

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES
1 21

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

1. DATE OF ORDER 05/23/2008	2. CONTRACT NO. (If any) HSHQDC-06-D-00 024	6. SHIP TO: a. NAME OF CONSIGNEE Department of Homeland Security
--------------------------------	--	--

3. ORDER NO. HSHQDC-08-J-00 134	4. REQUISITION/REFERENCE NO. ROOP-08-00054	b. STREET ADDRESS 245 Murray Lane Bldg. 410
------------------------------------	---	---

5. ISSUING OFFICE (Address correspondence to) Department of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528		c. CITY Washington	d. STATE DC	e. ZIP CODE 20528
--	--	-----------------------	----------------	----------------------

7. TO: a. NAME OF CONTRACTOR GENERAL DYNAMICS ONE SOURCE LLC	f. SHIP VIA
--	-------------

b. COMPANY NAME	8. TYPE OF ORDER <input type="checkbox"/> a. PURCHASE <input checked="" type="checkbox"/> b. DELIVERY
-----------------	---

c. STREET ADDRESS 3211 JERMANTOWN ROAD	REFERENCE YOUR: Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.	Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.
---	---	---

d. CITY FAIRFAX	e. STATE VA	f. ZIP CODE 22030
--------------------	----------------	----------------------

9. ACCOUNTING AND APPROPRIATION DATA See Schedule	10. REQUISITIONING OFFICE Department of Homeland Security
--	--



11. BUSINESS CLASSIFICATION (Check appropriate box(es)) <input type="checkbox"/> a. SMALL <input checked="" type="checkbox"/> b. OTHER THAN SMALL <input type="checkbox"/> c. DISADVANTAGED <input type="checkbox"/> d. WOMEN-OWNED <input type="checkbox"/> e. HUBZone <input type="checkbox"/> f. EMERGING SMALL BUSINESS	12 F.O.B. POINT Destination
---	--------------------------------

13. PLACE OF a. INSPECTION Destination	b. ACCEPTANCE Destination	14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)	16. DISCOUNT TERMS
--	------------------------------	------------------------	--	--------------------

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	DUNS Number: 610320215+0000 Continued ...					

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.	17(h) TOTAL (Cont. pages)
21. MAIL INVOICE TO: a. NAME Department of Homeland Security			\$10,000,000.00
b. STREET ADDRESS (or P.O. Box) Departmental Operations Branch Room 3621 245 Murray Lane, SW Building 410			17(i) GRAND TOTAL
c. CITY Washington	d. STATE DC	e. ZIP CODE 20528	

22. UNITED STATES OF AMERICA BY (Signature)  (b(6))	23. NAME (Typed) Purnell Drew TITLE: CONTRACTING/ORDERING OFFICER
22. GENERAL DYNAMICS ONE SOURCE LLC BY (Signature)  (b(6))	23. NAME (Typed) Laura Walsh-Steinman TITLE: LEAD CONTRACTS SPECIALIST

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

PAGE OF PAGES

2 21

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

DATE OF ORDER 05/23/2008 CONTRACT NO. HSHQDC-06-D-00024

ORDER NO. HSHQDC-08-J-00134

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
0001	<p>Admin Office: Department of Homeland Security Office of Procurement Ops. (ITAC) 245 Murray Drive Bldg. 410 Washington DC 20528</p> <p>CPFF Engineering support to the HSIN Next Generation in accordance with the attached Performance Work Statement (PWS) dated April 14, 2008 and the Functional Requirements Document (FRD) dated March , 11 2008</p> <p>Estimated Cost (b(4)) Fixed Fee (b(4)) Total CPFF \$18,948,705 Total Line Item Value \$18,948,405.00 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES</p> <p>Accounting Info: (b(2)) Funded: \$9,000,000.00 Accounting Info: (b(2)) Funded: \$1,000,000.00</p>	1	LO	(b(4))	10,000,000.00	
0002	<p>Option 1 CPFF Engineering support to the HSIN Next Generation in accordance with the attached Performance Work Statement (PWS) dated April 14, 2008 and the Functional Requirements Document (FRD) dated March , 11 2008</p> <p>Estimated Cost (b(4)) Fixed Fee (b(4)) Total CPFF (b(4)) Amount: (b(4)) (Option Line Item) Product/Service Code: R425 Product/Service Description: Continued ...</p>	1	LO	(b(4))	0.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

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

PAGE OF PAGES

3

21

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

DATE OF ORDER 05/23/2008 CONTRACT NO. HSHQDC-06-D-00024

ORDER NO. HSHQDC-08-J-00134

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
0003	<p>ENGINEERING & TECHNICAL SERVICES</p> <p>Option 2 CPFF Engineering support to the HSIN Next Generation in accordance with the attached Performance Work Statement (PWS) dated April 14, 2008 and the Functional Requirements Document (FRD) dated March , 11 2008</p> <p>Estimated Cost (b(4)) Fixed Fee (b(4)) Total CPFF (b(4))</p> <p>Amount: (b(4)) (Option Line Item) Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES</p>	1	LO	(b(4))	0.00	
0004	<p>Option 3 CPFF Engineering support to the HSIN Next Generation in accordance with the attached Performance Work Statement (PWS) dated April 14, 2008 and the Functional Requirements Document (FRD) dated March , 11 2008</p> <p>Estimated Cost (b(4)) Fixed Fee (b(4)) Total CPFF (b(4)) Amount: (b(4)) (Option Line Item) Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES</p>	1	LO	(b(4))	0.00	
0005	<p>Option 4 CPFF Engineering support to the HSIN Next Generation in accordance with the attached Performance Work Statement (PWS) dated April 14, 2008 and the Functional Requirements Document Continued ...</p>	1	LO	(b(4))	0.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

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

PAGE OF PAGES

4

21

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

DATE OF ORDER: 05/23/2008
CONTRACT NO.: HSHQDC-06-D-00024

ORDER NO.: HSHQDC-08-J-00134

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	<p>(FRD) dated March , 11 2008</p> <p>Estimated Cost (b(4)) Fixed Fee (b(4)) Total CPFF (b(4)) Amount: (b(4)) (Option Line Item)</p> <p>Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES</p> <p>The total amount of award: \$62,106,429.00. The obligation for this award is shown in box 17(i).</p>					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

Section D – Packaging and Marking

D.1 – Packaging and Marking

Packaging and marking shall be performed in accordance with the instructions of the basic EAGLE contract.

Section E – Inspection and Acceptance

E.1 – Inspection and Acceptance

EAGLE sections E.1 and E.2 FAR clauses incorporated by reference.

E.2 – Inspection and Acceptance – Quality Assurance

As a performance based task order, the contractor identified performance measures and metric/service level agreements will form the basis of the inspection and acceptance Quality Assurance program.

Using the contractor provided metrics, the Government and the contractor will agree on a Quality Assurance framework, and methodology to establish initial performance levels and the ongoing performance level management. The Governance framework will continuously seek to refine, allocate and adjust service levels to reflect changes in priority and to ensure that throughout the life of this agreement that the program delivers improved performance and reduced cost.

E.3 – Place of Inspection and Acceptance

Inspection and acceptance of all work performed, reports, and other deliverables under this task order shall be performed by the Contracting Officer's Technical Representative (COTR) in accordance paragraphs E.4 through E.8.

E.4 – Scope of Inspection

All deliverables will be inspected for content, completeness, accuracy and conformance to the task order requirements by the COTR.

E.5 – Basis of Acceptance

- a. The basis for acceptance of services will be in compliance with the best commercial practices and those requirements provided in the task order.
- b. Items such as Other Direct Costs (ODC) (e.g. travel, equipment purchases) must be approved in advance. Request for ODC purchases must include a ROM estimate. ODCs will be accepted upon receipt of proper documentation as specified in the performance work statement (PWS).
- c. Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

- d. The contractor shall provide electronic copies of each deliverable. Electronic copies shall be delivered via email attachment or other media by mutual agreement of the parties. The electronic copies shall be compatible with MS Office 2000 or other applications as appropriate and mutually agreed to by the parties.
- e. The contractor shall use best commercial practice for formatting deliverables under this contract.
- f. All of the Government's comments on deliverables must either be incorporated in the succeeding version or the contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.
- g. If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, improper format, or otherwise does not conform to the requirements stated within this solicitation, the document may be immediately rejected without further review and returned to the contractor for correction and re-submission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the COTR.
- h. For software development, the final acceptance of the software program will occur when all discrepancies, errors or other deficiencies identified in writing by the Government have been resolved, either through documentation updates, program correction, or other mutually agreeable methods.

E.6 – Draft Deliverables

The Government will provide written acceptance, comments and/or change requests, if any, within 15 working days from receipt by the Government of each initial deliverable. Upon receipt of the Government comments, the contractor shall have 15 working days to incorporate the government's comments and/or change requests and to resubmit the deliverable in its final form.

E.7 – Written Acceptance

The Government shall provide written notification of acceptance or rejection of all final deliverables within thirty (30) calendar days of receipt. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection. The contractor shall assume acceptance if not notified by the Government within thirty (30) calendar days.

E.8 – Non-Conforming Products or Services

Non-conforming products or services will be rejected. Deficiencies will be corrected within 30 calendar days of the rejection notice. If the deficiencies cannot be corrected within 30 calendar days, the contractor will immediately notify the COTR of the reason for the delay and provide a proposed corrective action plan within ten (10) working days of notification.

Section F – Deliveries and Performance

F.1 – Period of Performance

The task order's basic period of performance shall be from May 27, 2008 – May 26, 2009. Beyond the base period, there are four one-year option periods. Taken together with the base period and option periods, the task order term may last for a total period not to exceed five years.

Periods of Task Order Performance to begin as follows:

Base Period: May 27, 2008 – May 26, 2009
Option Year 1: May 27, 2009 – May 26, 2010
Option Year 2: May 27, 2010 – May 26, 2011
Option Year 3: May 27, 2011 – May 26, 2012
Option Year 4: May 27, 2012 – May 26, 2013

F.2 – Option to Extend the Term of the Contract

OPTION TO EXTEND THE TERM OF THE CONTRACT (FAR 52.217-9) (MAR 2000)

- (a) The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.
- (b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
- (c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months, excluding an extension under 52.217-8.

F.3 – Place of Performance

The primary place of performance for the HSIN NextGen task order contractor shall be at the contractor's facility which is required to be located within the National Capital Region, or a fifty mile radius of the DHS Office of Operations Coordination (OPS), currently at the Nebraska Avenue Complex (NAC) in NW Washington DC. HSIN NextGen system build activities shall be conducted at the DHS Data Centers (to be determined) and HSIN NextGen testing tasks may require periods of travel to one or more of the DHS HSIN NextGen stakeholder offices located in the continental United States, United States territories, and internationally.

Section G – Contract Administration Data

G.1 – Contracting Officer

The TO Contracting Officer (TO CO) is the only person authorized to make any changes, approve any changes in the requirements of this Task Order, obligate funds and authorize the expenditure of funds, and notwithstanding any provisions contained elsewhere in this task order, the said authority remains solely in the TO CO. In the event the contractor makes any changes at the direction of any person other than the TO CO, the change will be considered to have been without authority and no adjustment will be made in the task order price to cover any increase in costs occurred as a result thereof. It is incumbent on the Contractor to make sure that this requirement is enforced, or work performed will be performed at the Contractor's own risk.

The following TO Contracting Officer is assigned to this Task Order:

TO Contracting Officer:

NAME: Purnell Drew
PHONE NO.: (202) 447- (b(2))
EMAIL: (b(2))

G.2 – Contracting Officer's Technical Representative (COTR) COTR (HSAR 3052.242-72)(DEC 2003)

(a) The Contracting Officer may designate Government personnel to act as the Contracting Officer's Technical Representative (COTR) to perform functions under the task order such as review or inspection and acceptance of supplies, services, including construction, and other functions of a technical nature. The Contracting Officer will provide a written notice of such designation to the Contractor within five working days after task order award. The designation letter will set forth the authorities and limitations of the COTR under the task order.

(b) The principal role of the COTR is to support the Contracting Officer in managing the work conducted under Section C of this Task Order. This is done through furnishing technical direction within the confines of the task order, monitoring performance, ensuring requirements are met within the terms of the task order, and maintaining a strong relationship with the Contracting Officer. As a team, the Contracting Officer and COTR must ensure that program requirements are clearly communicated and that the services are performed to meet them.

G.3 – Contracting Officer's Technical Representative Designation The following TO COTR is assigned to this Task Order:

NAME: (b(2) b(6))
PHONE NO.: (202) 447- (b(2))
EMAIL: (b(2) b(6))

G.4 – Changes in COTR Designation(s)

The COTR may be changed at any time by the Government without prior notice to the Contractor. Notification of the change, including the name and phone number of the successor COTR, will be promptly provided to the Contractor by the TO Contracting Officer in writing.

G.5 – Invoice Submission - Data Elements

The data elements indicated below shall be included on each invoice. Details and format of invoices shall be consistent with structure specified by the COTR.

Vendor Name
Invoice Number
Invoice Date
Date of Service/Product provided
Payment/Vendor Address, Telephone Number, Other Contact information
Task Order Month
Fiscal Year
Payment Due Date
Contract Number
Task Order Number
Work Order number (if applicable)
DHS Functional/Budget Code/Accounting Data
Cumulative Value to Date
Total Amount Invoiced
Vendor Point-of-Contact
DHS Point-of-Contact
Grand Total per Invoice
Page Numbers
Shipping and Payment term

G.6 – Invoice Submission – Material Order Status Report

A report of all material/labor billed to DHS is required each month to track outstanding equipment in the “field” or residing at DHS HQ. The report shall include a status of the DHS 700-21 Material Inspection and Receiving Report, a government Point-of-Contact (POC), the equipment delivery location, equipment operational location, cost of each unit, lease duration/useful life, date of acquisition, type of equipment, system capabilities/specifications, and the bureau the equipment is supporting. The data must be provided in an application that is consistent with DHS approved software, preferably Microsoft Excel or Microsoft Access format.

G.7 – Electronic Invoice Submission

Electronic invoices must be submitted to:
www.DOB-Invoice@DHS.GOV within thirty (30) days of services rendered.

G.8 – Travel

Travel Regulations

As required by EAGLE Contract section H.6.1, the contractor shall comply with the guidance in FAR 31.205-46 using the regulations specified below.

