade Studies and analytical activities, Operations and Maintenance Planning, and the Program Coordination and Administration activities associated with the planning, preparation, collection and analysis of operational

metrics.

6.1.1 Systems Analysis and Architecture (1.1.9.2)

6.1.1.1 Modeling and Simulation (1.1.9.2.1, 1.2.2.4)

This task is to develop and validate models necessary to design and effectively predict border security system-of-systems architectures and concepts of operations. The intent is not to develop new models or simulations. The intent is to create models using combinations of existing modeling and simulation tools to find the appropriate model variable and constant input values, develop input scripts, and perform analysis on the output scripts. It includes reviewing and updating the needs statement for each model. Included in this task are the following:

Border Threat Migration Model. Develop and validate the Border Threat Migration Model using the SEAS and Rampart modeling tools to meet Task Order requirements. Run simulations and models to accomplish the Task Orders. Develop and present Pre- and Post-Run briefings, provide reports, and attend meetings to support the SBInet Architecture.

Sensor Placement Optimization Model. Develop and validate the Sensor Placement Optimization Model using the SEAS, Rampart, and OPNET modeling tools to meet Task Order requirements. Run simulations and models to accomplish the Task Orders. Develop and present Pre- and Post-Run briefings, provide reports, and attend meetings to support the SBInet Architecture.

Business Process Model. Develop and validate the Business Process Model using BAM and EXTEND modeling tools to, meet Task Order requirements. Run simulations and models to accomplish the Task Orders. Develop and Present Briefings both Pre- and Post-Runs, provide reports, and attend meetings to support the SBInet Architecture.

Cost Comparison Model. Develop and validate the Cost Comparison Model using the BACEM modeling tool to meet Task Order requirements. Run simulations and models to accomplish the Task Orders. Develop and present Pre- and Post-Run briefings, provide reports, and attend meetings to support the SBInet Architecture.

Force level models will also be used to manage the border environment. This includes the SEAS and Rampart modeling tools to determine asset locations and effectiveness. The models will be used to determine optimal sensor locations and pre-position BP assets. In addition, business process models will be used to simulate the time it takes to process and deport an alien. These flow models will be critical in sizing parameters within the fielded system. The CAIV models, using BACEM to determine the most cost-effective system to be fielded, shall also be incorporated. All of these models can be linked together either manually or automatically to iterate to the best fielded system possible.

6.1.1.2 Concept of Operations (1.1.9.2.2)

With the support of the CBP program office, document the SBInet concept of operations following the process defined in the System Engineering Master Plan. This will include system trade studies and system simulation results to date, the integration of SBInet organizations and systems, and integration with external agencies and systems.

6.1.1.3 Trade Studies (1.1.9.2.3)

Conduct trades studies to establish the SBInet architecture's (1) detail design, (2) component selection, and (3) system deployment. Trade studies shall adhere to a standard process. This process includes (1) establishing criteria, (2) defining

alternatives, and (3) analyzing alternatives relative to criteria and selection. This process also uses

simulation models, analyzes all pertinent requirements, and determines system measure of effectiveness.

6.1.2 Operations & Maintenance Planning (1.1.9.4)

Operations Planning develops and implements the Integrated Maintenance and Support Plan. Operations Planning also ensures the proper data accumulation and preparation for LCCM team CDRLs. The plan integrates the LCCM and Asset Management function reports.

6.1.3 Program Operational Metrics (1.1.1.2)

Program Administration and Coordination personnel accumulate, analyze, and disseminate program operational metrics. Program operational metrics are defined in the Quality Assurance Surveillance Plan (QASP).

6.2 Technology Development Task Area

Partnering with CBP, the Contractor shall establish a joint Integrated Deployment Team to refine the deployment approach. The team, organized by Sector, will consist of CBP sector experts and be jointly coordinated from Washington, D.C. The first sector deployed will be the path finder for each subsequent sector, depending on that sector's specific needs. The Contractor shall continually measure capability effectiveness and, together with CBP, shall identify future technological enhancements. This will feed an ongoing Capability Roadmap that identifies improvements necessary to enhance performance.

New technologies shall be assessed and proven in two ways: (1) operationally through pilots in CBP Sectors, and (2) through the Integration Center (IC). The IC shall (1) assess and qualify new technology and processes; (2) test, assess, certify, and deploy low-risk, common, reliable, modular, architecture components across the networked SBInet system; and (3) integrate with the CBP COP.

6.3 Prime Mission Product Task Area

The Contractor shall provide the Department of Homeland Security (DHS) and U.S. Customs and Border Protection (CBP) a comprehensive solution to the challenge of detecting, apprehending, and processing people who cross our borders illegally and/or smuggle personnel and contraband between the Ports-of-Entry or through the Ports-of-Entry. The solution will not only meet the U.S. Border Patrol's two primary border control goals (i.e. detecting illegal crossings of our borders and effectively responding to those detected), but will also seamlessly integrate with the overall Secure Border Initiative, including other efforts to reduce illegal immigration, such as the detention and removal function carried out by the Bureau of Immigration and Customs Enforcement (ICE).

This solution includes a toolbox of technologies for unique border environments. Components are common across border environments for efficient deployment, training, maintenance, and integration with other government systems.

The Prime Mission Product described herein includes four segments per the Government Work Breakdown Structure (GWBS): (1) field agent systems, (2) surveillance and detection systems, (3) command, control, and communications systems, and (4) mobile response platforms.

For this section the specific hardware items and quantities are identified in the SBInet Bill-of-Materials.

6.3.1 Field Agent Systems

Field Agent systems include communication and COP-related components that are deployed in the field with the agent or in the agent vehicle. Definition of specific items proposed as Field Agent Systems (delineated below) is included in the SBInet Equipment and Services Bill-of Materials (BOM).

6.3.2.1 Fixed Surveillance and Detection Systems

- Satellite Phones (1.2.6.3).
- C2 Hardware (Laptop, Tablet, PDA, Radios) (1.2.3.1).

6.3.2 Surveillance and Detection Systems

The Contractor shall provide a toolbox of proven technologies for improved surveillance, detection, and identification capabilities across all border environments. In urban environments, detection tools, such as legacy tools and new cameras, sensors, agent surveillance tools and fencing infrastructure, shall be integrated to provide a complete detection solution. In rural and remote land border areas, detection will be based heavily on ground-based radar (transportable and fixed). In land border areas where ground-based radar coverage is obscured, the Contractor will use a combination of enhanced Unattended Ground Sensors (UGS) and mobile Electro-Optical (EO) and Infrared (IR) camera payloads, in addition to existing CBP aircraft. In water environments (i.e. Great Lakes, Falcon Reservoir, and the St. Lawrence Seaway), the Contractor will use a combination of radar, waterborne, shore-based sensors, and airborne assets to detect illegal crossing activity. Definition of specific items proposed as Fixed Surveillance and Detection Systems (delineated below) is included in the SBInet Equipment and Services Bill-of-Materials (BOM)

- Imaging (1.2.4.1).
- Radar (Land) (1.2.4.2).
- UGS (1.2.4.3).
- Fixed Active Barriers (1.2.7.1.1.2).

6.3.2.2 Airborne Sensors

The Contractor shall provide new communications for existing aircraft sensors and cameras to integrate with the COP.

6.3.2.3 Marine Sensor Systems (1.2.4.2)

Marine radars shall be deployed for surveillance and detection of incursions across water borders (i.e. lakes, rivers).