- a. Federal Travel Regulations (FTR) - prescribed by the General Services Administration, for travel in the contiguous United States.
- b. Joint Travel Regulations (JTR), Volume 2, DoD Civilian Personnel, Appendix A. prescribed by the Department of Defense, for travel in Alaska, Hawaii, and outlying areas of the United States.
- c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas", prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

Travel Authorization Requests

Prior to any long distance travel, the contractor shall prepare a Travel Authorization Request for Government review and COTR approval. The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

Content of Travel Requests

Requests for travel approval shall contain:

Date, time and points of departure

Destination, time and dates of arrival

Name of each contractor employee and position title

Include a description of the travel proposed including a statement as to purpose

Identify the Task Order number

Identify the CLIN(s) associated with the travel

Be submitted in advance of the travel with sufficient time to permit review and approval.

G.9 – Incremental Funding

(1) The contractor is required to comply with the terms and conditions of the contract in accordance with FAR Clause 52.232-22, Limitation of Funds. A total of \$10,000,000.00 has been provided as incremental funding. The amount of (b(4)) as been allotted to cover the costs incurred in the performance of the services specified in the PWS. An additional (b(4)) has been allotted to cover the fixed fee.

(2) In accordance with the Limitation of Funds clause, the Government shall not be obligated to reimburse the contractor for any costs (including termination costs) in excess of the above-stated amount and the contractor will not be obligated to continue performance or incur cost in excess of the above-stated amount until additional funds are made available by the issuance of a unilateral modification from the Contracting Officer. In accordance with paragraph B of the Limitation of Funds clause, \$10,000,000.00 has been allotted to cover the costs and fee incurred in the performance of the services specified in the SOW.

(3) The above funds are estimated to cover the period from date of task order award through December 1, 2008.

Section H – Special Task Order Provisions

H.1 – General

The contractor shall comply with the terms and conditions of the EAGLE contract in addition to the special provisions set forth in the Task Order RFP.

H.2 – Key Personnel

Under H.2, KEY PERSONNEL, paragraph (b) of the basic contract, the following personnel are determined to be key personnel within the meaning of the provision:

NAME

POSITION

[b(4)]

Program Manager
Chief Architect
Development/Integration Manager
Operations Manager

H.3 - Security Requirements

All of the effort to be performed by this task order will require access/protection of SBU information/data. The contractor shall ensure that all appropriate security and protection actions are taken (including providing personnel and procedures) consistent with the task security requirements.

The contractor will have access to and be working with information that is sensitive but unclassified, as defined by the Computer Security Act of 1987. Furthermore, the information is subject to the provisions of the Privacy Act (or any other appropriate law that applies to the information to be handled). This information will be treated as confidential information.

If the contractor is to perform work at their site:

The contractor's facility and ADP systems are required to be accredited and certified in accordance with OMB Circular A-130 Appendix III. Contact DHS' Information System Security Office for additional information.

H.4 – Mandatory Security Requirement – Security Requirements for Unclassified Information Technology Resources

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

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

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

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

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

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

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

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

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

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.5, September 30, 2007) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

H.5 – Mandatory Security Requirement – Security Review

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS including the Office of Inspector General, Contracting Officers Technical Representative (COTR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

H.6 – Mandatory Security Requirement – Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 Information Technology Systems Security and the DHS Sensitive Systems Handbooks prescribe policies and procedures on security for IT resources. Compliance with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors is required for all work performed under this contract. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

H.7 – Mandatory Security Requirement – Interconnection Security Agreements

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnect service agreements.

Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both DAAs or by the officials designated by the DAA.

H.8 – Associate Contractors

Performance of this effort may require the task order contractor to work closely with other contractors. The close interchange with associate contractor(s) may require access to, or release of, proprietary or limited/restricted rights data. To facilitate close cooperation and maximum effectiveness, the Contractor shall enter into agreement(s) with associate contractors to adequately protect such data from unauthorized use or disclosure.

H.9 – Drug-Free Workplace

Performance under any task order resulting from this Request for Proposal shall be in accordance with FAR 52.223-6 Drug-Free Workplace.

H.10 – Contractor Personnel – Employment Eligibility

The Contractor will ensure that each employee and potential employee provide his/her name and verify their identity. The Contractor shall be responsible to the Government for acts and omissions of his employees as well as Subcontractor(s) and their employees.

Subject to existing law, regulations and/or other provisions of this contract, illegal or undocumented aliens shall not be employed by the Contractor or perform on this contract. The

Contractor shall ensure this provision is expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this contract.

DHS OPS has determined that performance of this contract requires the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), access to sensitive but unclassified (SBU) information. SBU is unclassified information for official use only. Contractor employees that do not have a security clearance and require access to SBU information will be given a suitability determination. Requirements for suitability determination are defined in Section H.15.

H.11 – Contractor Personnel – Continued Eligibility

If a prospective employee is found to be ineligible for access to DHS facilities or information, the Contracting Office Technical Representative (COTR) will advise the Contractor that the employee shall not continue to work or be assigned to work under the contract.

DHS reserves the right to deny and/or restrict entrance to government facilities, prohibit employees from assigned work under the contract, deny and/or restrict handling of classified documents/material to any Contractor employee who DHS determines to present a risk of compromising sensitive Government information.

The Contractor shall report to the DHS Office of Security any and all adverse information brought to their attention concerning employees performing under this contract. Reports based on rumor or innuendo shall not be included. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the employee's name and social security number, along with the adverse information being reported.

H.12 – Contractor Personnel - Termination

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

H.13 – Contractor Personnel – Suitability Determination

DHS shall exercise full control over granting, denying, withholding or terminating unescorted government facility and/or access to or handling of both classified and sensitive Government information to Contractor employees based upon the results of a background investigation. DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the task order. No employee of the Contractor shall be allowed unescorted access to a DHS facility without a favorable EOD decision or suitability determination by the DHS Office of Security.

H.14 – Contractor Personnel – Background Investigation

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position sensitivity analysis based on the duties, outlined in the Position Designation Determination (PDD) for Contractor Personnel, each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI. Prospective Contractor employees shall submit the following completed forms to OSI through the COTR no less than thirty (30) days before the start date of the contract or thirty (30) days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

- a. Standard Form 85P, "Questionnaire for Public Trust Positions"
- b. FD Form 258, "Fingerprint Card" (2 copies)
- c. DHS Form 11000-6, "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
- d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
- e. Position Designation Determination for Contract Personnel Form
- f. Foreign National Relatives or Associates Statement

Required forms will be provided by DHS at the time of award of the contract. Only complete packages will be accepted by DHS Office of Security. Specific instructions on submission of packages will be provided upon award of the task order.

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

The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this contract for any position that involves access to or development of any DHS Information Technology (IT) systems. DHS OPS will consider only U.S. Citizens and LPRs for employment on this task order. DHS OPS will not approve LPRs for employment on this task order in any position that requires the LPR to access or assist in the development operation, management or maintenance of DHS IT systems. By signing this task order, the Contractor agrees to this restriction. In those instances where other non-IT requirements contained in the contract can be met by using LPRs, those requirements shall be clearly described.

H.15 – Contractor Personnel – Information Technology Security Clearance

When sensitive government information is processed on DHS telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed and adhere to the procedures governing such data as outlined in "DHS IT Security

Program – Publication DHS MD 4300.Pub”. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

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

H.16 Contractor Personnel – Information Technology Security Training and Oversight

All Contractor employees using DHS automated systems or processing DHS sensitive data shall be required to receive Security Awareness Training.

Contractors involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of DHS, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. DHS Contractors, with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual’s duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access DHS information systems will be continually evaluated while performing these duties. Supervisors should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the DHS Security Office.

H.17 – Security Assurances

DHS Management Directive 4300 requires compliance with standards set forth by NIST, for evaluating computer systems used for processing SBU information. The Contractor shall ensure that requirements are allocated in the functional requirements and system design documents to security requirements are based on the DHS policy, NIST standards and applicable legislation and regulatory requirements. Systems shall offer the following visible security features:

- User Identification and Authentication (I&A) – I&A is the process of telling a system the identity of a subject (for example, a user) (I) and providing that the subject is who it claims to be (A). Systems shall be designed so that the identity of each user shall be established prior to authorizing system access, each system user shall have his/her own user ID and password, and each user is authenticated before access is permitted. All system and database administrative users shall have strong authentication, with passwords that shall conform to established DHS standards. All DHS Identification and Authentication shall be done using the Password Issuance Control System (PICS) or its successor. Under no circumstances will Identification and Authentication be performed by other than the DHS standard system in use at the time of a systems development.
- Discretionary Access Control (DAC) – DAC is a DHS access policy that restricts access to system objects (for example, files, directories, devices) based on the identity of the users and/or groups to which they belong. All system files shall be protected by a secondary access control measure.

- Object Reuse – Object Reuse is the reassignment to a subject (for example, user) of a medium that previously contained an object (for example, file). Systems that use memory to temporarily store user I&A information and any other SBU information shall be cleared before reallocation.
- Audit – DHS systems shall provide facilities for transaction auditing, which is the examination of a set of chronological records that provide evidence of system and user activity. Evidence of active review of audit logs shall be provided to the OPS IT Security Office on a monthly basis, identifying all security findings including failed log in attempts, attempts to access restricted information, and password change activity.
- Banner Pages – DHS systems shall provide appropriate security banners at start up identifying the system or application as being a Government asset and subject to government laws and regulations. This requirement does not apply to public facing internet pages, but shall apply to intranet applications.

H.18 – Data Security

SBU systems shall be protected from unauthorized access, modification, and denial of service. The Contractor shall ensure that all aspects of data security requirements (i.e. confidentiality, integrity, and availability) are included in the functional requirements and system design, and ensure that they meet the minimum requirements as set forth in the DHS Sensitive Systems Handbook and policies and procedures. These requirements include:

- Integrity – The computer systems used for processing SBU shall have data integrity controls to ensure that data is not modified (intentionally or unintentionally) or repudiated by either the sender or the receiver of the information. A risk analysis and vulnerability assessment shall be performed to determine what type of data integrity controls (e.g., cyclical redundancy checks, message authentication codes, security hash functions, and digital signatures, etc.) shall be used.
- Confidentiality – Controls shall be included to ensure that SBU information collected, stored, and transmitted by the system is protected against compromise. A risk analysis and vulnerability assessment shall be performed to determine if threats to the SBU exist. If it exists, data encryption shall be used to mitigate such threats.
- Availability – Controls shall be included to ensure that the system is continuously working and all services are fully available within a timeframe commensurate with the availability needs of the user community and the criticality of the information processed.
- Data Labeling. – The contractor shall ensure that documents and media are labeled consistent with the DHS Sensitive Systems Handbook.

H.19 – DHS Information Technology Standards – Homeland Security Enterprise Architecture (HLS EA) Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures as it relates to this Task Order. Specifically, the contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

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

H.20 – Section 508 of the Rehabilitation Act

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

All EIT deliverables, including but not limited to IOE Implementation Plans, within this work statement shall indicate how compliance with Section 508 standards will be accomplished for both products and services and shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable standards have been identified:

36 CFR 1194.21 – Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this task order including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

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

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

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

36 CFR 1194.25 – Self Contained, Closed Products, applies to all EIT products such as printers, copiers, fax machines, kiosks, etc. that are procured or developed under this task order. Specifically but not limited to items using biometrics as described in this work order shall apply with this requirement as well as any other technical standard involving the use of software or Web based interfaces.

36 CFR 1194.26 – Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.

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

36 CFR 1194.41 – Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required “1194.31 Functional Performance Criteria”, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this task order that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Exceptions for this task order have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

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

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

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

H.21 – Advertisements, Publicizing Awards, and News Releases

All press releases or announcements about agency programs, projects, and contract (task order) awards need to be cleared by the Program Office and the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any

publicity news release or commercial advertising without first obtaining explicit written consent to do so from the Program Office and the Contracting Officer.

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

Section I – Task Order Clauses		
Federal Acquisition Regulation (48 CFR Chapter 1) Solicitation Clauses (http://www.arnet.gov/far/)		
FAR Clause No.	Title	Date
52.251-1	Government Supply Sources	Apr 1984
52.204-2	Security Requirements	Aug 2006
52.204-9	Personal Identity Verification of Contractor Personnel	Sep 2007
52.215-19	Notifications of Ownership Changes	Oct 1997
52.215-21	Requirements For Cost Or Pricing Data Or Information Other Than Cost Or Pricing Data – Modifications Alternate IV	Oct 1997
52.232-20	Limitation Of Costs	Apr 1984
52.232-22	Limitation Of Funds	Apr 1984
52.217-8	Option To Extend Services (Fill-in: 30 days)	Nov 1999
52.219-8	Utilization Of Small Business Concerns	May 2004
52.219-9	Small Business Subcontracting Plan	Sep 2006
52.227-14	Rights In Data – General Alternates IV And V	Jun 1987
52.227-21	Technical Data Declaration Revision And Withholding Of Payment – Major Systems	Jan 1997
52.232-18	Availability Of Funds	Apr 1984
52.237-3	Continuity of Services	Jan 1991
52.244-6	Subcontracts For Commercial Items	Mar 2007
52.245-1	Government Property	Jun 2007
52.245-2	Government Property Installation Operation Services	Jun 2007

DHS AND FAR CLAUSES

Homeland Security Acquisition Regulation (HSAR) Clauses Incorporated By Reference
 (<http://farsite.hill.af.mil/vfhsara.htm>)

HSAR Clause No.	Title	Date
3052.204-70 (EAGLE I.2)	Security Requirements for Unclassified Information Technology Resources	Dec 2003
3052.204-71 (EAGLE I.13)	Contractor Employee Access	Jun 2006
3052.209-70 (EAGLE I.3)	Prohibitions on Contracts with Corporate Expatriates	Dec 2003
3052-209-72 (EAGLE H.33)	Organizational Conflict of Interest	Jul 2004
3052-209-73	Limitation of Future Contracting	Jul 2004
3052.222-70	Strikes or Picketing Affecting Timely Completion of the Contract Work	Dec 2003
3052.222-71	Strikes or Picketing Affecting Access to a DHS Facility	Dec 2003
3052.245-70	Government Property Reports	Jun 2006
If Applicable (EAGLE Ref):		
3052.216-72 (I.7)	Performance Evaluation Plan	Dec 2003