6.3.2.4 Sensor Processing

The Sensor Signal Processing functions of acquiring, processing, and correlating sensor data are included in the SOW paragraphs for the Common Operating Picture (COP) 6.3.3.1.

6.3.2.5 Inspection Systems

6.3.3 Command Control and Communications Systems

6.3.3.1 Common Operating Picture

The Contractor shall provide a multi-level, real-time, Common Operating Picture (COP) of the environment, assets, and actions occurring at the northern and southern U.S. border regions and ports of entry. The COP solution shall provide mutually agreed upon levels of situational awareness and visibility to CBP and DHS. The situational awareness and visibility shall be in accordance with security guidance assigned to SBInet. This solution will increase the operational efficiency and effectiveness of currently deployed CBP assets and personnel, as well as provide a framework for long term growth, technical insertion of new monitoring capabilities and integration of personnel assets in to a functional and scaleable command and control system.

The COP is a geospatially-aware framework that visually represents sensor inputs, vector and raster-based map data, deployed assets/resources, known targets of interest and allows for the control of these dissimilar entities throughout the area operation.

6.3.3.1.1 C2 Software (1.2.3.2)

C2 Software development includes acquiring the basic Intergraph I/CAD software suite and developing the necessary sensor and communications interface and display provisions required to tailor the

Intergraph I/CAD system or other COTS, GOTS, or custom-developed software and systems. This provides a multi-level, real-time, common operating picture of the environment, assets, and actions occurring within the northern and southern U.S. border regions and at the Ports of Entry (POE).

6.3.3.1.2 C2 Integration (1.2.3.3) C2 integration includes the definition and implementation of the COP within the SBInet system-ofsystems. Interface protocols and provisions to external databases and open-source intelligence systems shall be defined and the COP deployment increments will be integrated into a cohesive national system.

6.3.3.2 Case Processing Systems

The SBInet information infrastructure shall support secure data communication and database interoperability necessary for the implementation of case processing provisions to improve generation, filing, and sharing of illegal immigrant case-related information within and among CBP, DRO, and other law enforcement agencies.

6.3.3.3 Intelligence Systems and Applications

The Contractor shall use open-source intelligence to anticipate smuggling and illegal crossing trends based on geo-political and other developments in Canada, Mexico, and Central and South America, and based on tactical intelligence from border towns. A commercial service (IJET), already being provided to CBP, will be leveraged to provide expanded predictive capabilities related to illegal immigration and narcotics smuggling, tunneling, or other activities on the other side of the southern and northern borders that would be of interest to CBP.

6.3.3.4 Wireless Communications

The Contractor shall ensure BP Agents have reliable voice communications at all times, in all locations. Provisions shall be provided to physically locate a BP Agent by means of his vehicle anywhere within the sector. In addition to the coverage footprint, voice communications shall have available channels/bandwidth at all times. BP Agents and CBP Officers shall be provided with reliable, interoperable voice communications with each other, with local law enforcement, and with BP agents in other sectors and CBP officers. To accomplish this, the Contractor shall design and deploy communications infrastructure that will:

- Increase coverage, reliability, and interoperability of voice communications.
- Simplify and consolidate agent communication devices.
- Support multiple data/media types.
- Integrate with IWN in the future.

Definition of specific items proposed under Wireless Communications is included in the SBInet Equipment and Services Bill-of-Materials (BOM).

- Fixed Terrestrial (1.2.6.1).
- Mobile and Wireless (1.2.6.2).
- Satellite (1.2.6.3).

6.3.3.5 Information Technology (IT) Infrastructure

- Information Infrastructure includes hardware (i.e., servers, routers, gateways, storage devices, switches, commercially leased communication lines) and system software (i.e., database management, operating system, and network management) that provide an environment for operating and maintaining software applications. The Contractor's Information Infrastructure shall comply with the goals of the DHS enterprise architecture and align with the continuing IT initiatives of CBP and DHS (i.e. U.S.- VISIT, ENFORCE/IDENT, IWN and EAGLE). The elements of Information Infrastructure are standards-based,

open-architecture, COTS products that provide the backbone for information dissemination and collaboration. Definition of specific items (delineated below) proposed as IT Infrastructure is included in the SBInet Equipment and Services Bill-of-Materials (BOM). The Contractor shall design, develop, implement, operate and monitor, and provide user support for all IT components.

- C2 Hardware (Servers, Workstations, Displays) (1.2.3.1).
- Hardware (1.2.5.1).
- Software (1.2.5.2).

Databases (1.2.5.3).

6.3.4 Mobile Response Platforms

The Contractor-proposed Mobile Response platforms include sensor and communications upgrades for manned aircraft (included under Surveillance and Detection 6.3.2 and Wireless Communications 6.3.3.2, respectively), Unmanned Surveillance Aircraft, Manned Aircraft, Water Vehicles, and Rapid Response Transport Vehicles. Definition of specific items (delineated below) proposed as Mobile Response Platforms is included in the SBInet Equipment and Services Bill-of-Materials (BOM).

- Manned Aircraft.
- Unmanned Aircraft (1.2.8.1).
- Water Vehicles (1.2.8.2).
- Response Ground Vehicles. Land Vehicles (1.2.8.3). Detainee transportation (1.2.7.5).

6.4 Facilities and Infrastructure Task Area

The Contractor shall determine requirements for, plan for, architect and engineer, design, construct, test, and maintain such facilities and infrastructure required for control of the borders. Such infrastructure shall include tactical infrastructure (fences, roads, lighting, and barriers), power and data infrastructure, and equipment supporting Checkpoints, POEs, Sector HQ, and Border Patrol Stations. The Contractor shall plan and execute land-use regulatory activities associated with deployed systems and facilities.

6.4.1 Tactical Infrastructure

Tactical Infrastructure includes passive vehicle barriers, support structures, power and data infrastructure, roads, lighting, and the installation of roads and fences. Definition of specific items (delineated below) proposed as Tactical Infrastructure is included in the SBInet Equipment and Services Bill-of-Materials (BOM).

- Fixed Passive Barriers (1.2.7.1.1.1).
- Fixed Support Structures (1.2.7.2.1).
- Power Infrastructure (1.2.7.3.1).
- Data Infrastructure (1.2.7.3.2).
- Roads (1.2.7.3.3).
- Lighting (1.2.7.3.4).
- Installation (Roads and Fences) (1.2.9.1).

6.4.2 Facilities

6.4.2.1 SBInet Facilities

Facilities include equipment designated to support Checkpoints, Forward Operating Base locations, POEs, Border Patrol Stations, and Headquarters facilities. Also included in this SOW paragraph is the planning and execution of land-use regulatory activities. Definition of specific items (delineated below) proposed as facilities-related equipment is included in the SBInet Equipment and Services Bill-of-Materials (BOM).

- Checkpoints (1.2.7.4.1).
- Detention (1.2.7.4.2).
- POEs (1.2.7.4.3).

- Sector HQ (1.2.7.4.4).
- Border Patrol Station (1.2.7.4.5).
- Forward Operating Bases.

6.4.2.1.1 Land-Use Regulatory Activities (1.1.6, 1.2.1.9)

The Contractor shall coordinate with local, state, and federal agencies to obtain land use permits,

certificates, and clearances including:

- Land Acquisition and Use.
- State and Local Historic Preservation Issues.
- US Fish and Wildlife Service.

The Contractor will plan and manage public outreach meetings and hearings as dictated by statutory and regulatory requirements. The Contractor will also provide a liaison function between program management, systems engineering, construction, and external agencies relative to land use regulatory matters for all authorized Task Orders.

For each Task Order, the Contractor shall (1) obtain land use permits, certificates, and clearances with local, state, and federal agencies; and (2) execute public outreach meetings and hearings as dictated by statutory and regulatory requirements. Potential cooperating agencies (federal) may include the Bureau of Indian Affairs (BIA), Forest Service (FS), Bureau of Land Management (BLM), National Parks Service (NPS), Bureau of Reclamation (BOR), and the Army Corps of Engineers (COE).

6.4.3 Environmental (1.1.6, 1.2.1.9)

The Contractor shall plan and execute the necessary environmental regulatory activities associated with deployed systems and facilities.

The Contractor shall (1) coordinate with local, state, and federal agencies to obtain National Environmental Policy Act permits, certificates, and clearances; (2) plan and manage public outreach meetings and hearings as dictated by statutory and regulatory requirements; and (3) provide a liaison function between program management, systems engineering, construction, and external agencies relative to environmental regulatory matters for all authorized Task Orders.

For each Task Order, the Contractor shall (1) execute the effort to obtain National Environmental Policy Act permits, certificates, and clearances with local, state, and federal agencies; and (2) execute public outreach meetings and hearings as dictated by statutory and regulatory requirements.

6.5 Systems Engineering Task Area

The systems engineering functions shall include the following: (1) architectural definition, (2) life cycle cost and affordability, (3) configuration and data management, (4) requirements management, (5) product design, (6) risk management, (7) quality and mission assurance, (8) specialty engineering, and (9) product/process improvement. The Contractor shall (1) perform and document architecture design and synthesis, including integration with the CBP and DHS Enterprise Architecture; (2) perform and document all necessary design reviews and all required analysis of technical solution alternatives; and (3) develop, collect, publish, and analyze Technical Performance Measures (TPM) during the course of development, production, deployment, and operation.

6.5.1 Engineering Management (1.2.2.1)

The Systems Engineering Management tasks for each task order include the following:

- Management of the resources assigned to the SBI program to implement the Task Order including: Cost Account Management (budget definition, tracking, and reporting), Work Break-down Structure (WBS) definition, Schedule performance (identification of the tasks being performed by each of the functions, scheduling those tasks and monitoring performance to schedule). Requirements Adherence: Ensuring that all functions being performed and products being delivered are in accordance with the contractual requirements and meet the intent of the Statement of Work.

- Customer Relationship Management. Receive feedback from and respond to Award Fee feedback from the customer. Providing additional customer support as requested/required. Response to

- customer-generated corrective actions.
  Providing inputs and support to all program reviews.

Design reviews. Management reviews. Customer reviews.

6.5.2 Architecture (1.2.2.3)

This task is to develop the architecture that will be robust enough to handle changing conditions such as (1) shifting illegal entry patterns, (2) equipment developments, (3) equipment failures, and (4) weather and federal budget changes. The purpose of this system is to assist the Border Patrol Agents in more effectively performing their job.

6.5.3 Life-Cycle Cost/Affordability (1.1.9.1.1)

The Contractor shall implement the Affordability/CAIV process as a part of the SBInet program. The Contractor shall prepare Affordability trade study reports and LCC reports and analysis, support competitive assessment, prepare proposals, and develop models. The Contractor shall provide a traceable, credible, and defendable LCC estimate.

6.5.4 Configuration and Data Management (1.1.9.1.2, 1.2.1.3)

Configuration/Change Management. Develop a Configuration Management Plan, maintain documentation under configuration control, identify configuration items, establish the configuration baseline, provide delivery support, provide administrative support to FAT/SAT, provide change management for class I and II changes, and provide technical compliance support.

Data Management/Engineering Release. Implement Data Management processes, act as single-point Data Management Focal with Customer, prepare and maintain schedule reports, perform document control, prepare data transmittal forms, monitor contract data deliveries, perform engineering release functions, and perform contract closeout and certification.

Software Configuration Management. Develop a Software Configuration Management Plan (SCMP), implement the software change request (SCR) tracking system to be available for tracking problems and other changes in the software products and processes, identify software products to be controlled and the level of control for these products, control the identified software products according to the SCMP, maintain the software development library (SDL), support FAT and SAT, CSCI qualification, coordinate production and shipment of software and documentation, and attend meetings.

6.5.5 Requirements Management (1.1.9.1.3)

This task includes development of a top specification and lower tier specification requirements and verification statements. The specifications and the Verification Logic Network (VLN) shall be maintained in a DOORS requirements database. This database will indicate requirements allocations and traceability to/between different task orders and product end items. The VLN traces the verification requirements to the verification activities down to the verification completion notices that "close out" the verification.

6.5.6 Requirements, Interfaces, and Verification (1.2.2.2)

This task tailors the requirements for the solution, to define Task Order particular interface requirements and prepare and complete verification of requirements. Integration and Verification planning, documented in verification plans and activities as well as verification completion notices, will be recorded in DOORS.

6.5.7 Product Design (1.2.2.5)

This task includes the Task Order layout to the block level arrangement of components, integration of the results of the requirements analysis, trade studies, and customer meetings to develop a top-level design that best satisfies all system-of-systems needs. This includes quarterly reviews and briefings through Technical Interchange Meetings (TIM) and partner meetings to address design oversight. This also allows for interactive feedback.

6.5.8 Software Management (1.1.9.1.4, 1.2.2.8)

Software Management shall establish policy and guidelines to ensure software is developed in accordance with CMMI Level 3 or higher. Software Management shall monitor the development and testing of software in accordance with metrics established in the QASP.

Software Management shall define a plan for software validation, certification, and accreditation. This plan will satisfy the CBP requirement to obtain approval of all software deployed in the SBInet infrastructure and DHS Certification and Accreditation (C&A) process as described in National Institute of Standards and Technology (NIST) Special Publication 800-37. Software interfacing shall merge additional disparate items between CBP and the Contractor.

The Software Management effort for each Task Order will be defined and estimated separately under this SOW. The effort under this SOW includes the validation, certification, and accreditation of software developed under the Task Order scope of work.

6.5.9 Risk Management (1.1.4, 1.2.1.7)

The Contractor shall act as Risk Manager (RM) for the SBInet Program Management Task Order and conduct all Risk Management Team (RMT) meetings. The Contractor shall support the SBInet program manager and the Risk Management Board (RMB) by reporting and creating visibility of risk at program reviews and control boards, and in disseminating risk across the program to incorporate into program activity. The Contractor shall coordinate and lead all risk activity for the Program Management Task Order, which includes the following:

- Implement the Contractor risk management process across the program: be the program focal point for identification, analysis, handling, tracking, and communicating of risk.
- Lead all program risk mitigation activities: ensure that risk mitigation activities are incorporated into program budget and IMS.
- Be the focal point for use of the Risk Management tool.
- Develop and report risk metrics to assist the program in assessing the effectiveness of the risk management process on the program and assess risk resolution on the program.
- Perform Issues and Opportunities Management process using the Risk Management Tool to support program management in executing the program.

The Contractor shall develop and maintain Risk Tracking Documents. These documents consist of a Risk List, a Risk Mitigation Summary, and a Risk Burndown Summary, with monthly delivery of these Risk Tracking Documents to CBP.