- END OF TASK ORDER PROVISIONS AND CLAUSES -

Section J – List of Attachments

J.1 – List of Attachments

Attachment J-1 – Performance Work Statement

Attachment J-2 – Functional Requirements Document



**Homeland Security Information System (HSIN) Next Generation (NextGen)
Task Order**

PERFORMANCE-BASED WORK STATEMENT

April 14, 2008

Department of Homeland Security
Office of Procurement Operations

TABLE OF CONTENTS

1.0 BACKGROUND	3
2.0 SCOPE	4
2.1 Program Objectives.....	5
3.0 APPLICABLE DOCUMENTS.....	6
4.0 PERFORMANCE REQUIRMENTS.....	7
4.1 Base Year	7
4.1.1 Program and Technical Management.....	7
4.1.2 Spiral 1 – HSIN Critical Sectors (HSIN-CS)	12
4.1.3 Spiral 2 – HSIN NextGen IOC.....	14
4.1.4 Spiral 4 – HSIN NextGen FOC.....	19
4.1.5 HSIN NextGen Operations and Maintenance (O&M) Support	22
4.2 Option 1	23
4.2.1 Program and Technical Management.....	23
4.2.2 Spiral 3 – HSIN NextGen Maturing Operational Capability (MOC).....	26
4.2.3 Spiral 4 – HSIN NextGen FOC.....	27
4.2.4 HSIN NextGen O&M Support.....	30
4.3 Option 2	32
4.3.1 Program and Technical Management.....	32
4.3.2 HSIN NextGen O&M Support.....	34
4.4 Option 3	35
4.4.1 Program and Technical Management.....	35
4.4.2 HSIN NextGen O&M Support.....	38
4.5 Option 4	39
4.5.1 Program and Technical Management.....	39
4.5.2 HSIN NextGen O&M Support.....	41
5.0 PERFORMANCE STANDARDS	43
6.0 INCENTIVES.....	43
7.0 DELIVERABLES AND DELIVERY SCHEDULE	43
8.0 GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION.....	45
9.0 PLACE OF PERFORMANCE.....	45
9.1 Travel Requirements.....	45
10.0 PERIOD OF PERFORMANCE.....	46
11.0 SECURITY.....	46
12.0 QUALITY ASSURANCE SURVEILLANCE PLAN.....	47
13.0 PERFORMANCE STANDARDS	48
14.0 PWS/SOO/FRD CROSS REFERENCE TABLE	55
15.0 CONTRACT WORK BREAKDOWN STRUCTURE.....	60
16.0 PWS/SOO/CWBS CROSS REFERENCE MATRIX.....	64
17.0 CWBS/LABOR CATEGORY/HOURS CROSS REFERENCE MATRIX	69
ATTACHMENT A – IMS CHART.....	82

1.0 BACKGROUND

The purpose of the Enterprise Acquisition Gateway for Leading Edge Solutions (EAGLE) Homeland Security Information Network (HSIN) Next Generation (NextGen) Task Order is to acquire IT support services for the Department of Homeland Security (DHS) Office of Operations Coordination (OPS) Directorate to develop, operate, maintain, and enhance the HSIN NextGen. This Performance Work Statement (PWS) identifies DHS OPS' HSIN NextGen performance requirements for the HSIN NextGen task order contractor.

The mission of the HSIN NextGen is to provide a national secure and trusted platform for information sharing and collaboration between Federal, State, Local, Tribal, Territorial, Private Sector, and International partners engaged in preventing, protecting from, responding to, and recovering from all threats, hazards, and incidents within the authority of DHS.

To support the Department mission, HSIN provides a common, interoperable IT architecture for gathering, fusing, analyzing, and reporting information and threats to the US Homeland. The Common Operational Picture (COP) service is hosted by HSIN and provides leaders and stakeholders with timely, accurate, relevant, and highly integrated all-source information to enhance operational situational awareness and actionable decision making. HSIN and COP are governed by the Homeland Security Act (HSA) of 2002, Homeland Security Presidential Directive (HSPD) #5, DHS Strategic Plan, and DHS Objectives.

The HSIN NextGen task order encompasses the full range of IT infrastructure engineering design, development, implementation, and integration support services required to meet DHS OPS responsibilities under Federal legislation, Presidential Directives, and DHS mission and objectives.

HSIN is a national information sharing and collaboration platform that provides and/or serves as a conduit to Sensitive But Unclassified (SBU) data and analysis regarding people, places, things, events, resources, and activities lawfully owned and maintained by, and shared in a multi-directional, trusted, and secure environment among, DHS and other domestic and international users who are in mission partnership with DHS for the purpose of supporting missions to prevent, protect from, respond to, and recover from all threats, hazards, and incidents included within the scope of DHS authority.

HSIN NextGen will update the current HSIN technology to better enable DHS to meet the requirements of a trusted and secure environment, combined with enhanced capabilities in many areas, such as collaboration tools and information sharing. HSIN NextGen will provide a robust, flexible, and highly reliable framework for implementation of tools and services based on Open-Architecture (OA) and open standards-based Commercial Off-The-Shelf (COTS)/Government Off-The-Shelf (GOTS) products and technologies.

2.0 SCOPE

The Department of Homeland Security (DHS) is conducting a task order competition under the EAGLE program for Information Technology (IT) services, Functional Category 1 (FC1), infrastructure engineering design, development, implementation, and integration.

The contractor shall develop, test, and deliver HSIN NextGen that supports the rapid insertion of COTS/ GOTS products, services, applications, processes and network capabilities with the goal of reducing development costs, shortening lead times to field new technologies. HSIN NextGen will provide DHS, DHS partners, and DHS stakeholders information management capabilities and services including a portal, search, collaboration, enterprise content management, and Service Oriented Architecture (SOA)-based information integration and analysis functions to facilitate their collaboration and information sharing needs for SBU data.

The contractor shall be responsible for providing all necessary information technology development and support services needed to analyze requirements, develop and implement recommended solutions, and operate all IT products and services needed to provide as well as to maintain information technology services for the DHS OPS HSIN NextGen. This includes taking the “as is” state and providing transition to and successful outcomes of the “to be” solution. The contractor shall provide information technology development and support services to design, develop, enhance, provide and manage an architecture and information technology infrastructure that is timely, standard, reliable, secure, flexible, responsive, compliant, and cost efficient in meeting needs of DHS, OPS, HSIN and its stakeholders.

The contractor shall operate and maintain the current HSIN technology, which includes the Common Operating Picture (COP) application, services, tools and associated Oracle database, until all users and data have been migrated to the HSIN NextGen technology. At this point, the current HSIN technology will be decommissioned and operations and maintenance support will continue for HSIN NextGen.

The DHS OPS HSIN NextGen scope is intended to accommodate advances in technology that will allow it to continue to improve the DHS OPS' HSIN NextGen mission performance. Throughout the life of the task order, the contractor shall seek ways to incorporate innovative and emerging technologies and information management techniques that, in the most economic and efficient manner and with a view to return on investment objectives, improve both information technology system performance and support and improve DHS OPS HSIN NextGen's overall mission performance.

The requirements for HSIN NextGen shall be implemented based on an iterative spiral implementation approach. The HSIN NextGen spirals are defined as hardware, infrastructure, software, and the COTS/GOTS products, services, and applications identified for inclusion in a specific spiral. HSIN NextGen spirals as defined by the HSIN Statement of Objectives (SOO) are: HSIN-CS Priority requirements; Initial Operational Capability (IOC); Maturing Operational Capability (MOC); and Final Operational Capability (FOC). The contractor shall use the portal and architecture standards approved by the DHS Enterprise Architecture Board (EAB) (see Task Order Attachment J3, DHS Portal Standards). The HSIN-CS Priority Requirements shall be implemented during the first spiral effort. The second spiral effort shall implement the current HSIN 2.X functional requirements described in the HSIN NextGen Functional Requirements Document (FRD) (Task Order Attachment J1), along with the required technical and security

Attachment J-1

requirements, and transition of users from the current HSIN technology. The third spiral shall complete the transition of users from the current HSIN technology to HSIN NextGen and decommission the current HSIN technology. The fourth spiral shall implement all new functionality (HSIN 3.X) as outlined in the HSIN NextGen FRD, based upon available funding after the completion of the preceding three spirals.

A major intent of the Task Order SOO is to create a “partnership” between DHS OPS and the task order contractor. The DHS OPS/contractor partnership will reflect the attributes of an open, collaborative, and customer-oriented professional relationship; and will serve to ensure the contractors goals are in alignment with those of DHS. In addition to meeting program objectives, the task order contractor is will:

- Establish a contractor/business partner relationship to support the DHS OPS HSIN NextGen;
- Consistently take steps to understand DHS OPS HSIN NextGen’s crucial business issues and opportunities;
- Share the risks and responsibilities of joint implementation and initiatives;
- Ensure its products and services deliver tangible and meaningful business benefits;
- Work collaboratively with other contractors, government agencies, and business partners to ensure project success;
- Resolve the complexities and difficulties that are characteristics of implementing, integrating, maintaining, and securing mission-critical IT systems and solutions, as related to HSIN NextGen; and
- Periodically measure and forecast capacity and systems growth in sync with DHS capital planning requirements and constraints.

Under a performance-based task order structure, performance metrics and Service Level Agreements (SLAs) will be used extensively to monitor the performance of this task order. DHS OPS and the task order contractor will baseline and monitor progress using agreed-to performance metrics and SLAs.

2.1 Program Objectives

The contractor shall support DHS OPS HSIN NextGen requirements to provide and maintain an operational, secure and trusted information sharing and collaboration information technology platform and infrastructure to support DHS’ mission. The objectives of this requirement are to:

- Receive, under a performance-based task order, highly reliable and secure IT services and support that meet or exceed functional requirements and customer expectations;
- Demonstrate improved performance, reliability, security, and reduced cost of the delivered product and service;
- Demonstrate and measure improved performance and outcome with respect to DHS OPS Mission Needs, including rapid, effective collaboration, timely sharing of high-quality, accurate and relevant information, and intelligent, measured automation of critical business processes;

Attachment J-1

- Establish a flexible, transparent, and responsive performance management information system that provides accurate and timely information and data on program status and performance reporting throughout the life cycle of the HSIN NextGen;
- Develop and provide an enhanced HSIN platform that supports DHS OPS' compliance with Government standards and requirements as well as appropriate inventory, security, quality, control, architecture standards, and reporting requirements;
- Maintain appropriate data rights, documentation of the "design" and "as-built" configurations of both instances of HSIN NextGen, and cooperation for transition to another provider, to ensure continuity of services in the event of task order termination, or upon task order re-competition; and
- Establish interconnection security agreements, conduct security reviews and maintain physical security of unclassified information technology resources and sensitive information in this task order.

3.0 APPLICABLE DOCUMENTS

The HSIN NextGen program shall be compliant with the following Government standards and requirements:

- Department of Homeland Security System Life Cycle Guide, Draft, Version 0.9
- Department of Homeland Security Portal Standards (as defined in Task Order Attachment J-3)
- Homeland Security Information Network (HSIN) Functional Requirements Document (FRD), Version 5.0, dated March 11 2008
- Homeland Security Enterprise Architecture (HLS EA)
- HLS EA Technical Reference Model (TRM) Standards and Products Profile
- DHS Geospatial Information Infrastructure (GII)
- Federal Enterprise Architecture
- Computer Security Act of 1987
- Government Information Security Reform Act of 2000
- Federal Information Security Management Act of 2002
- OMB Circular A-130 Appendix III
- Section 508 of the Rehabilitation Act of 1973 (amended)
- Federal Travel Regulations, General Services Administration
- Joint Travel Regulations, Volume 2, DoD Civilian Personnel, Appendix A
- Department of State Standardized Regulations, Section 925

The contractor shall incorporate the best commercial practices, industry standards and procedures as defined below:

- Earned Value Management System ANSI/EIA Standard 748-A
- Capability Maturity Model Integrated (CMMI) for Development
- ISO 9001:2000 Quality Management System

4.0 PERFORMANCE REQUIREMENTS

This section is divided into 5 subsections, a Base Year subsection and a subsection for each of the four Option years.

4.1 Base Year

This section is divided into the major activities within the Base Year, including Program and Technical Management, Spiral 1, Spiral 2, Spiral 4 (initial effort), and Operations & Maintenance. Note Spiral 3 is not included in this section since Spiral 3 is an Option 1 year activity, and is included in the Option 1 section.

4.1.1 Program and Technical Management

4.1.1.1 Program Planning and Execution

The contractor shall perform program planning and management to support DHS objectives of the HSIN NextGen.

The contractor shall provide overall program and technical management including active participation in the development of an innovative and efficient transition plan that facilitates the transition from the current HSIN technology to HSIN NextGen. The transition plans shall include strategies and schedules for the agency to transition from the current HSIN technology to HSIN NextGen. The contractor shall ensure that HSIN NextGen installation will not affect other systems located in the designated facility, and that HSIN NextGen downtime is minimized. The contractor will ensure that current users services are not interrupted during the transition and must mitigate risks to achieve a seamless transfer of data.

The program and technical management will involve investment reviews and analysis, as well as contributions to OPS Capital Planning and Investment Control (CPIC) activities and development of Certification and Accreditation (C&A) documents, including Privacy Impact Assessments. The program and technical management will involve contributions to DHS/OPS Enterprise Architecture and Security governance boards and processes.

The contractor shall efficiently provide ongoing delivery of the HSIN NextGen capabilities, technology and services. Ongoing delivery of HSIN NextGen capabilities, technology and services include quality management activities such as the management of related performance measures and execution of quality assurance and quality control plans; management of required changes to SLAs and other agreements relevant to achieving optimal ongoing service delivery; collaboration and frequent communications between the task order contractor and stakeholders internal and external to DHS OPS to ensure optimal service delivery. The contractor shall promote the sense of partnership and provide a service delivery solution architecture that ensures cooperative relationships to solve operational problems.

The contractor shall consider risk management an integral part of the HSIN NextGen service delivery to be performed. Risk management includes ongoing analysis and recommendations regarding existing internal systems and applications that are currently performing at acceptable levels.

The contractor shall also provide program and technical management to include the development of program plans that are consistent with DHS OPS constraints, fall within the bounds of legal authority, and achieve the following objectives:

Attachment J-1

- Maintain and sharpen the DHS OPS focus on mission-oriented services;
- Promote innovative solutions that can be leveraged by the government; and
- Provide increased flexibility and reduction in time to deploy system and/or process changes (fewer barriers to stakeholders for implementing enhancements).

The contractor shall provide best practices, technologies, tools, and support to quality and operational assessments, integration testing and system test and evaluation, including security certification and accreditation, for IT systems.

The contractor shall participate with independent verification and validation to assure the monitoring and evaluation of projects.