Specific Quality and Mission Assurance tasks, activities, and deliverables include the following:

- Quality Engineer (QE). Draft QA Plan/Policy. Participate in developing and reviewing procedures for handling, inspection, and disposition of Customer-Furnished Equipment (CFE). Support development and procurement activities. Review supplier system and process control/support IPT infrastructure.
- Software Assurance Engineer (SWA). Evaluate customer requirements. Perform RFP evaluation. Participate in source selection activities. Assess Capability Maturity Model/Capability Maturity Model. Support CMMI Level 3 certification process.
- Product Quality Assurance Representative (QA). Pre-contract customer proposal support. Review requirements and determine manufacturing/inspection capability. Review manufacturing plan, develop QA, integrate and test plan, support test data analysis, and obtain customer input.
- Procurement Quality Assurance Representatives (PQA).

Provide quality requirements for Purchase Contracts. Receive and Disposition (accept or reject) of product or services. Conduct quality assurance product acceptance activities at supplier's facilities.

- Quality System Integrity Representative (QSI). Internal Quality Audit. Process Records. Task Nonconformance data collection and metrics.
- Safety, Health and Environmental Affairs Representative (SHEA).Safety, Health and Environmental Affairs Representative Oversight activities.

The following are the tasks that Quality and Mission Assurance shall provide to support each Task Order:

- Provide support for: Hardware maintenance. Spares inventory. Configuration and data management. Requirements interfaces and verifications.
- Provide support for Integration Acceptance Testing of the following: Mobile Sensor towers. Upgrades for existing towers. Unattended ground sensors. Upgrade UAV. Agent vehicles. Existing agent vehicles. DRO and mobile command Upgrades for Station. Upgrades for Sector.
- Provide SHEA assistance/guidance to NEPA requirements.
- Provide support for maintenance of system security certification and accreditation.

6.5.10 Specialty Engineering (1.2.2.6)

Specialty engineering is all the engineering disciplines that require specialized knowledge or insight in determining the solution to complex problems. This includes areas such as Reliability, Availability, Maintainability and Test (RAM&T), Environmental, Parts Materials and Processes (PM&P), Frequency Management, and System Security. These specialties are matrixed across the elements of the design, Systems engineering, sensors communications, architecture, and modeling and simulations.

6.5.11 Product/Process Improvement (1.1.9.1.5)

This task provides quality training, monitors metrics to ensure quality of engineering products, ensures the Contractor best practices are executed across the company and with subcontractor teams, and develops and archives lessons learned.

6.6 Test and Evaluation Task Area (1.1.9.3)

The Contractor shall conduct an independent test and evaluation program through the use of prototype, production, or specifically fabricated hardware/software to obtain or validate engineering data on the performance of the SBInet solution. Test and evaluation activities shall include conducting detailed planning, testing, support, data reduction and report preparation. The Contractor shall design and produce all models, specimens, fixtures, and instrumentation required to support the system-level test program. The Contractor shall support an independent operational test and evaluation program conducted by the government to assess SBInet's operational effectiveness and suitability, security, and logistics (i.e. compatibility, interoperability, reliability, maintainability, logistic requirements.), cost of ownership, and modification requirements. The Contractor will prepare test and evaluation result reports.

6.6.1 ITV Planning (1.1.9.3.1)

The Contractor shall develop the overall concept for Integration, Test, and Verification. The Contractor shall develop Master Integrated Test Plans and Test Procedures. These plans shall provide the basic ground rules and protocols for the recurring Test and Verification activities to be performed under the separately funded task orders.

6.6.2 Integration Lab (1.1.9.3.2)

Two primary Integration Labs are planned for SBInet. One is a software integration facility located in Huntsville and the second is the Joint Contractor/CBP Integration Center located in El Paso, Texas. An additional Contractor integration and test facility is located at the Kollsman facility in Merrimack, NH, which will be used for testing of SBInet systems in representative northern border environments. A sustaining level of effort shall maintain the lab infrastructure for the integration and software development activities.

6.6.3 Test and Evaluation (1.2.2.7)

The Contractor shall develop and perform the system test strategy. Full interoperability testing verifies the ability of the system to operate cooperatively with selected systems from the internal interfaces to

national SBInet systems. This testing is designed to verify interfaces and information exchanges within the SBInet systems. As the specific test objectives are defined, entrance and exit criteria are developed to demonstrate platform/system readiness.

6.6.4 Integration (1.2.2.9)

The Contractor shall execute the following for the Task Order:

- Integration of HW-SW Mobile Elements: Integrate mobile component hardware and software to assure functionality and performance.
- Integration of HW-SW Fixed Elements: Integrate fixed sensing and communication relay component hardware and software to assure functionality and performance.
- Integration of HW-SW Balance of Implementation: Integrate Sector and station component hardware to software to assure functionality and performance.

6.6.5 System Acceptance Testing (SAT) (1.2.9.2)

System Acceptance Testing shall be performed to ensure deployed SBInet systems are thoroughly validated prior to proceeding with full-scale implementation. System Acceptance testing shall establish that the system performs as expected in an environment that represents the intended deployment environment. Supporting documentation and reference materials shall be updated, in support of System Acceptance Testing, to ensure consistency with the final delivered system.

6.7 Training Task Area (1.3.1)

CBP and support personnel training shall ensure efficient and effective use of staff and technology. The Contractor shall provide a modular train-the-trainer solution for operations. Operation training shall take place in the field and include system functionality as well as exercises unique to each sector. The Contractor approach includes a combination of instructor-led training, train-the-trainer, in-field training and exercises, Computer-Based Training (CBT), and hands-on learning. The proposed Integration Center housing the modeling and simulation and technology insertion activities also will play a role in the integrated training approach.

6.8 Integrated Logistics Support Task Area

Integrated Logistics Support includes all activities and processes necessary to support and maintain the SBInet Border control solution through the end of the solution's service life. Integrated Logistics services include (1) maintenance management and system support analysis,
(2) call center operations, (3) asset management, (4) critical property and spare parts storage, (5) management and inventory records, (6) field services, (7) maintenance and overhaul, and (8) training. The Contractor shall submit an Integrated Logistics Support plan 45 days after ATP to define the logistics and maintenance infrastructure necessary to keep the capability reliably deployed in the field.

6.8.1 Asset Management (1.2.1.4)

For each authorized Task Order, the Contractor shall execute the asset management functions required for government asset identification, control and traceability, formal accountability records, and disposition of CBP assets. In addition, asset management shall perform all financial reporting documents and perform risk/liability management on behalf of the Contractor for CBP assets in custodial care.

6.8.2 Hardware Maintenance (1.3.2)

The Operation support team shall develop and implement LCCM team execution planning and support Field Service operations.

6.8.3 Software Maintenance (1.3.4)

The software maintenance process begins after formal delivery. Maintenance activities include

identifying and analyzing problems including administering a Problem Report and/or Change Request system as well as the actual changes to the software itself. The software maintenance process does not include planned functional block upgrades.

6.8.4 Spares and Inventory (1.3.3)

The Contractor Inventory Asset Management Team is comprised of product support inventory managers and Government property specialists. The combination of these two skill-sets provides inventory/spares analysis and control and SBInet supply-chain accountability.

6.9 Deployment and Installation Task Area (1.2.9.1)

The Contractor shall provide the materials and services for installation of prime mission and support equipment (including facilities) for the complete SBInet solution. This includes deployment, on-site integration, and checkout or shakedown to ensure operational status. The Contractor shall prepare necessary deployment and installation engineering plans, checkout procedures, and schedules. The Contractor shall perform required site preparation, deployment package integration, and installation.

6.10 Operations Support Task Area

The Contractor shall provide the operational support required for the SBInet solution, exclusive of integrated logistics support. This support will include operating the Network Operations Center and Security Operations Center, manning the Customer Support (Help Desk), and IT Systems Support as required by CBP.

6.10.1 Operations Support (1.3.6)

The Contractor shall provide a Network Operations Center (NOC) and Security Operations Center (SOC) as a subelement of the existing CBP Network. The NOC will provide standard network management services for the infrastructure as described in the ISO FCAPS framework. The SOC will provide security services required to ensure monitoring and security compliance with CBP security policies, including managing firewalls and intrusion-detection systems. Both the SBInet NOC and SOC will operate within the CBP network domain as either an integrated segment of the overall network or as a separately managed subnetwork within the CBP domain. Both will be collocated with CBP network and security management activities.

6.10.2 Customer Support (Help Desk) (1.3.5)

A Customer Support Help Desk shall be established and staffed to resolve user issues and to ensure availability and responsiveness of all information technology applications and IT infrastructure components.

6.10.3 Information Technology (IT) Systems Support (1.3.7)

IT Systems support shall manage firewalls and intrusion-detection systems. IT Systems Support will provide installation and maintenance for fielded systems and will create, maintain, and remove user

accounts, user login controls, and perform password maintenance.

6.11 Program Management Task Area

The Contractor Program Management plans, organizes, coordinates, authorizes, and controls the overall program to meet technical, quality, cost, and schedule requirements. Program Management services are applied over the entire SBInet program life and include all activities and processes from contract award through the period of performance.

6.11.1 Program Management Office (1.1.1)

6.11.1.1 Program Manager/Deputy/Chief Engineer (1.1.1.1)

The Contractor shall designate a Program Manager (PM), Deputy Program Manager (DPM), and Chief

Engineer (CE) to provide the SBInet Program and Technical governance and be the key points of contact for all programmatic and technical matters. The PM and DPM shall have the responsibility and authority to represent and commit the Contractor on programmatic matters. The PM and DPM are responsible for creating a partnering environment with CBP and ensuring that the Integrated Product Teams work in a collaborative manner. The DPM is also responsible for implementing the Program Management Best Practices model and associated measurement and program visibility tools. The PM and DPM are supported by a small team of Program Specialists to ensure that Program Management Best Practices and nonoperational metrics are captured and to support communications and the welfare of the team. Additional support is provided to ensure that there is full visibility to CBP.

6.11.1.2 Program Coordination and Administrative Support (1.1.1.2)

Program Coordination is responsible for tracking issues and action items and developing reports to support weekly and monthly program reviews and to rapidly respond to ad-hoc requests for program-related information. Other responsibilities include coordinating and de-conflicting program reviews, independent and nonadvocate reviews, and internal and external compliance audits. Administration functions are responsible for the overall support of the Program Management effort through the provision of the office administration.

6.11.2 Project (Task Order) Office

6.11.2.1 Project Manager (1.2.1.1)

The Task Order Management tasks include:

- Manage the resources assigned to the SBI program to implement the Task Order Tasks: Cost Account Management (budget definition, tracking, and reporting), Work Breakdown Structure (WBS) definition, Schedule performance (identification of the tasks being performed by each of the functions, scheduling those tasks, and monitoring performance to schedule. Requirements adherence: Ensuring that all functions being performed and products being delivered are in accordance with the contractual requirements and meet the intent of the Statement of Work.
- Customer Relationship Management. Receive feedback from and respond to Award Fee feedback from the customer. Provide additional customer support as requested/required. Respond to customer generated corrective actions.
- Provide inputs and support to all program reviews. Design reviews. Management reviews. Customer reviews.

6.11.2.2 Project Coordination and Administrative Support (1.2.1.2)

The Task Order Management tasks for Project Coordination and Admin Support include:

- Support operations in areas such as metrics collection.
- Coordinate meetings and reviews including distribution of meeting minutes and agendas.

6.11.3 Business Management (1.1.2)

6.11.3.1 Cost and Schedule Management (EVMS) (1.1.2.1, 1.2.1.5.1)

Cost and Schedule Management is responsible for preparing, implementing, and maintaining the performance management baseline (PMB) as well as preparing and maintaining the following documents, to be used during the performance of the program: Integrated Performance Management Plan (IPMP), Work Breakdown Structure (WBS), Work Authorizations (WA), Integrated Master Schedule (IMS), weekly and monthly Equivalent Persons (EP) reports, weekly and monthly Earned Value (EVMS) reports, weekly and monthly IMS updates, and various analytical products and Business Reports and Briefing Packages, which shall include a weekly and monthly Program Management Review package, monthly Cost Performance Report (CPR), quarterly Contract Funds Status Report (CFSR), and quarterly

Estimates at Completion. In addition, cost and schedule performance data across the program will be integrated into a single database for an integrated set of cost and schedule performance metrics and schedule status reports available electronically.

6.11.3.2 Contracts Management (1.1.2.2, 1.2.1.5.2)

The Contractor shall designate a contracts administrator as the single point of contact for contractual matters. The Contract Administrator shall be responsible for and have authority to represent and commit the Contractor on contract-related program issues. The Contractor shall distribute work packages across the company's business units in accordance with the program plan. The Contractor shall perform Interorganizational Work Authorization Administration as the means to document and communicate the work breakdown. This task encompasses the contracts administration effort associated with the model contract. Contracts administrator manager shall perform general contract administration support during the period of performance of the program. The administrator shall serve as the customer focal point for contractual matters, and shall support program reviews. The administrator shall issue and track correspondences items (incoming and outgoing), and maintain a change history log. The administrator shall also maintain a GFE/GFP log tracking receipt and registration. The administrator shall perform obligation analysis to assess the impact of change activity with regard to scope, change board activities, funding requirements, and export compliance activities. The administrator shall coordinate property administration on the status and maintenance of GFP, support budgetary and planning exercises, and monitor incoming Interorganizational Work Authorizations as needed.

6.11.3.3 Task Order Preparation (1.1.2.3)

Business Management shall (1) cooperatively develop the detailed Task Orders for SBINet by evaluating options using existing cost and schedule data to model alternate choices to achieve customer objectives within funding and schedule constraints, (2) develop a detailed IMS and preliminary resource loads, (3) update the IMS and resource loads through a proposal preparation process, (4) support the implementation team in finalizing the PMB, and (5) participate in Integrated Baseline Reviews (IBRs) for each new Task Order. This WBS element shall cover the Task Order preparation activities of the Business Management function. Other functions will participate in Task Order preparation as noted in their individual write-ups.