The contractor and/or its teaming partners/major subcontractors performing systems engineering on this contract shall use the CMM Integration® (CMMI®) Level 3 processes of the prime contractor or teaming partners/major subcontractors' business unit leading the engineering work on this contract. This includes following the DHS documented System Life Cycle (SLC).

The HSIN NextGen program shall be managed in accordance with the following plans:

- Program Plan
- Tailored Development Processes
- Risk Management Plan
- IT Security Plan
- Master Test and Evaluation Plan
- Software Development Plan
- Quality Assurance Surveillance Plan
- Service Level Agreements
- Integrated Master Plan
- Integrated Master Schedule
- Subcontractor Management Plan
- Configuration Management Plan
- Data Management Plan
- Program Quality Plan
- Training Plans

4.1.1.1.1 Program Plan

The contractor shall develop a Program Plan to define the necessary activities to support DHS OPS objectives.

4.1.1.1.2 Tailored Development Process

The contractor shall define tailored processes and procedures for managing system engineering, software development, implementation, COTS/GOTS integration, organizational change and training, and maintenance. The contractor's processes and DHS System Life Cycle Guide shall be used to establish the specific processes for HSIN development.

4.1.1.1.3 Risk Management Plan

The contractor shall develop a Risk Management Plan to describe the approach to be followed for identification, management and mitigation of program risks including technical, schedule and cost risks.

Attachment J-1

4.1.1.1.4 IT Security Plan

The contractor shall abide by DHS's policies and procedures on contractor personnel security requirements, set forth in various management directives (MDs). MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how contractors must handle sensitive but unclassified information. MD 4300.1, entitled Information Technology Systems Security, and the DHS Sensitive Systems Handbook, prescribe the policies and procedures on security for Information Technology resources. Compliance with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically, is required in all contracts that require access to facilities, IT resources or sensitive information.

The contractor shall use system security processes in accordance with DHS Information Technology Security Program Publication 4300A and DHS Information Technology Security Program Publication 4300B. The contractor shall provide, implement, and maintain an IT Security Plan for HSIN NextGen within 30 days after contract award. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. Within 6 months after contract award, the contractor shall submit written proof of IT HSIN NextGen Security accreditation to DHS for approval by the DHS Contracting Officer.

The IT Security Plan shall comply with Federal laws that include but are not limited to the following:

- Computer Security Act of 1987,
- Government Information Security Reform Act of 2000,
- Federal Information Security Management Act of 2002, and
- OMB Circular A-130.

4.1.1.1.5 Master Test and Evaluation Plan

The contractor shall identify and document the scope, content, methodology, sequence, management and responsibilities for HSIN test activities in the Master Test and Evaluation Plan (MTEP).

4.1.1.1.6 Software Development Plan

The contractor shall develop a Software Development Plan (SDP) for the HSIN NextGen work. The contractor shall document the tailored engineering development activities from the contractor's processes and DHS System Life Cycle.

4.1.1.1.7 Quality Assurance Surveillance Plan

The contractor shall support the Government in developing a Quality Assurance Surveillance Plan (QASP) that aligns to the performance goals of the DHS OPS HSIN NextGen.

4.1.1.1.8 Service Level Agreements (SLA)

The contractor shall support the Government in developing Service Level Agreements (SLA) that align to the performance goals of the DHS OPS HSIN NextGen. The contractor shall monitor and make appropriate adjustments as approved by the Government.

4.1.1.2 Earned Value Management Systems (EVMS)

The contractor shall develop and submit monthly Earned Value reports addressing all applicable tasks under this task order as required by the overarching EAGLE contract, section H.32. The contractor shall submit four (4) hard copies of the required Cost Performance Report (CPR) Formats 1, 3, and 5 and the Contractor Funds Status Report ((CSFR) at the task order level) Earned Value reports to the Contracting Officer's Technical Representative (COTR) on a monthly basis by the 15th business day of each month. In addition, the contractor shall submit the Earned Value reports to the COTR via email. The soft copy Earned Value reports shall be transmitted in Microsoft format.

The required Earned Value reports shall include the following:

- CPR Format 1 - WBS-oriented cost report: All costs incurred for the applicable tasks under this order shall be organized according to the WBS at a level to be directed by the COTR.
- CPR Format 3 - Baseline Report. This format shall provide information on the task order baseline and change tracking. The contractor shall report the following measures: Budgeted Cost of Work Scheduled (BCWS), Actual Cost of Work Performed (ACWP), Budgeted Cost of Work Performed (BCWP – Earned Value), cumulative Cost Performance Index (CPI), and cumulative Schedule Performance Index (SPI). Contractor shall also furnish the cumulative time-based Schedule Performance Index.
- CPR Format 5 - Problem Analysis Report/Variance Narrative: This report shall discuss and provide explanations for cost and schedule variances that have exceeded threshold. In addition, this report shall provide an explanation as to why the variance occurred and descriptions on how the contractor plans to resolve the cause of the variance. Contractor shall also furnish data monthly on the success for previous corrective actions taken.
- Contract Funds Status Report: This report shall address the current task order funding levels for all task order CLINs.

The Contractor shall use the information in these EVM reports to analyze the effectiveness of the EVMS and both the contract performance and the overall program progress. The Contractor shall take appropriate action based on those findings.

The contractor shall build an event-based Integrated Master Plan (IMP) for the HSIN and HSIN NextGen system that correlates to the Integrated Master Schedule (IMS), Contract Work Breakdown Structure (CWBS), PWS, EVMS and the contractor's organizational structure. The contractor shall identify, based on the CWBS, a hierarchy of key program Events, Accomplishment, Criteria and supporting efforts that define the HSIN NextGen Program. Each program Event, Accomplishment and Criteria shall have specific entrance and exit criteria.

The contractor shall develop and maintain an Integrated Master Schedule (IMS) developed by logically networking detailed program activities. The schedule shall contain the contract IMP events and milestones, accomplishments, criteria, and activities from contract award to the completion of the contract. The contractor shall ensure schedule integration with its subcontractors and shall verify and ensure the validity of the subcontractors' schedule data, including demonstrating effective methods for incorporating schedule data from subcontractors into the contractor's IMS.

Attachment J-1

The contractor shall participate in the Integrated Baseline Review within 90 calendar days after contract award. The contractor shall also participate in an IBR within 90 calendar days whenever a major task order modification has been awarded. The objective of the integrated baseline review is for the Government and the contractor to jointly assess areas, such as the Contractor's planning, to ensure complete coverage of the statement of work, logical scheduling of the work activities, resources, and identification of inherent risks.

4.1.1.3 Subcontract Management

The contractor shall develop a Subcontract Management Plan for planning and oversight of the HSIN program subcontractors.

4.1.1.4 Configuration Management

The contractor shall develop and maintain a Configuration Management Plan (CMP). The contractor shall develop and maintain a Data Management Plan (DMP) as an appendix to the CMP. CM personnel shall provide technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, audit and verify compliance with specified requirements.

4.1.1.5 Program Quality Assurance

The contractor shall establish a Program Quality Plan to identify the appropriate quality assurance activities, methods, and tools for the HSIN NextGen program. The Quality Assurance personnel will perform the activities in accordance with the Program Quality Plan and Quality Assurance Surveillance Plan (QASP):

- Monitor program activities, as described in the QASP,
- Perform work product inspections, including review of deliverables,
- Audit activities and products against their documented processes, specifications, standards, and requirements
- Witness tests,
- Monitor quality activities of subcontractors,
- Manage the quality of products received from suppliers,
- Ensure that corrective or preventive action taken to eliminate the causes of actual or potential non-conformities is appropriate for scope of the problem and the associated risks,
- Report the results of QA activities, and
- Assist the Government in quality activity, upon request.

4.1.1.6 Program Reviews

The contractor shall conduct program reviews to assess program status. The contractor shall develop and deliver agendas prior to the conduct of customer program review meetings. Program reviews shall identify program risks and issues supporting course-correction planning. The contractor shall prepare minutes that detail the review.

4.1.1.7 Performance Measures

The contractor shall develop and support performance measures collection and reporting derived from this document and the HSIN Functional Requirement Document (FRD). The contractor shall collect and report performance measures in accordance with the QASP. The contractor performance on the HSIN contract shall be verified against performance based metrics that

Attachment J-1

permit the Government to monitor and report on the contractor's cost, schedule, technical, and management performance while executing the HSIN NextGen contract. The Government may perform surveillance on the contractor's performance in accordance with the surveillance methodologies presented in the QASP. The Contractor Performance Measurement Matrices may be used by Government evaluators to determine compliance with contracted performance required under the contract.

4.1.2 Spiral 1 – HSIN Critical Sectors (HSIN-CS)

This section provides the core activities that support the technical objectives specified by the Statement of Objectives unique to Spiral 1 HSIN-CS capabilities. Spiral 1 shall be completed 30 days after contract award.

4.1.2.1 Technical Management

The contractor Integrated Product Team (IPT) Lead and team members will participate in Spiral 1 program planning, planning for an efficient HSIN to HSIN-CS technology transition, risk identification and mitigation, and tailoring the development process. All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. The contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware or software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model.
- In compliance with OMB mandates, all network hardware shall be Internet Protocol version 6 (IPv6) compatible without modification, upgrade, or replacement.

As appropriate, the contractor will contribute to DHS/OPS EA and Security governance boards and processes.

The contractor implementations shall comply with the policies and requirements set forth in the DHS Geospatial Information Infrastructure (GII), including the following:

- The DHS geospatial model shall be used building the GII.
- All data within the GII, whether adopted or developed, shall be submitted to the DHS EDMO for review and insertion into the DHS Reference Model.

4.1.2.2 Architecture and System Engineering

The contractor shall develop system requirements and architecture to support HSIN-CS functional requirements as defined by Task Order Attachment J2 to support up to 20,000 users. The HSIN-CS architecture shall support the basic functionality required from an information sharing portal. The contractor shall document the HSIN-CS system requirements in a draft HSIN System Specification and system architecture in a draft System Design Document (SDD). System requirements shall be allocated to system design components and trace matrix included with the SDD. System design documentation shall include interfaces between the current HSIN

and HSIN NextGen to facilitate integrated data exchange in accordance with guidance provided from DHS OPS.

4.1.2.3 Analysis, Design, Development and Implementation

The contractor shall implement HSIN-CS functional requirements as defined by Task Order Attachment J2 to support up to 20,000 users. The HSIN-CS implementation will support the basic functionality required from an information sharing portal.

The contractor will set up lab services and install and configure GOTS and COTS products. Activities will include update of user and access information as well as generation of specialized bulk upload scripts.

The contractor shall document unit and integration test plans and procedures and execute tests to ensure the proper operation and function of the HSIN-CS functional requirements. The contractor shall obtain Government approval to transition to System Integration Testing.

The contractor shall develop Spiral 1 software Version Description Document (VDD) describing the software baseline and/or changes that are incorporated in the software release, all of the physical media and documentation associated with the version, applicable security and privacy considerations and license provisions.

4.1.2.4 Certification and Accreditation

The Government will complete Spiral 1 Certification and Accreditation (C&A) activities. The contractor will provide support to the Government to complete the C&A activities.

4.1.2.5 System Test and Evaluation

The contractor shall test HSIN-CS functional requirements as defined by Task Order Attachment J2 to support up to 20,000 users. The HSIN-CS testing shall support the basic functionality required from an information sharing portal.

The contractor shall document and execute test procedures to ensure the proper operation, usability, and function of the HSIN-CS requirements. The contractor shall also perform regression testing to ensure related capabilities are not degraded. The contractor shall include usability testing from the initial design stages through user acceptance. The contractor shall document the results of the testing performed. The contractor shall include support for Government required testing (e.g. user acceptance testing, security test and evaluation, 508 Compliance, Independent Validation and Verification (IV&V)) and C&A. The contractor shall obtain Government approval to transition to site activation.

The contractor shall hold a Customer Operational Readiness Review to obtain Government approval for site activation. The contractor shall develop and deliver presentation materials prior to the conduct of the review. The contractor shall prepare minutes that detail the review.

4.1.2.6 Organizational Change and Training

4.1.2.6.1 Organizational Change

Organizational change management is an integral part of the implementation of the HSIN NextGen solution. The contractor shall be an active participant in the identification of organizational change issues (e.g. stakeholder and workforce management, communications and

training) and in developing strategies for mitigating the impact and facilitating the adoption of new and reengineered business processes and supporting applications.

The contractor shall include communication mediums and forums that clearly and concisely communicate the anticipated changes; activities that identify and assess areas of organizational resistance; development of tailored strategies and plans to help guide specific stakeholder groups through the transition; and development of plans to mitigate the adverse affects of the proposed changes and promote the benefits of the transformed business process. The contractor shall interview major stakeholders and determine their information resources and needs for the conduct of their mission. The contractor will communicate the potential benefits, timing and training opportunities associated with the HSIN project.

4.1.2.6.2 Training

The contractor shall design and develop a HSIN Training Plan to facilitate the transition of the users to the HSIN-CS technology; develop training materials; and coordinate training schedules.

The contractor shall prepare training materials to include specific operating techniques for all equipment and for maintenance and test.

The contractor shall support delivery of training to the users of HSIN-CS prior to, concurrent with, or shortly after site activation.

4.1.2.7 Operational/Site Activation

The contractor shall activate HSIN-CS functional requirements as defined by Task Order Attachment J2 to support up to 20,000 users. HSIN-CS shall support the basic functionality required from an information sharing portal.

4.1.2.7.1 Installation Plan

The contractor shall design, develop and provide an installation plan that details overall planning, coordination and site preparations, installation procedures, interconnection with existing systems and conversion of data from legacy systems for HSIN-CS.

4.1.2.7.1.1 Facilities Management. The contractor shall develop and execute a facilities management program that plans, modifies, installs and supports the development, initial and continued operations and life cycle support activities of the HSIN NextGen.

4.1.2.7.1.2 Installation Drawings. The contractor shall design, develop and provide a complete set of detailed Installation Drawings in electronic medium that support installation of HSIN NextGen equipment in DHS and contractor facilities designated for HSIN NextGen operations and support and the interconnection with the facility infrastructure and interconnecting systems such as power, cooling, grounding and communications networks.

4.1.3 Spiral 2 – HSIN NextGen IOC

This section provides the core activities that support the technical objectives specified by the Statement of Objectives unique to Spiral 2 HSIN NextGen IOC capabilities. The contractor shall deliver the Spiral 2 system for IV&V within 8 months after award and achieve IOC within 12 months after the contract award.

4.1.3.1 Technical Management

The contractor IPTs shall participate in program planning, planning for an efficient HSIN-CS to HSIN NextGen technology transition, risk identification and mitigation, incorporation of lessons learned from the Spiral 1, and tailoring the development process. The contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware or software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model.
- In compliance with OMB mandates, all network hardware shall be IPv6 compatible without modification, upgrade, or replacement.

As appropriate, the contractor will contribute to DHS/OPS EA and Security governance boards and processes.

The contractor implementations shall comply with the policies and requirements set forth in the DHS Geospatial Information Infrastructure (GII), including the following:

- The DHS geospatial model shall be used building the GII.
- All data within the GII, whether adopted or developed, shall be submitted to the DHS EDMO for review and insertion into the DHS Reference Model.

4.1.3.2 Architecture and System Engineering

The contractor shall develop a system architecture to support IOC HSIN 2.X functional requirements, including Information Assurance (IA) requirements, a multi-level secure platform, and interfaces with existing HSIN services.

HSIN NextGen shall:

- Enable smooth transition from current HSIN technology;
- Meet the requirements of a trusted and secure environment;
- Provide DHS, partners, and stakeholders with information management capabilities and services including a portal, search, collaboration, enterprise contact management; and
- Provide a Service-Oriented Architecture-based information integration.

HSIN NextGen shall be based on Open Architecture and open standards-based Commercial Off-The-Shelf/Government Off-The-Shelf (COTS/GOTS) products and technologies. HSIN NextGen shall interface with existing HSIN services such as COP and Integrated Common Analytical Viewer (iCAV). The contractor shall participate fully in integration support as dictated by ISAs and joint review & deployment processes to interface with COP and iCAV.

The proposed HSIN NextGen architecture solution shall maximize the use of current HSIN services and applications where feasible. HSIN NextGen will provide a robust, flexible, and highly reliable framework for implementation of tools and services based on open, SOA and

COTS products and technologies. The HSIN NextGen architecture solution shall be aligned with the DHS and Federal Enterprise Architectures. The contractor's architecture and systems engineering solution shall expedite deployment of capabilities and retirement of appropriate legacy systems, combined with enhanced capabilities in many areas, such as collaboration tools and information sharing. The contractor's proposed architecture and systems engineering solution will include transition strategies and high-level plans for migrating the current HSIN to the HSIN NextGen. The contractor's proposed architecture and systems engineering solution shall include an assessment of the risks and rewards associated with various architecture, engineering and operating decisions.

The contractor shall minimize risk by proposing architecture and systems engineering solutions that utilize services currently available and proven in the commercial marketplace and, in some cases, sold as COTS and GOTS products, services, applications, processes and network capabilities with the goal of reducing development costs and shortening lead times to field new technologies.

The contractor will establish a system requirements baseline using the Dynamic Object-Oriented Requirements System (DOORS) tool set and document the HSIN NextGen Spiral 2 IOC system requirements in the HSIN System Specification and system architecture in the HSIN NextGen SDD. System requirements shall be allocated to system design components and the trace matrix included with SDD. The SDD shall include interfaces between the current HSIN and HSIN NextGen to facilitate integrated data exchange in accordance with guidance provided from DHS OPS. The contractor shall define and document the design component interface requirements in an Interface Requirement Specification (IRS).

The contractor shall hold a System Requirements Review (SRR). The contractor shall develop and deliver presentation materials prior to the conduct of the review. The contractor shall prepare minutes that detail the review.

4.1.3.3 Analysis, Design, Development and Implementation

The contractor shall facilitate a smooth transition from the current HSIN technology to the HSIN NextGen capabilities and technology. The contractor shall conduct ongoing evaluation, analysis and validation of system requirements to ensure the delivery of anticipated information technology resources, and sensitive information. Planning and implementation of continuous process improvement solutions are included in this activity.

The contractor shall also provide the planning, analysis, design, development, documentation, integration and qualification of this spiral, including developing, documenting, updating and maintaining interfaces between and among the new HSIN NextGen and the current HSIN that facilitate integrated data exchange of appropriate data in accordance with guidance provided by the DHS OPS. The contractor shall provide the integration of all built or procured HSIN NextGen capabilities and IT Services. In addition, the contractor shall include the development and execution of a strategy and plan for the decommissioning of the current HSIN as HSIN NextGen is incrementally deployed.

The contractor shall implement IOC HSIN 2.X functional requirements, including IA requirements, a multi-level secure platform, and interfaces with existing HSIN services. The contractor shall define and document the design component interface definitions in an Interface Design Document.

Attachment J-1

The contractor shall document unit and integration test plans and procedures and execute tests to ensure the proper operation and function of the HSIN 2.X functional requirements.

The contractor shall provide ongoing service delivery assessments that result in the validation of required outcomes and performance measures. These may include additional market research, alternative analyses, cost benefit analyses, return on investment studies, as well as validation of operational arrangements for the services required in each increment. The contractor shall assist the government in developing SLAs and QASP with measures that align to the performance goals of the DHS OPS HSIN NextGen.

The contractor shall hold a customer Critical Design Review (CDR). The contractor shall develop and deliver presentation materials prior to the conduct of the review. The contractor shall prepare minutes that detail the review.

The contractor shall develop Spiral 2 software Version Description Document describing the software baseline and/or changes that are incorporated in the software release, all of the physical media and documentation associated with the version, applicable security and privacy considerations and license provisions.

4.1.3.4 Certification and Accreditation

The contractor shall develop, maintain and update the HSIN NextGen C&A package to reflect fielded HSIN NextGen capabilities, architectural changes, and addition of or changes to core services for Spiral 2. The Government will be responsible for completing the C&A activities.

4.1.3.5 System Test and Evaluation

Prior to the deployment of HSIN NextGen capabilities and services, the contractor shall provide system testing. This testing shall ensure the operation and function of the transformed business process and service validating the integration, system, performance and acceptance of the HSIN NextGen capabilities and services. The contractor shall develop and implement test plans, procedures, and documentation to support the various stages of testing (e.g., unit, integration, system, performance, and acceptance) for all HSIN NextGen increments and interfaces. The contractor shall include usability testing from the initial design stages through user acceptance.

The contractor shall test HSIN 2.X functional requirements, including Information Assurance requirements, a multi-level secure platform, interfaces with existing HSIN services, and DHS standards. The contractor shall deliver the HSIN 2.X system for IV&V and C&A within 8 months of contract award. IOC shall be achieved 12 months after contract award. The contractor shall document test plans and procedures and execute tests to ensure the proper operation, usability, and function of the IOC HSIN 2.X requirements. The contractor shall also perform regression testing to ensure related capabilities are not degraded. The contractor shall document the results of the testing performed.

The contractor shall hold a customer Production Readiness Review (PRR) to obtain Government approval to proceed to production. The contractor shall develop and deliver presentation materials prior to the conduct of the review. The contractor shall prepare minutes that detail the review.

The contractor shall hold a customer Operational Readiness Review to obtain Government approval to site activation. The contractor shall develop and deliver presentation materials prior to the conduct of the review. The contractor shall prepare minutes that detail the review.

Attachment J-1

4.1.3.5.1 Independent Verification and Validation

The contractor shall develop and execute Spiral 2 verification and validation testing. The Government will have approval authority of the test procedures. The Government will witness a subset of the test execution.

4.1.3.6 Organizational Change and Training

4.1.3.6.1 Organizational Change

Organizational change management is an integral part of the implementation of the HSIN NextGen solution. The contractor shall be an active participant in the identification of organizational change issues (e.g. stakeholder and workforce management, communications and training) and in developing strategies for mitigating the impact and facilitating the adoption of new and reengineered business processes and supporting applications.

The contractor shall include communication mediums and forums that clearly and concisely communicate the anticipated changes; activities that identify and assess areas of organizational resistance; development of tailored strategies and plans to help guide specific stakeholder groups through the transition; and development of plans to mitigate the adverse affects of the proposed changes and promote the benefits of the transformed business process. The contractor shall interview major stakeholders and determine their information resources and needs for the conduct of their mission. The contractor will communicate the potential benefits, timing and training opportunities associated with the HSIN project. The contractor shall document Spiral 2 organization change activities in the HSIN Organizational Change Communication Plan and the results in Stakeholder Assessment Reports.

4.1.3.6.2 Training

The contractor shall design and develop a HSIN NextGen Training Plan. This plan shall define the activities needed to:

- Facilitate transition of the HSIN users to the HSIN 2.X capabilities;
- Identify organizational change issues;
- Developing strategies for mitigating the impact and facilitating the adoption of new and reengineered business processes and supporting applications;
- Identifying communication mediums and forums that clearly and concisely communicate the anticipated changes;
- Develop tailored strategies and plans to help guide specific stakeholder groups through the transition;
- Develop plans to mitigate the adverse affects of the proposed changes and promote the benefits of the transformed business process;
- Coordinate of training schedules; and
- Support delivery of training.

The contractor shall prepare training materials to include specific operating techniques for all equipment, completed technical data on all requirements, and equipment required for maintenance and test.

The contractor shall support delivery of training to the users of HSIN 2.X functional requirements prior to, concurrent with, or shortly after site activation.

4.1.3.7 Operational/Site Activation

The contractor shall activate IOC HSIN 2.X functional requirements, including Information Assurance requirements, a multi-level secure platform, and interfaces with existing HSIN services. Fifty percent of the users and data will be transitioned from the current HSIN technology to HSIN NextGen, including HSIN-CS users. Appropriate waves of user and data transitioning will be accomplished. Lessons learned from the transition shall be captured to improve future transitions.

4.1.3.7.1 Installation Plan

The contractor shall develop transition plans to facilitate transition of the HSIN technology to the HSIN NextGen. The contractor shall design, develop and provide an Installation Plan that details overall planning, coordination and site preparations, installation procedures, interconnection with existing systems and conversion of data from legacy systems for Spiral 2. The contractor will update the test environment/platform for checkout of new capabilities, regression testing, and performance analysis.

4.1.3.7.1.1 Facilities Management. The contractor shall develop and execute a facilities management program that plans, modifies, installs and supports the development, initial and continued operations and life cycle support activities of the HSIN NextGen.

4.1.3.7.1.2 Installation Drawings. The contractor shall design, develop and provide a complete set of detailed Installation Drawings in electronic medium that support installation of HSIN NextGen equipment in facilities designated for HSIN NextGen operations and support and the interconnection with the facility infrastructure and interconnecting systems such as power, cooling, grounding and communications networks.

4.1.4 Spiral 4 – HSIN NextGen FOC

This section provides the base year core activities that support the technical objectives specified by the Statement of Objectives unique to Spiral 4 HSIN NextGen capabilities. FOC shall be accomplished 18 months after contract award.

4.1.4.1 Technical Management

The contractor IPTs shall participate in program planning, planning for an efficient HSIN 2.X to 3.X technology transition, risk identification and mitigation, incorporation of lessons learned from the Spiral 2, and tailoring the development process. The contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware or software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model.
- In compliance with OMB mandates, all network hardware shall be IPv6 compatible without modification, upgrade, or replacement.

As appropriate, the contractor will contribute to DHS/OPS Enterprise Architecture and Security governance boards and processes.

The contractor implementations shall comply with the policies and requirements set forth in the DHS Geospatial Information Infrastructure (GII), including the following:

- The DHS geospatial model shall be used building the GII.
- All data within the GII, whether adopted or developed, shall be submitted to the DHS EDMO for review and insertion into the DHS Reference Model.

4.1.4.2 Architecture and System Engineering

The proposed HSIN NextGen architecture solution shall maximize the use of current HSIN services and applications where feasible. HSIN NextGen will provide a robust, flexible, and highly reliable framework for implementation of tools and services based on open, SOA and COTS products and technologies. The HSIN NextGen architecture solution shall be aligned with the DHS and Federal Enterprise Architectures. The contractor's architecture and systems engineering solution shall expedite deployment of capabilities and retirement of appropriate legacy systems, combined with enhanced capabilities in many areas, such as collaboration tools and information sharing. The contractor's proposed architecture and systems engineering solution will include transition strategies and high-level plans for migrating the current HSIN to the HSIN NextGen. The contractor's proposed architecture and systems engineering solution shall include an assessment of the risks and rewards associated with various architecture, engineering and operating decisions.

The contractor shall minimize risk by proposing architecture and systems engineering solutions that utilize services currently available and proven in the commercial marketplace and, in some cases, sold as commercial off-the-shelf and Government off-the-shelf products, services, applications, processes and network capabilities with the goal of reducing development costs and shortening lead times to field new technologies.

The contractor shall develop a system architecture to support the remaining HSIN 3.X functional requirements, including Information Assurance requirements, a multi-level secure platform, and interfaces with existing HSIN services.

The contractor shall update the system requirements in the HSIN NextGen System Specification and system architecture in the HSIN NextGen System Design Document. System requirements shall be allocated to system design components and trace matrix included with System Design Document. The contractor shall update the Interface Requirements Specification for data requirement changes.

The contractor shall hold a customer SRR for Spiral 4. The contractor shall develop and deliver presentation materials prior to the conduct of the review. The contractor shall prepare minutes that detail the review.

4.1.4.3 Analysis, Design, Development and Implementation

The contractor shall facilitate a smooth transition from the current HSIN 2.X capabilities to the HSIN 3.X capabilities. The contractor shall conduct ongoing evaluation, analysis and validation of system requirements to ensure the delivery of anticipated information technology resources, and sensitive information. Planning and implementation of continuous process improvement solutions are included in this activity.

The contractor shall also provide the planning, analysis, design, development, documentation, integration and qualification of this spiral, including developing, documenting, updating and

maintaining interfaces that facilitate integrated data exchange of appropriate data in accordance with guidance provided by the DHS OPS. The contractor shall provide the integration of all built or procured HSIN NextGen capabilities and IT Services. In addition, the contractor shall include the development and execution of a strategy and plan for the decommissioning of the current HSIN as HSIN NextGen is incrementally deployed.

The contractor shall provide ongoing service delivery assessments that result in the validation of required outcomes and performance measures. These may include additional market research, alternative analyses, cost benefit analyses, return on investment studies, as well as validation of operational arrangements for the services required in each increment. The contractor shall assist the government in developing SLAs and QASP with measures that align to the performance goals of the DHS OPS HSIN NextGen.

The contractor shall implement FOC, HSIN 3.X functional requirements. The contractor shall update the Interface Design Document for data definition changes.

The contractor shall document unit and integration test plans and procedures and execute tests to ensure the proper operation and function of the HSIN 3.X functional requirements.