6.11.4 Supplier Management and Procurement (1.1.3, 1.2.1.6)

In support of the Program Management Office, SM&P shall be responsible for the following:

- Establish, implement, and maintain a Subcontract Management/Procurement Plan.
- The Subcontract Management Plan for this task shall embody all of the elements of sourcing and subcontracting for the SBInet program. The Plan shall be developed in conjunction with Supplier/Program Management Best Practices.
- Create/maintain major subcontract umbrella task order contracts and flow down coordination and communication to the SM&P task order team.
- EBOM to MBOM configuration and macro requirements flowdown (make/buy) to SM&P task order team.
- Procurement Contracts shall be issued in accordance with the Contractor's approved procurement systems.
- CBP and supplier team interface/coordination for subcontract team decisions.
- Assess new supplier technologies and capabilities and implement/maintain new PIAs, MOUs, MOAs, and TAs.
- Create and establish competitive source selection evaluation criteria and team requirements, including subcontract award fee criteria.
- Participate in program reviews with respect to subcontractor performance, supporting EAC, IMS analysis and schedule management activities, evaluating data items, evaluating and maintaining effective supplier performance metrics, and assessing subcontractor risk, issues, and opportunities.
- Ensuring that subcontractor work scope requirements (i.e., PWSs, specifications, drawings, etc, items/dates) are developed, maintained, and released to the SM&P task order organization for contractual implementation
- Work closely with suppliers and supply chain members to develop a fully integrated supply-chain visibility system for components, subassemblies, material, and supplies in order to monitor points of

delivery and delivery times to support schedule.

- Travel to sectors and SM&P task order office to assess needs and staffing requirements.
- Mentor Protégé Development.
- Oversight for SM&P task order team and on-site sector support which includes

procurement readiness as follows: Major Subcontract: Proposal evaluation, negotiation, procurement contracts ready for placement. COTS: Leverage the Contractor enterprise commodity teams for COTS procurement order placement. Services Contracts: Model purchase contracts developed. Small Business: Small Businesses identified and provided with model contact. eBuy/Exostar: Identify products and services for reverse auctions and quick response e-commerce. Purchasing Cards: Available for emergency and low value procurements.

For each Task Order, the Contractor Supplier Management and Procurement function shall direct all SM&P task order activity, and serve as the primary SM&P liaison for sector support, customer integration, and supplier Interface. The Contractor Supplier Management shall oversee task order staffing and budgetary and schedule requirements, (2) conduct periodic strategy discussions with the Washington, D.C., Program Management Team, (3) ensure requirements flowdown including providing the necessary management, and (4) act as technical liaison and customer and administrative support.

[redacted] (1.1.8, 1.2.1.11)

a. Provide the program infrastructure for information security, including certifying and accrediting SBInet information systems and infrastructure. The information security system design shall meet the SBI's Cyber Security Standards and related federal security policies. It shall incorporate industry best practices that improve incident identification and mitigation and increase probability of protection in the future. The Contractor SBInet security solution shall:

- Comply fully with industry standards to implement data authentication, verification, encryption, and information exchange.
- Incorporate security services in a consistent manner such that the SBI's information is protected and accessible.
- Provide unimpeded and readily available business services.
- Include controls and processes to support the security architecture, so that in the event of an attack by an unauthorized entry, the response will be quick and efficient.
- Depict clearly in the security architecture the interconnection and dependencies associated with physical and environment threats.
- Emphasize, as a priority, that responses to security incidents that do occur be quick and effective and that controls will be tightened iteratively to deter future occurrences.

To ensure SBInet system security is fully compliant with all applicable Government security standards, one full-time Information Systems Security Officer (ISSO) is planned. The ISSO is a

security expert and has full responsibility for information program security including but not limited to:

- Developing and maintaining all required security plans.
- Capital planning for security.
- Contingency and disaster recovery planning .
- Coordinating with CBP/DHS to ensure compliance of SBInet systems and information processing facilities.

In accordance with the planning and infrastructure established and managed under the Program Security Task, ensure SBInet system security is compliant with applicable Government security standards as

applicable to the specific Task Order implementations.

(b) This requirement applies to the extent that it involves access to information classified "Confidential," "Secret," or "Top Secret."

The Contractor shall comply with -

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

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

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

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

(c) With some facilities there will be the need for TS/SCI access and storage, Communications Security (COMSEC) information will be utilized, and require that the contractor have and maintain a COMSEC account for proper maintenance of communications security. Boeing shall ensure the proper types of access be imposed on the subcontractor for COMSEC information. Prior approval is required before a prime contractor (Boeing) grants COMSEC access to a subcontractor. The following Boeing facilities sites will handle classified information:

FACILITY & ADDRESS	CAGE CODE	SAFEGUARDING LEVEL	ACCESS LEVEL
1. The Boeing Company (b) (6)	3A768	(b) (7)(F)	COMSEC
2. McDonnell Douglas Corp. The Boeing Company (b) (6)	18355	(b) (7)(F)	COMSEC
3. The Boeing Company (b) (6)	1J649	(b) (7)(F)	CNWDI
4. The Boeing Company (b) (6)	54669	(b) (7)(F)	COMSEC
5. The Boeing Company (b) (6)	2D627	(b) (7)(F)	COMSEC

6. Autometric Inc. (b) (6)	2R708	(b) (7)(F)	COMSEC
7. The Boeing Company (b) (6)	33472	(b) (7)(F)	COMSEC
8. McDonnell Douglas Helic Com The Boeing Company (b) (6)	8V613	(b) (7)(F)	COMSEC
9. The Boeing Company (b) (6)	2D627	(b) (7)(F)	COMSEC
10. Boeing Service Com. (b) (6)	3L1K7	(b) (7)(F)	COMSEC
11. The Boeing Company (b) (6)	0Bct4	(b) (7)(F)	COMSEC

7 Assumptions and Constraints

The following are assumptions and constraints imposed on the Contractor and any solution for border security.

7.1 Assumptions

The assumptions are grouped by (1) Business; (2) Program, based on conditions within the DHS, CBP, and SBInet environments; and (3) Technical, based on CBP's current technical environment and expected target-state outcomes.

A. Business

1 The SBInet program will serve stakeholders both within and outside DHS such as: federal, state, local, and tribal governments; international partners; industry, and the general public.

2 DHS and CBP business processes and requirements will continue to evolve throughout the life of the SBInet program to reflect new laws, regulations, policies, and threats.

3 The Department of Homeland Security has determined that the product(s) and service(s) to be acquired from the successful offeror pursuant to this solicitation will be good candidates for designation as a Qualified Anti-Terrorism Technology (QATT) as that term is defined by the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, sections 441-444 of title 6, United States Code (the "SAFETY Act") and the SAFETY Act implementing regulations (6 CFR Part 25). While it is not possible to definitively state that the product(s) and

service(s) will be designated as QATTs under the SAFETY Act, the consideration of any application for such designation will be expedited if the successful Offeror seeks SAFETY Act liability protections. Moreover, the SAFETY Act application process for the successful Offeror will be streamlined.

SAFETY Act protections are not a requirement of this procurement. Firms are free to submit applications with the Department's Office of SAFETY Act Implementation at any time for any anti-terrorism technology. Whether an Offeror has previously obtained SAFETY Act protections will not be evaluated as part of this procurement. Offerors are not required to seek SAFETY Act protections in order to submit an offer or to receive an award. Whether to seek the liability protections of the SAFETY Act for a proposed product or service is entirely up to the Offeror. Additional information about the SAFETY Act may be found at the SAFETY Act website at http: //www.SAFETYAct.gov. Proposals in which pricing or any other term or condition is contingent upon SAFETY Act protections of the proposed product(s) or service(s) will not be considered for award. The SBInet Program Office will work with the DHS Office of SAFETY Act Implementation (OSAI) to facilitate and expedite the evaluation and analysis that would be required prior to any final decision on SAFETY Designation or Certification. Offerors may begin the SAFETY Act application process prior to submitting a

proposal in response to the SBInet Solicitation. In fact, OSAI has a pre-application process through which OSAI provides applicants preliminary guidance regarding a technology's prospects for SAFETY Act Designation. Interested parties should contact OSAI at 1-866-788-9318. It is our intent to cooperate with the OSAI in order to minimize the time required to reach a final decision on Designation or Certification. However, no final decision may be reached in the absence of information about the effectiveness of the particular technology that the offeror intends to provide.

1 Unique requirements and conditions (e.g., bonds for construction, labor regulations, etc.) will be specified in applicable task order(s).
2 Additional Business Assumptions were provided in the Contractor response to the SBInet RFP Amendment 7submittal on 4 August 2006.

B. Program

1 The contract resulting from this solicitation will be for use by all components of DHS.
2 CBP, its selected integration partner, and other DHS and CBP Contractors and service providers, must effectively function and coordinate to achieve SBInet's objectives.
3 The funding/appropriations process may constrain the ordering and implementation needed to put solutions in place.
4 The Contractor is responsible for its own security, equipment, and manpower (storage, moving own equipment).

Additional Program Assumptions were provided in the Contractor response to the SBInet RFP Amendment 7 submittal on 4 August 2006.

C. Technical

1 SBInet integration Contractor must interface both directly and indirectly, with DHS and its components throughout the term of the contract, including periods covered by the exercise of any task order renewal options. Some development, modification, or enhancement to legacy systems, infrastructure, and processes by current CBP employees and Contractors may be required to ensure integration and interoperability of SBInet solutions within the DHS and CBP environment.
2 The SBInet program solution(s) shall be implemented in a manner that balances interruption of operations with mission improvement for CBP, DHS, and external stakeholders.
3 SBInet solution(s) will utilize products, standards, and services that promote an open and flexible architecture. The Contractor will use Commercial Off-The-Shelf (COTS) and Government Off-The-Shelf (GOTS) products whenever possible. The Contractor will use approved DHS and CBP products, standards, and services

when appropriate, but can propose additional elements, as needed, in support of innovative, interoperable, and best-value solutions. The Contractor is expected to plan for the use of DHS planned and existing contracts including, but not limited to: Integrated Wireless Network (IWN) (wireless technology), EAGLE and First Source (information technology products and services), OneNet, and SAFECOM.

4 The SBInet solution(s) must maximize officer and other personnel safety and the welfare of the communities.

5 The deployment and/or capability of IWN, EAGLE, First Source, OneNet, and SAFECOM may not be synchronized or sufficient to support SBInet.

7.2 Constraints

In addition to contractual provisions specified herein and the Laws, Regulations, and Policies specified in Section J, Attachment 02, the following constraints are applicable to all solutions provided under this contract. The Contractor, subcontractors, and teaming partners will adhere to all applicable federal laws, regulations, and policies, including but not limited to the following:

A. Development

1 ISO 9001 Standards certifications or Software Engineering Institute (SEI) Capability Maturity Model (CMM) Level 3 or CMM Integration (CMMI) Level 3 appraisals for the Contractor Team Member doing applicable software development work.

2 The Contractor shall follow DHS and CBP configuration, change, and baseline management practices, and operate within established DHS and CBP configuration management governance structures and guidelines.

3 Where possible, the Contractor will utilize approved DHS and CBP services, products, and standards, as reflected in the DHS and CBP Technical Reference Models (TRM) and Standards Profiles. If additional services, products, and standards are needed for the SBInet solution, proposals for these shall be coordinated and controlled through the appropriate DHS and CBP governance bodies, in accordance with documented Technology and Renewal Processes. Proposals to utilize new or previously unapproved products, services, and standards will be appropriately justified and explicitly linked to the tenets of innovative, flexible, reliable, interoperable, and secure best-value design.

4 The Contractor shall incorporate as much of the available technology, infrastructure, and personnel already deployed in the geographic area as practicable without unduly burdening the utility of any solution(s).

5 Federal Enterprise Architecture (FEA), including compliance with FEA Business, Performance, Data, Service Component, and Technical Reference models. Alignment with FEA is required as a component of OMB budget submissions. The FEA is available at http://www.egov.gov .

6 DHS Enterprise Architecture. Access to the DHS Enterprise Architecture will be restricted until after contract award. Alignment of the selected SBInet solution will be assessed following contract award in accordance with the DHS Capital Planning and Investment Control process.

7 CBP Enterprise Architecture. Access to the CBP Enterprise Architecture technical and application architecture has been made available during Due Diligence Review. Alignment of the selected SBInet solution will be assessed following contract award in accordance with the DHS Capital Planning and Investment Control process.

The Contractor and the Government will work together to identify where Section 508 Accessibility Requirements (www.section508.gov) are applicable.

8 CBP Systems Development Life Cycle (SDLC) and Enterprise Life Cycle Methodology (ELCM) guidelines.

9 Asset Management Policies and Procedures (refer to the SBInet library).

10 CBP will approve all software deployed to the SBInet infrastructure or supporting the DHS program using the Certification and Accreditation (C&A) process as described in National Institute of Standards and Technology (NIST) Special Publication 800-37. The Contractor must fully support the C&A process.

11 There are a number of external systems dependencies on CBP, including, but not limited to, International, federal, state, local, and tribal law enforcement system dependencies.

B. Security

1 The Contractor shall safeguard the Government's data security and the physical and data security of its operations and personnel. The Contractor shall comply with all applicable security requirements not previously

identified.
2 Contractor employees must have favorably adjudicated background investigation files prior to being given full access to CBP system and sensitive information.
3 Software solutions developed in support of SBInet will follow e-authentication guidelines issued by the National Institute of Standards and Technology (NIST).
☐ 4. The Contractor shall ensure its employees adhere to legal and contract requirements concerning U.S. citizenship or, if permitted, legal alien status. The following are the required Best Hiring Practices:
☐ a. Use the Basic Pilot Program for all hiring.
☐ b. Establish an internal training program, with annual updates, on how to manage completion of Form I-9 (Employment Eligibility Verification Form) and on how to detect the fraudulent use of documents in the I-9 process.
☐ c. Permit the I-9 and Basic Pilot Program process to be conducted only by individuals who have received this training—and include a secondary review as part of each employee's verification, to minimize the potential for a single individual to subvert the process.
☐ d. Arrange for semi-annual I-9 audits by an external auditing firm or a trained employee not otherwise involved in the I-9 process.
☐ e. Establish a self-reporting procedure for the reporting to ICE of any violations or discovered deficiencies.
☐ f. Establish a protocol for responding to no-match letters received from the Social Security Administration.
☐ g. Establish a Tip Line for employees to report activity relating to the employment of unauthorized aliens, and a protocol for responding to employee tips.
☐ h. Designate a Compliance Officer to ensure that employment practices are in accordance with these best practices (only for employers with more than 50 employees).
☐ i. Establish and maintain safeguards against use of the verification process for unlawful discrimination.
☐ j. Establish a protocol for assessing the adherence to the best practices guidelines by the company's Contractors/subcontractors.

C. Site

1. Office of Field Operations (OFO) and Office of Border Patrol (OBP) facilities, including POEs, are owned and/or managed by various federal, municipal, and private organizations, including the General Services Administration, municipal

port authorities, and CBP. The Contractor will operate within the DHS and CBP governance structures. This includes an advisory role to the SBI Program Executive Officer, the PMO, the SBInet Project Office, and interaction with the appropriate change control board(s).