4.1.4.4 Certification and Accreditation

The contractor shall develop, maintain and update the HSIN NextGen C&A package to reflect fielded HSIN NextGen capabilities, architectural changes, and addition of or changes to core services for Spiral 4. The Government will be responsible for completing the C&A activities.

4.1.4.5 System Test and Evaluation

Prior to the deployment of HSIN 3.X capabilities and services, the contractor shall provide system testing. This testing shall ensure the operation and function of the transformed business process and service validating the integration, system, performance and acceptance of the HSIN NextGen capabilities and services. The contractor shall develop and implement test plans, procedures, and documentation to support the various stages of testing (e.g., unit, integration, system, performance, and acceptance) for all HSIN NextGen increments and interfaces. The contractor shall include usability testing from the initial design stages through user acceptance. The contractor shall include support for Government required testing (e.g. user acceptance testing, security test and evaluation, 508 Compliance, IV&V and C&A.)

The contractor shall test Full Operational Capability (FOC) HSIN 3.X functional requirements, including Information Assurance requirements, a multi-level secure platform, and DHS standards.

The contractor shall document test plans and procedures and execute tests to ensure the proper operation, usability, and function of the FOC HSIN 3.X requirements. The contractor shall also perform regression testing to ensure related capabilities are not degraded. The contractor shall document the results of the testing performed.

4.1.4.6 Organizational Change and Training

4.1.4.6.1 Organizational Change

Organizational change management is an integral part of the implementation of the HSIN NextGen solution. The contractor shall be an active participant in the identification of organizational change issues (e.g. stakeholder and workforce management, communications and

Attachment J-1

training) and in developing strategies for mitigating the impact and facilitating the adoption of new and reengineered business processes and supporting applications.

The contractor shall include communication mediums and forums that clearly and concisely communicate the anticipated changes; activities that identify and assess areas of organizational resistance; development of tailored strategies and plans to help guide specific stakeholder groups through the transition; and development of plans to mitigate the adverse affects of the proposed changes and promote the benefits of the transformed business process. The contractor shall interview major stakeholders and determine their information resources and needs for the conduct of their mission. The contractor will communicate the potential benefits, timing and training opportunities associated with the HSIN project. The contractor shall document Spiral 4 organization change plans in the HSIN Organizational Change Communication Plan.

4.1.4.6.2 Training

The contractor will update the HSIN NextGen Training Plan to facilitate transition of the HSIN NextGen Spiral 2 users to the HSIN NextGen Spiral 4 capabilities, and incorporate HSIN 3.X functional requirements.

The contractor shall prepare training materials to include specific operating techniques for all equipment, completed technical data on all requirements, and equipment required for maintenance and test.

4.1.5 HSIN NextGen Operations and Maintenance (O&M) Support

4.1.5.1 Program Management

The contractor shall update the Transition Plan submitted with the HSIN Proposal. The draft plan will be provided within 3 days after contract award and the final within 15 days after contract award. The contractor shall transition the O&M services for the current HSIN technology, including COP, within 90 days of task order award.

The contractor shall operate and maintain the current HSIN-CS technology and HSIN NextGen IOC, which includes the Common Operating Picture (COP) application and, services, tools, associated Oracle database, and transition of users and data. The O&M support shall provide:

- Personnel, equipment, and materials necessary to provide Help Desk Services [excluding GFE provided Help Desk tools: e.g. 866 help desk number, help desk email, Remedy Ticketing Solution and CISCO call centers with associated hardware] to include the associated hardware and software licenses, their currency and upgrades as required, and all other maintenance documentation and support agreements that will enable complete Operations & Maintenance (O&M) support at all levels.
- System Monitoring (on-site or remote capability utilizing an approved network performance monitoring tool).
- Capture system and mission performance metrics and provide reporting versus SLA
- Support development of, modification to, and execution of all O&M related SLA
- Support and maintenance of approved interfaces with other systems and subsystems
- Support to Configuration Management Process
- Preventative Maintenance on hardware, software per a defined schedule
- Corrective maintenance as required to include patch management

Attachment J-1

- System security vulnerability monitoring and proactive management of hardware and software security enhancements
- Support to Certification and Accreditation activities
- Development, test, and release of Engineering Change Requests (ECR)
- Over the phone training support for users and close interaction with Organization Change and Training Team to address user training needs
- Highly trained Surge Staffing (all tiers) in direct support of National Security Special Events and National Level Exercises or incidents that require a coordinated national response (i.e. Presidential elections, TOPOFF-5, Hurricanes etc.).

4.1.5.2 Help Desk Services

The contractor shall maintain a Help Desk providing 24x7x365 services to the HSIN NextGen user community. The contractor shall provide phone based level 1 support for customer requests for service, user training via phone communications, reports of incidents through a Help Desk responsible for end-to-end call and problems management. The contractor shall track and measure average speed to answer.

4.1.5.3 Tier 2 – System Administration

The contractor shall provide Tier 2 - System Administration staff to perform system monitoring, system and application maintenance, new site creation and site modifications and upgrades as captured within the Change Management automated processing tool and approved by the Change Control Board (CCB), problem detection and correction, and backup/recovery. The Tier 2 - System Administration staff will also be responsible for minor bug fixes and patches and conduct system security vulnerability scans.

4.1.5.4 Tier 3 – Infrastructure & Network Services

The contractor shall provide Tier 3 staff to install or integrate requested and approved hardware and software modifications, baseline Engineering Change Packages (ECP) and implement enhancements approved by the HSIN NextGen PMO and HSIN NextGen CCB, and test/implement major patches or fixes that may be required. The Tier 3 staff will also work directly with the Spiral 1, 2 and 4 IPT to assume responsibility for all system functional improvements once these improvements have been approved by DHS and moved to production. Tier 3 staff will also provide system security support to include enhancements, corrections and fixes to ensure the highest level of security across HSIN NextGen.

4.2 Option 1

This section is divided into the major activities of Option 1 year, including Program and Technical Management, Spiral 3, Spiral 4, and Operations & Maintenance.

4.2.1 Program and Technical Management

4.2.1.1 Program Planning and Execution

The contractor will continue program and technical management, risk management, and update plans to incorporate necessary changes including IPT Structure (e.g. removal of Spiral 1 and 2 IPTs), and to incorporate lessons learned from completed Spirals. Plans to be updated include:

- Program Plan

Attachment J-1

- Integrated Master Plan
- Integrated Master Schedule
- Tailored Development Process
- Master Test and Evaluation Plan
- Software Development Plan
- Quality Assurance Surveillance Plan
- Service Level Agreements

4.2.1.2 Earned Value Management Systems (EVMS)

The contractor shall develop and submit monthly Earned Value reports addressing all applicable tasks under this task order as required by the overarching EAGLE contract, section H.32. The contractor shall submit four (4) hard copies of the required Cost Performance Report (CPR) Formats 1, 3, and 5 and the Contractor Funds Status Report ((CSFR) at the task order level) Earned Value reports to the COTR on a monthly basis by the 15th business day of each month. In addition, the contractor shall submit the Earned Value reports to the COTR via email. The soft copy Earned Value reports shall be transmitted in Microsoft format.

The required Earned Value reports shall include the following:

- CPR Format 1 - WBS-oriented cost report: All costs incurred for the applicable tasks under this order shall be organized according to the WBS at a level to be directed by the COTR.
- CPR Format 3 - Baseline Report: This format shall provide information on the task order baseline and change tracking. The contractor shall report the following measures: Budgeted Cost of Work Scheduled (BCWS), Actual Cost of Work Performed (ACWP), Budgeted Cost of Work Performed (BCWP – Earned Value), cumulative Cost Performance Index (CPI), and cumulative Schedule Performance Index (SPI). Contractor shall also furnish the cumulative time-based Schedule Performance Index.
- CPR Format 5 - Problem Analysis Report/Variance Narrative: This report shall discuss and provide explanations for cost and schedule variances that have exceeded threshold. In addition, this report shall provide an explanation as to why the variance occurred and descriptions on how the contractor plans to resolve the cause of the variance. Contractor shall also furnish data monthly on the success for previous corrective actions taken.
- Contract Funds Status Report: This report shall address the current task order funding levels for all task order CLINs.

The Contractor shall use the information in these EVM reports to analyze the effectiveness of the EVMS and both the contract performance and the overall program progress. The Contractor shall take appropriate action based on those findings.

The contractor shall build an event-based Integrated Master Plan (IMP) for the HSIN and HSIN NextGen system that correlates to the Integrated Master Schedule (IMS), CWBS, Performance Work Statement (PWS), EVMS and the contractor's organizational structure. The contractor shall identify, based on the CWBS, a hierarchy of key program Events, Accomplishment, Criteria and supporting efforts that define the HSIN Program. Each program Event, Accomplishment and Criteria shall have specific entrance and exit criteria.

The contractor shall develop and maintain an Integrated Master Schedule (IMS) developed by logically networking detailed program activities. The schedule shall contain the contract IMP

Attachment J-1

events and milestones, accomplishments, criteria, and activities from contract award to the completion of the contract. The contractor shall ensure schedule integration with its subcontractors and shall verify and ensure the validity of the subcontractors' schedule data, including demonstrating effective methods for incorporating schedule data from subcontractors into the contractor's IMS.

The contractor shall participate in the Integrated Baseline Review within 90 calendar days after Option 1 award. The contractor shall also participate in an IBR within 90 calendar days whenever a major task order modification has been awarded. The objective of the integrated baseline review is for the Government and the contractor to jointly assess areas, such as the Contractor's planning, to ensure complete coverage of the statement of work, logical scheduling of the work activities, resources, and identification of inherent risks.

4.2.1.3 Subcontract Management

The contractor shall update the Subcontract Management Plan for planning and oversight of the HSIN program subcontractors. The subcontract program manager will provide programmatic direction and oversight to the subcontractor.

4.2.1.4 Configuration Management

The contractor shall update the CM Plan. CM personnel will continue to provide technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, audit and verify compliance with specified requirements.

4.2.1.5 Program Quality Assurance

The contractor shall update the Program Quality Plan to identify the appropriate quality assurance activities, methods, and tools for the HSIN NextGen program. The QA personnel will perform the activities in accordance with the Program Quality Plan and QASP:

- Monitor program activities, as described in the QASP,
- Perform work product inspections, including review of deliverables,
- Audit activities and products against their documented processes, specifications, standards, and requirements
- Witness tests,
- Monitor quality activities of subcontractors,
- Manage the quality of products received from suppliers,
- Ensure that corrective or preventive action taken to eliminate the causes of actual or potential non-conformities is appropriate for scope of the problem and the associated risks,
- Report the results of quality assurance activities, and
- Assist the Government in quality activity, upon request.

4.2.1.6 Program Reviews

The contractor shall conduct program reviews to assess program status. The contractor shall develop and deliver agendas prior to the conduct of customer program review meetings. Program reviews shall identify program risks and issues supporting course-correction planning. The contractor shall prepare minutes that detail the review.

4.2.1.7 Performance Measures

The contractor shall update and continue support performance measures collection and reporting.

4.2.2 Spiral 3 – HSIN NextGen Maturing Operational Capability (MOC)

This section provides the core activities that support the technical objectives specified by the Statement of Objectives unique to Spiral 3 HSIN NextGen capabilities. Core activities include:

- Program and Technical Management
- Organizational Change and Training

4.2.2.1 Technical Management

The contractor IPTs will participate in program planning, planning for an efficient transition of users and data, risk identification and mitigation, and appropriate tailoring or the development process.

4.2.2.2 Organizational Change and Training

4.2.2.2.1 Organizational Change

Organizational change management is an integral part of the implementation of the HSIN NextGen solution. The contractor shall be an active participant in the identification of organizational change issues (e.g. stakeholder and workforce management, communications and training) and in developing strategies for mitigating the impact and facilitating the adoption of new and reengineered business processes and supporting applications.

The contractor shall include communication mediums and forums that clearly and concisely communicate the anticipated changes; activities that identify and assess areas of organizational resistance; development of tailored strategies and plans to help guide specific stakeholder groups through the transition; and development of plans to mitigate the adverse affects of the proposed changes and promote the benefits of the transformed business process. The contractor shall interview major stakeholders and determine their information resources and needs for the conduct of their mission. The contractor will communicate the potential benefits, timing and training opportunities associated with the HSIN project.

4.2.2.2.2 Training

The contractor shall support delivery of training to the remaining users of HSIN-CS prior to, concurrent with, or shortly after site activation.

4.2.2.3 Operational/Site Activation

The contractor shall develop transition plans to facilitate decommissioning of the current HSIN technology. The contractor shall activate the remaining users and data from the current HSIN technology to the HSIN NextGen 16 months after contract award. The contractor shall decommission the current technology and perform regression testing as appropriate.

4.2.2.4 Decommissioning

The contractor shall transition the remaining users and data from the current HSIN technology to the HSIN NextGen. The contractor shall decommission the current HSIN technology.

4.2.3 Spiral 4 – HSIN NextGen FOC

This section provides the Option 1 year core activities that support the technical objectives specified by the Statement Of Objectives unique to Spiral 4 HSIN NextGen capabilities. Core activities include:

- Program and Technical Management
- Architecture and Systems Engineering of HSIN NextGen
- HSIN NextGen Analysis, Design, Development and Implementation
- Testing
- Deployment
- Organizational Change and Training

4.2.3.1 Technical Management

The contractor IPTs will participate in program planning, planning for an efficient HSIN 2.X to 3.X technology transition, risk identification and mitigation, incorporation of lessons learned from the Spiral 1, and tailoring the development process. The contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware or software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model.
- In compliance with OMB mandates, all network hardware shall be Internet Protocol version 6 compatible without modification, upgrade, or replacement.

As appropriate, the contractor will contribute to DHS/OPS Enterprise Architecture and Security governance boards and processes.

4.2.3.2 Architecture and System Engineering

The contractor shall continue development of the system architecture to support the remaining FOC HSIN 3.X functional requirements, including Information Assurance requirements, a multi-level secure platform, and interfaces with existing HSIN services.

The proposed HSIN NextGen architecture solution shall maximize the use of current HSIN services and applications where feasible. HSIN NextGen will provide a robust, flexible, and highly reliable framework for implementation of tools and services based on open, SOA and COTS products and technologies. The HSIN NextGen architecture solution shall be aligned with the DHS and Federal Enterprise Architectures. The contractor's architecture and systems engineering solution shall expedite deployment of capabilities and retirement of appropriate legacy systems, combined with enhanced capabilities in many areas, such as collaboration tools and information sharing. The contractor's proposed architecture and systems engineering solution will include transition strategies and high-level plans for migrating the current HSIN to the HSIN NextGen. The contractor's proposed architecture and systems engineering solution shall include an assessment of the risks and rewards associated with various architecture, engineering and operating decisions.

Attachment J-1

The contractor shall minimize risk by proposing architecture and systems engineering solutions that utilize services currently available and proven in the commercial marketplace and, in some cases, sold as commercial off-the-shelf and Government off-the-shelf products, services, applications, processes and network capabilities with the goal of reducing development costs and shortening lead times to field new technologies.

The contractor shall update the system requirements in the HSIN NextGen System Specification and system architecture in the HSIN NextGen System Design Document. System requirements shall be allocated to system design components and trace matrix included with System Design Document. The contractor shall update the Interface Requirements Specification for data requirement changes.

4.2.3.3 Analysis, Design, Development and Implementation

The contractor shall facilitate a smooth transition from the current HSIN 2.X capabilities to the HSIN 3.X capabilities and technology. The contractor shall conduct ongoing evaluation, analysis and validation of system requirements to ensure the delivery of anticipated information technology resources, and sensitive information. Planning and implementation of continuous process improvement solutions are included in this activity.

The contractor shall also provide the planning, analysis, design, development, documentation, integration and qualification of this spiral, including developing, documenting, updating and maintaining interfaces that facilitate integrated data exchange of appropriate data in accordance with guidance provided by the DHS OPS. The contractor shall provide the integration of all built or procured HSIN NextGen capabilities and IT Services. In addition, the contractor shall include the development and execution of a strategy and plan for the decommissioning of the current HSIN as HSIN NextGen is incrementally deployed.

The contractor shall provide ongoing service delivery assessments that result in the validation of required outcomes and performance measures. These may include additional market research, alternative analyses, cost benefit analyses, return on investment studies, as well as validation of operational arrangements for the services required in each increment. The contractor shall assist the government in developing SLAs and QASP with measures that align to the performance goals of the DHS OPS HSIN NextGen.

The contractor shall implement FOC, HSIN 3.X functional requirements. The contractor shall update the Interface Design Document for data definition changes.

The contractor shall document unit and integration test plans and procedures and execute tests to ensure the proper operation and function of the HSIN 3.X functional requirements.

The contractor shall develop and deliver presentation materials prior to the conduct of the review. The contractor shall prepare minutes that detail the review.

The contractor shall develop Spiral 4 software Version Description Document describing the software baseline and/or changes that are incorporated in the software release, all of the physical media and documentation associated with the version, applicable security and privacy considerations and license provisions.

4.2.3.4 Certification and Accreditation

The contractor shall develop, maintain and update the C&A package to reflect fielded HSIN NextGen capabilities, architectural changes, and addition of or changes to core services for Spiral 4. The Government will be responsible for completing the C&A activities.

4.2.3.5 System Test and Evaluation

Prior to the deployment of HSIN NextGen capabilities and services, the contractor shall provide system testing. This testing shall ensure the operation and function of the transformed business process and service validating the integration, system, performance and acceptance of the HSIN NextGen capabilities and services. The contractor shall develop and implement test plans, procedures, and documentation to support the various stages of testing (e.g., unit, integration, system, performance, and acceptance) for all HSIN NextGen increments and interfaces. The contractor shall include usability testing from the initial design stages through user acceptance. The contractor shall include support for Government required testing (e.g. user acceptance testing, security test and evaluation, 508 Compliance, IV&V and C&A.)

The contractor shall test FOC HSIN 3.X functional requirements, including Information Assurance requirements, a multi-level secure platform, and DHS standards. FOC shall be achieved 18 months after contract award.

The contractor shall document test plans and procedures and execute tests to ensure the proper operation, usability, and function of the FOC HSIN 3.X requirements. The contractor shall also perform regression testing to ensure related capabilities are not degraded. The contractor shall document the results of the testing performed.

The contractor shall hold a customer Production Readiness Review to obtain Government approval to proceed to production. The contractor shall develop and deliver presentation materials prior to the conduct of the review. The contractor shall prepare minutes that detail the review.

The contractor shall hold a customer Operational Readiness Review to obtain Government approval to site activation. The contractor shall develop and deliver presentation materials prior to the conduct of the review. The contractor shall prepare minutes that detail the review.

4.2.3.5.1 Independent Verification and Validation

The contractor shall develop and execute Spiral 4 verification and validation testing. The Government will have approval authority of the test procedures. The Government will witness a subset of the test execution.

4.2.3.6 Organizational Change and Training

4.2.3.6.1 Organizational Change

Organizational change management is an integral part of the implementation of the HSIN NextGen solution. The contractor shall be an active participant in the identification of organizational change issues (e.g. stakeholder and workforce management, communications and training) and in developing strategies for mitigating the impact and facilitating the adoption of new and reengineered business processes and supporting applications.

The contractor shall include communication mediums and forums that clearly and concisely communicate the anticipated changes; activities that identify and assess areas of organizational

Attachment J-1

resistance; development of tailored strategies and plans to help guide specific stakeholder groups through the transition; and development of plans to mitigate the adverse affects of the proposed changes and promote the benefits of the transformed business process. The contractor shall interview major stakeholders and determine their information resources and needs for the conduct of their mission. The contractor will communicate the potential benefits, timing and training opportunities associated with the HSIN project. The contractor shall document Spiral 4 organization change activities in the HSIN Organizational Change Communication Plan and the results in Stakeholder Assessment Reports.

4.2.3.6.2 Training

The contractor will update the HSIN NextGen Training Plan to facilitate transition of the HSIN 2.X users to the HSIN 3.X capabilities.

The contractor shall prepare training materials. Training materials shall contain specific operating techniques for all equipment, completed technical data on all requirements, and equipment required for maintenance and test.

The contractor shall support delivery of training to the users of HSIN NextGen functional requirements 3.X prior to, concurrent with, or shortly after site activation.

4.2.3.7 Operational/Site Activation

The contractor shall activate FOC, HSIN 3.X functional requirements 18 months after contract award.

4.2.3.7.1 Installation Plan

The contractor shall develop transition plans to facilitate transition of the HSIN NextGen Spiral 2 technology to the HSIN NextGen Spiral 4 technology. The contractor shall design, develop and provide an Installation Plan that details overall planning, coordination and site preparations, installation procedures, interconnection with existing systems and conversion of data from legacy systems for Spiral 4. The contractor will update the test environment/platform for checkout of new capabilities, regression testing, and performance analysis.

4.2.3.7.1.1 Facilities Management. The contractor shall update the facilities management program that plans, modifies, installs and supports the development, initial and continued operations and life cycle support activities of the HSIN NextGen.

4.2.3.7.1.2 Installation Drawings. The contractor shall design, develop and provide a complete set of detailed Installation Drawings in electronic medium that support installation of HSIN NextGen equipment in facilities designated for HSIN NextGen operations and support and the interconnection with the facility infrastructure and interconnecting systems such as power, cooling, grounding and communications networks.

4.2.4 HSIN NextGen O&M Support

4.2.4.1 Program Management

The contractor shall operate and maintain the current HSIN technology, through MOC; and HSIN NextGen IOC (FRD 2.X) / MOC / FOC (FRD 3.X); which includes the Common Operating Picture (COP) application and, services, tools, associated Oracle database and transition of users and data. The O&M support shall provide:

- Personnel, equipment, and materials necessary to provide Help Desk Services

Attachment J-1

[excluding GFE provided Help Desk tools: e.g. 866 help desk number, help desk email, Remedy Ticketing Solution and CISCO call centers with associated hardware] to include the associated hardware and software licenses, their currency and upgrades as required, and all other maintenance documentation and support agreements that will enable complete Operations & Maintenance (O&M) support at all levels.

- System Monitoring (on-site or remote capability utilizing an approved network performance monitoring tool)
- Capture system and mission performance metrics and provide reporting versus SLA
- Support development of, modification to, and execution of all O&M related SLA
- Support and maintenance of approved interfaces with other systems and subsystems
- Support to Configuration Management Process
- Preventative Maintenance on hardware, software per a defined schedule
- Corrective maintenance as required to include patch management
- System security vulnerability monitoring and proactive management of hardware and software security enhancements
- Support to C&A activities
- Development, test, and release of Engineering Change Requests (ECR)
- Over the phone training support for users and close interaction with Organization Change and Training Team to address user training needs
- Highly trained Surge Staffing (all tiers) in direct support of National Security Special Events and National Level Exercises or incidents that require a coordinated national response (i.e. Presidential elections, TOPOFF-5, Hurricanes etc.).

4.2.4.2 Help Desk Services

The contractor shall maintain a Help Desk providing 24x7x365 services to the HSIN NextGen user community. The contractor shall provide phone based level 1 support for customer requests for service, user training via phone communications, reports of incidents through a Help Desk responsible for end-to-end call and problems management. The contractor shall track and measure average speed to answer.

4.2.4.3 Tier 2 – System Administration

The contractor shall provide Tier 2 - System Administration staff to perform system monitoring, system and application maintenance, new site creation and site modifications and upgrades as captured within the Change Management automated processing tool and approved by the Change Control Board (CCB), problem detection and correction, and backup/recovery. The Tier 2 - System Administration staff will also be responsible for minor bug fixes and patches and conduct system security vulnerability scans.

4.2.4.4 Tier 3 – Infrastructure & Network Services

The contractor shall provide Tier 3 staff to install or integrate requested and approved hardware and software modifications, baseline Engineering Change Packages (ECP) and implement enhancements approved by the HSIN NextGen PMO and HSIN NextGen CCB, and test/implement major patches or fixes that may be required. The Tier 3 staff will also work directly with the Spiral 1, 2 and 4 IPT to assume responsibility for all system functional

improvements once these improvements have been approved by DHS and moved to production. Tier 3 staff will also provide system security support to include enhancements, corrections and fixes to ensure the highest level of security across HSIN NextGen.

4.3 Option 2

This section is divided into the major activities of Option 2 year, including Program and Technical Management and Operations & Maintenance.

4.3.1 Program and Technical Management

This section provides the Option 2 year Program and Technical Management activities that support the technical objectives specified by the SOO.

4.3.1.1 Program Planning and Execution

The contractor will continue program and technical management, risk management, and update plans to incorporate necessary changes including IPT Structure, and to incorporate lessons learned from completed Spirals. Plans to be updated include:

- Program Plan
- Integrated Master Plan
- Integrated Master Schedule
- Tailored Development Process
- Master Test and Evaluation Plan
- Software Development Plan
- Quality Assurance Surveillance Plan
- Service Level Agreements

4.3.1.2 Earned Value Management Systems (EVMS)

The contractor shall develop and submit monthly Earned Value reports addressing all applicable tasks under this task order as required by the overarching EAGLE contract, section H.32. The contractor shall submit four (4) hard copies of the required Cost Performance Report (CPR) Formats 1, 3, and 5 and the Contractor Funds Status Report ((CSFR) at the task order level) Earned Value reports to the COTR on a monthly basis by the 15th business day of each month. In addition, the contractor shall submit the Earned Value reports to the COTR via email. The soft copy Earned Value reports must be transmitted in Microsoft format.

The required Earned Value reports shall include the following:

- CPR Format 1 - WBS-oriented cost report: All costs incurred for the applicable tasks under this order shall be organized according to the WBS at a level to be directed by the COTR.
- CPR Format 3 - Baseline Report: This format shall provide information on the task order baseline and change tracking. The contractor shall report the following measures: Budgeted Cost of Work Scheduled (BCWS), Actual Cost of Work Performed (ACWP), Budgeted Cost of Work Performed (BCWP – Earned Value), cumulative Cost Performance Index (CPI), and cumulative Schedule Performance Index (SPI). Contractor shall also furnish the cumulative time-based Schedule Performance Index.
- CPR Format 5 - Problem Analysis Report/Variance Narrative: This report shall discuss and provide explanations for cost and schedule variances that have exceeded threshold. In addition, this report shall provide an explanation as to why the variance occurred and

Attachment J-1

descriptions on how the contractor plans to resolve the cause of the variance. Contractor shall also furnish data monthly on the success for previous corrective actions taken.

- **Contract Funds Status Report:** This report shall address the current task order funding levels for all task order CLINs.

The Contractor shall use the information in these EVM reports to analyze the effectiveness of the EVMS and both the contract performance and the overall program progress. The Contractor shall take appropriate action based on those findings.

The contractor shall build an event-based Integrated Master Plan (IMP) for the HSIN and HSIN NextGen system that correlates to the Integrated Master Schedule (IMS), CWBS, Performance Work Statement (PWS), EVMS and the contractor's organizational structure. The contractor shall identify, based on the CWBS, a hierarchy of key program Events, Accomplishment, Criteria and supporting efforts that define the HSIN Program. Each program Event, Accomplishment and Criteria shall have specific entrance and exit criteria.

The contractor shall develop and maintain an Integrated Master Schedule (IMS) developed by logically networking detailed program activities. The schedule shall contain the contract IMP events and milestones, accomplishments, criteria, and activities from contract award to the completion of the contract. The contractor shall ensure schedule integration with its subcontractors and shall verify and ensure the validity of the subcontractors' schedule data, including demonstrating effective methods for incorporating schedule data from subcontractors into the contractor's IMS.

The contractor shall participate in the Integrated Baseline Review within 90 calendar days after Option 2 award. The contractor shall also participate in an IBR within 90 calendar days whenever a major task order modification has been awarded. The objective of the integrated baseline review is for the Government and the contractor to jointly assess areas, such as the Contractor's planning, to ensure complete coverage of the statement of work, logical scheduling of the work activities, resources, and identification of inherent risks.

4.3.1.3 Subcontract Management

The contractor shall update the Subcontract Management Plan for planning and oversight of the HSIN program subcontractors. The subcontract program manager will provide programmatic direction and oversight to the subcontractor.

4.3.1.4 Configuration Management

The contractor shall update the Configuration Management Plan (CMP). The contractor shall update the Data Management Plan. Configuration Management personnel will provide technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, audit and verify compliance with specified requirements.

4.3.1.5 Program Quality Assurance

The contractor shall update the Program Quality Plan to identify the appropriate quality assurance activities, methods, and tools for the HSIN NextGen program. The Quality Assurance personnel will perform the activities in accordance with the Program Quality Plan and QASP:

Attachment J-1

- Monitor program activities, as described in the QASP,
- Perform work product inspections, including review of deliverables,
- Audit activities and products against their documented processes, specifications, standards, and requirements,
- Witness tests,
- Monitor quality activities of subcontractors,
- Manage the quality of products received from suppliers,
- Ensure that corrective or preventive action taken to eliminate the causes of actual or potential non-conformities is appropriate for scope of the problem and the associated risks,
- Report the results of quality assurance activities, and
- Assist the Government in quality activity, upon request.