1 Flyover rights and permission shall be coordinated with the appropriate FAA and local authorizing entities.
2 Local, federal, and state codes must be considered and complied with when accomplishing construction.
3 When required, certain regions and areas will require environmental impact assessment and compliance studies.
4 Policies, agreements, and the governances dealing with tribal lands and state and local governments must be adhered to.
5 To plan and execute construction of infrastructure and facilities along the specified border regions including POEs, SBInet must interface with multiple Government service providers including the U.S. Army Corps of Engineers and the General Services Administration.

Schedule of Deliverables

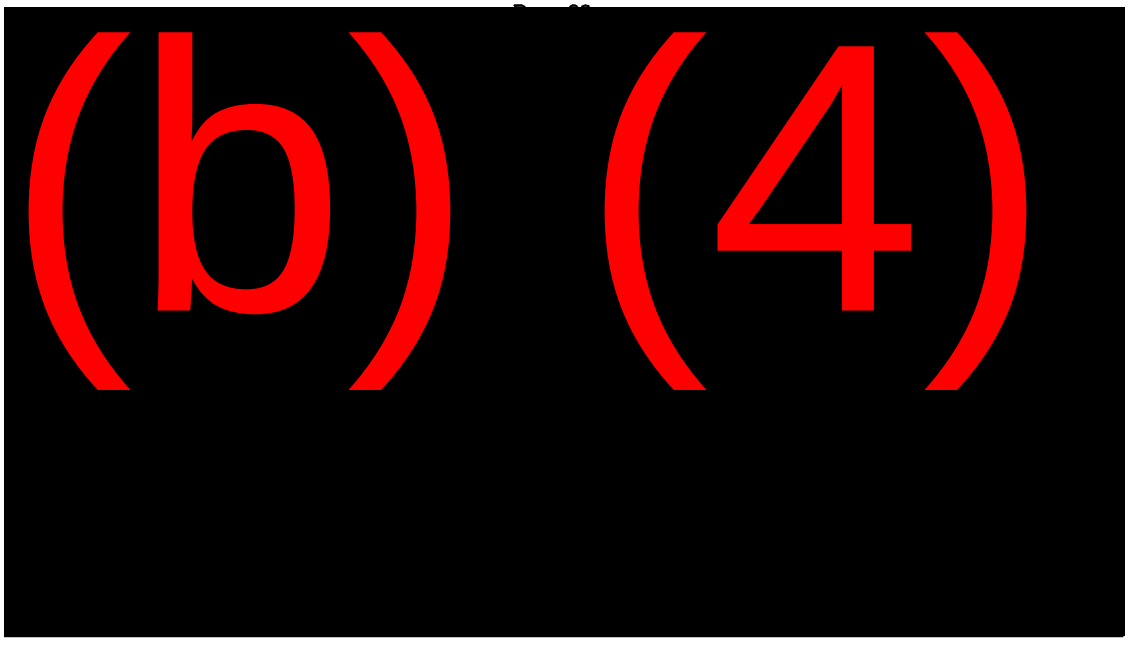
The time-phasing (Figure 1) of the Contractor SBInet solution is designed to gain full control of the border in three

years. The Program Management Task will span all phases of contract activity and will provide the necessary Program Management and System-of-Systems Engineering to support the individual IDIQ Task Orders. The execution of the Contractor-proposed solution for the Southern and Northern border sectors will be authorized, planned, and executed via discrete Task Orders per the basic IDIQ contract.

The deliverables identified in Figure 2 shall be provided in the specified formats and in accordance with the schedules specified for the individual Task Orders. As-Built documentation shall include an inventory of installed components and shall depict a complete layout (physical and functional) of the system including drawings and schematics detailing equipment enclosure layouts, tower profiles, control room layouts, conduit runs, rack drawings, equipment interfaces, and other required drawings.

Detailed operating manuals enable Government maintenance personnel to become fully conversant, knowledgeable, and able to perform all system operations. Detailed maintenance manuals enable personnel to perform routine preventive and restorative maintenance on system components.

All deliverables shall be submitted for review and acceptance by the Contracting Officer's Technical Representative (COTR). Upon completion of the review, the plans shall be updated with changes. The Final Design Plan and Final Implementation Plan shall then be submitted to the COTR for approval.



Deliverable Name	Format
Project Management Plan	MS Word
Scope Management Plan	MS Word
Scope Definition	MS Word
Work Breakdown Structure	MS Project 2000

Project Schedule	MS Project 2000
Cost Management Plan	MS Word
Cost Estimates	MS Word, MS Excel
Quality Management Plan	MS Word
Staffing Management Plan	MS Word
Communications Management Plan	MS Word
Risk Management Plan	MS Word
Procurement Management Plan	MS Word
Test and Evaluation Plan	MS Word
Acceptance Plan	MS Word
Design Plan	MS Word, AutoCAD, Printed on D-sheet size, individual PDF files for all drawings for all Layout and Model Views
Communications Design Plan	MS Word, AutoCAD, Printed on D-sheet size, individual PDF files for all drawings for all Layout and Model Views

Figure 2. SBInet Contract Data Requirements List

Deliverable Name	Format
Sensor Design Plan	MS Word, AutoCAD, Printed on D-sheet size, individual PDF files for all drawings for all Layout and Model Views
Infrastructure Design Plan	MS Word, AutoCAD, Printed on D-sheet size, individual PDF files for all drawings for all Layout and Model Views
Mobile Platform Design Plan	MS Word, AutoCAD, Printed on D-sheet size, individual PDF files for all drawings for all Layout and Model Views
Concept of Operations Design Plan	MS Word, AutoCAD, Printed on D-sheet size, individual PDF files for all drawings for all Layout and Model Views

Integration Design Plan	MS Word, AutoCAD, Printed on D-sheet size, individual PDF files for all drawings for all Layout and Model Views
Weekly, monthly, quarterly reports	MS Word
Meeting minutes	MS Word
Risk tracking documents	MS Word
Test reports	MS Word
Draft Design Plan	AutoCAD, Printed on D-sheet size, individual PDF files for all drawings for all Layout and Model Views
Bill of Materials	MS Excel, with PDF duplicate copy for record Final Design Plan AutoCAD, Printed on D-sheet size, individual PDF files for all drawings and Layout and Model Views
Final Implementation Plan	AutoCAD, Printed on D-sheet size, individual PDF files for all drawings and Layout and Model Views
Operating Manuals, warranties, test results, and registrations	Per manufacturer, PDF or Word
Invoice Submissions	MS Excel with PDF duplicate copy for record
Training Plan	MS Word
Training Materials	Per manufacturer, PDF or MS Word
As-Built Documentation	AutoCAD, Printed on D-sheet size, individual PDF files for all drawings and Layout and Model Views
Status Reports	MS Word
PDR Briefing Package	MS PowerPoint
Developmental Test and Evaluation (DT&E) Plan	MS Word
CDR Briefing Package	MS PowerPoint
DT&E Report	

Figure 2. SBInet Contract Data Requirements List (Continued)

Deliverable Name	Format
MS Word	
Operational Test and Evaluation (OT&E) Plan	MS Word
Operator Report	MS Word
OT&E Report	MS Word

Figure 2. SBInet Contract Data Requirements List (Continued)

[END OF ATTACHMENT 01] -Page 25