4.3.1.6 Program Reviews

The contractor shall conduct program reviews to assess program status. The contractor shall develop and deliver agendas prior to the conduct of customer program review meetings. Program reviews shall identify program risks and issues supporting course-correction planning. The contractor shall prepare minutes that detail the review.

4.3.1.7 Performance Measures

The contractor shall update and continue support performance measures collection and reporting.

4.3.2 HSIN NextGen O&M Support**4.3.2.1 Program Management**

The contractor shall operate and maintain HSIN NextGen, which includes the Common Operating Picture (COP) application and, services, tools and associated Oracle database. The O&M support shall provide:

- Personnel, equipment, and materials necessary to provide Help Desk Services [excluding GFE provided Help Desk tools: e.g. 866 help desk number, help desk email, Remedy Ticketing Solution and CISCO call centers with associated hardware] to include the associated hardware and software licenses, their currency and upgrades as required, and all other maintenance documentation and support agreements that will enable complete Operations & Maintenance (O&M) support at all levels.
- System Monitoring (on-site or remote capability utilizing an approved network performance monitoring tool).
- Capture system and mission performance metrics and provide reporting versus SLA
- Support development of, modification to, and execution of all O&M related SLA
- Support and maintenance of approved interfaces with other systems and subsystems
- Support to Configuration Management Process
- Preventative Maintenance on hardware, software per a defined schedule
- Corrective maintenance as required to include patch management
- System security vulnerability monitoring and proactive management of hardware and software security enhancements
- Support to Certification and Accreditation activities

Attachment J-1

- Development, test, and release of Engineering Change Requests (ECR)
- Over the phone training support for users and close interaction with Organization Change and Training Team to address user training needs
- Highly trained Surge Staffing (all tiers) in direct support of National Security Special Events and National Level Exercises or incidents that require a coordinated national response (i.e. Presidential elections, TOPOFF-5, Hurricanes etc.).

4.3.2.2 Help Desk Services

The contractor shall maintain a Help Desk providing 24x7x365 services to the HSIN NextGen user community. The contractor shall provide phone based level 1 support for customer requests for service, user training via phone communications, reports of incidents through a Help Desk responsible for end-to-end call and problems management. The contractor shall track and measure average speed to answer.

4.3.2.3 Tier 2 – System Administration

The contractor shall provide Tier 2 - System Administration staff to perform system monitoring, system and application maintenance, new site creation and site modifications and upgrades as captured within the Change Management automated processing tool and approved by the Change Control Board (CCB), problem detection and correction, and backup/recovery. The Tier 2 - System Administration staff will also be responsible for minor bug fixes and patches and conduct system security vulnerability scans.

4.3.2.4 Tier 3 – Infrastructure & Network Services

The contractor shall provide Tier 3 staff to install or integrate requested and approved hardware and software modifications, baseline Engineering Change Packages (ECP) and implement enhancements approved by the HSIN NextGen PMO and HSIN NextGen CCB, and test/implement major patches or fixes that may be required. The Tier 3 staff will also work directly with the Spiral 1, 2 and 4 IPT to assume responsibility for all system functional improvements once these improvements have been approved by DHS and moved to production. Tier 3 staff will also provide system security support to include enhancements, corrections and fixes to ensure the highest level of security across HSIN NextGen.

4.4 Option 3

This section is divided into the major activities of Option 3 year, including Program and Technical Management and Operations & Maintenance.

4.4.1 Program and Technical Management

This section provides the Option 3 year Program and Technical Management activities that support the technical objectives specified by the Statement Of Objectives.

4.4.1.1 Program Planning and Execution

The contractor shall perform program planning and management to support DHS objectives of the HSIN NextGen. The contractor shall update plans for Option 3 and incorporate lessons learned from completed Spirals. Plans to be updated include:

- Program Plan
- Integrated Master Plan
- Integrated Master Schedule
- Tailored Development Process

Attachment J-1

- Master Test and Evaluation Plan
- Software Development Plan
- Quality Assurance Surveillance Plan
- Service Level Agreements

4.4.1.2 Earned Value Management Systems (EVMS)

The contractor shall develop and submit monthly Earned Value reports addressing all applicable tasks under this task order as required by the overarching EAGLE contract, section H.32. The contractor shall submit four (4) hard copies of the required Cost Performance Report (CPR) Formats 1, 3, and 5 and the Contractor Funds Status Report ((CSFR) at the task order level) Earned Value reports to the COTR on a monthly basis by the 15th business day of each month. In addition, the contractor shall submit the Earned Value reports to the COTR via email. The soft copy Earned Value reports must be transmitted in Microsoft format.

The required Earned Value reports shall include the following:

- CPR Format 1 - WBS-oriented cost report: All costs incurred for the applicable tasks under this order shall be organized according to the WBS at a level to be directed by the COTR.
- CPR Format 3 - Baseline Report: This format shall provide information on the task order baseline and change tracking. The contractor shall report the following measures: Budgeted Cost of Work Scheduled (BCWS), Actual Cost of Work Performed (ACWP), Budgeted Cost of Work Performed (BCWP – Earned Value), cumulative Cost Performance Index (CPI), and cumulative Schedule Performance Index (SPI). Contractor shall also furnish the cumulative time-based Schedule Performance Index.
- CPR Format 5 - Problem Analysis Report/Variance Narrative: This report shall discuss and provide explanations for cost and schedule variances that have exceeded threshold. In addition, this report shall provide an explanation as to why the variance occurred and descriptions on how the contractor plans to resolve the cause of the variance. Contractor shall also furnish data monthly on the success for previous corrective actions taken.
- Contract Funds Status Report: This report shall address the current task order funding levels for all task order CLINs.

The Contractor shall use the information in these EVM reports to analyze the effectiveness of the EVMS and both the contract performance and the overall program progress. The Contractor shall take appropriate action based on those findings.

The contractor shall build an event-based Integrated Master Plan (IMP) for the HSIN and HSIN NextGen system that correlates to the Integrated Master Schedule (IMS), CWBS, Performance Work Statement (PWS), EVMS and the contractor's organizational structure. The contractor shall identify, based on the CWBS, a hierarchy of key program Events, Accomplishment, Criteria and supporting efforts that define the HSIN Program. Each program Event, Accomplishment and Criteria shall have specific entrance and exit criteria.

The contractor shall develop and maintain an Integrated Master Schedule (IMS) developed by logically networking detailed program activities. The schedule shall contain the contract IMP events and milestones, accomplishments, criteria, and activities from contract award to the completion of the contract. The contractor shall ensure schedule integration with its subcontractors and shall verify and ensure the validity of the subcontractors' schedule data,

Attachment J-1

including demonstrating effective methods for incorporating schedule data from subcontractors into the contractor's IMS.

The contractor shall participate in the Integrated Baseline Review within 90 calendar days after Option 3 award. The contractor shall also participate in an IBR within 90 calendar days whenever a major task order modification has been awarded. The objective of the integrated baseline review is for the Government and the contractor to jointly assess areas, such as the Contractor's planning, to ensure complete coverage of the statement of work, logical scheduling of the work activities, resources, and identification of inherent risks.

4.4.1.3 Subcontract Management

The contractor shall update the Subcontract Management Plan for planning and oversight of the HSIN program subcontractors. The subcontract program manager will provide programmatic direction and oversight to the subcontractor.

4.4.1.4 Configuration Management

The contractor shall update the Configuration Management Plan (CMP). The contractor shall update the Data Management Plan. Configuration Management personnel will provide technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, audit and verify compliance with specified requirements.

4.4.1.5 Program Quality Assurance

The contractor shall update the Program Quality Plan to identify the appropriate quality assurance activities, methods, and tools for the HSIN NextGen program. The Quality Assurance personnel will perform the activities in accordance with the Program Quality Plan and QASP:

- Monitor program activities, as described in the QASP,
- Perform work product inspections, including review of deliverables,
- Audit activities and products against their documented processes, specifications, standards, and requirements,
- Witness tests,
- Monitor quality activities of subcontractors,
- Manage the quality of products received from suppliers,
- Ensure that corrective or preventive action taken to eliminate the causes of actual or potential non-conformities is appropriate for scope of the problem and the associated risks,
- Report the results of quality assurance activities, and
- Assist the Government in quality activity, upon request.

4.4.1.6 Program Reviews

The contractor shall conduct program reviews to assess program status. The contractor shall develop and deliver agendas prior to the conduct of customer program review meetings. Program reviews shall identify program risks and issues supporting course-correction planning. The contractor shall prepare minutes that detail the review.

4.4.1.7 Performance Measures

The contractor shall update and continue support performance measures collection and reporting.

4.4.2 HSIN NextGen O&M Support

4.4.2.1 Program Management

The contractor shall operate and maintain HSIN NextGen, which includes the Common Operating Picture (COP) application and, services, tools and associated Oracle database. The O&M support shall provide:

- Personnel, equipment, and materials necessary to provide Help Desk Services [excluding GFE provided Help Desk tools: e.g. 866 help desk number, help desk email, Remedy Ticketing Solution and CISCO call centers with associated hardware] to include the associated hardware and software licenses, their currency and upgrades as required, and all other maintenance documentation and support agreements that will enable complete Operations & Maintenance (O&M) support at all levels
- System Monitoring (on-site or remote capability utilizing an approved network performance monitoring tool)
- Capture system and mission performance metrics and provide reporting versus SLA
- Support development of, modification to, and execution of all O&M related SLA
- Support and maintenance of approved interfaces with other systems and subsystems
- Support to Configuration Management Process
- Preventative Maintenance on hardware, software per a defined schedule
- Corrective maintenance as required to include patch management
- System security vulnerability monitoring and proactive management of hardware and software security enhancements
- Support to Certification and Accreditation activities
- Development, test, and release of Engineering Change Requests (ECR)
- Over the phone training support for users and close interaction with Organization Change and Training Team to address user training needs
- Highly trained Surge Staffing (all tiers) in direct support of National Security Special Events and National Level Exercises or incidents that require a coordinated national response (i.e. Presidential elections, TOPOFF-5, Hurricanes etc.).

4.4.2.2 Help Desk Services

The contractor shall maintain a Help Desk providing 24x7x365 services to the HSIN NextGen user community. The contractor shall provide phone based level 1 support for customer requests for service, user training via phone communications, reports of incidents through a Help Desk responsible for end-to-end call and problems management. The contractor shall track and measure average speed to answer.

4.4.2.3 Tier 2 – System Administration

The contractor shall provide Tier 2 - System Administration staff to perform system monitoring, system and application maintenance, new site creation and site modifications and upgrades as captured within the Change Management automated processing tool and approved by the Change

Control Board (CCB), problem detection and correction, and backup/recovery. The Tier 2 - System Administration staff will also be responsible for minor bug fixes and patches and conduct system security vulnerability scans.

4.4.2.4 Tier 3 – Infrastructure & Network Services

The contractor shall provide Tier 3 staff to install or integrate requested and approved hardware and software modifications, baseline Engineering Change Packages (ECP) and implement enhancements approved by the HSIN NextGen PMO and HSIN NextGen CCB, and test/implement major patches or fixes that may be required. The Tier 3 staff will also work directly with the Spiral 1, 2 and 4 IPT to assume responsibility for all system functional improvements once these improvements have been approved by DHS and moved to production. Tier 3 staff will also provide system security support to include enhancements, corrections and fixes to ensure the highest level of security across HSIN NextGen.

4.5 Option 4

This section is divided into the major activities of Option 4 year, including Program and Technical Management and Operations & Maintenance.

4.5.1 Program and Technical Management

This section provides the Option 4 year Program and Technical Management activities that support the technical objectives specified by the Statement Of Objectives.

4.5.1.1 Program Planning and Execution

The contractor shall perform program planning and management to support DHS objectives of the HSIN NextGen. The contractor shall update plans for Option 4 and incorporate lessons learned from completed Spirals. Plans to be updated include:

- Program Plan
- Integrated Master Plan
- Integrated Master Schedule
- Tailored Development Process
- Master Test and Evaluation Plan
- Software Development Plan
- Quality Assurance Surveillance Plan
- Service Level Agreements

4.5.1.2 Earned Value Management Systems (EVMS)

The contractor shall develop and submit monthly Earned Value reports addressing all applicable tasks under this task order as required by the overarching EAGLE contract, section H.32. The contractor shall submit four (4) hard copies of the required Cost Performance Report (CPR) Formats 1, 3, and 5 and the Contractor Funds Status Report ((CSFR) at the task order level) Earned Value reports to the COTR on a monthly basis by the 15th business day of each month. In addition, the contractor shall submit the Earned Value reports to the COTR via email. The soft copy Earned Value reports must be transmitted in Microsoft format.

The required Earned Value reports shall include the following:

- CPR Format 1 - WBS-oriented cost report: All costs incurred for the applicable tasks under this order shall be organized according to the WBS at a level to be directed by the COTR.

Attachment J-1

- **CPR Format 3 - Baseline Report:** This format shall provide information on the task order baseline and change tracking. The contractor shall report the following measures: Budgeted Cost of Work Scheduled (BCWS), Actual Cost of Work Performed (ACWP), Budgeted Cost of Work Performed (BCWP – Earned Value), cumulative Cost Performance Index (CPI), and cumulative Schedule Performance Index (SPI). Contractor shall also furnish the cumulative time-based Schedule Performance Index.
- **CPR Format 5 - Problem Analysis Report/Variance Narrative:** This report shall discuss and provide explanations for cost and schedule variances that have exceeded threshold. In addition, this report shall provide an explanation as to why the variance occurred and descriptions on how the contractor plans to resolve the cause of the variance. Contractor shall also furnish data monthly on the success for previous corrective actions taken.
- **Contract Funds Status Report:** This report shall address the current task order funding levels for all task order CLINs.

The Contractor shall use the information in these EVM reports to analyze the effectiveness of the EVMS and both the contract performance and the overall program progress. The Contractor shall take appropriate action based on those findings.

The contractor shall build an event-based Integrated Master Plan (IMP) for the HSIN and HSIN NextGen system that correlates to the Integrated Master Schedule (IMS), CWBS, Performance Work Statement (PWS), EVMS and the contractor's organizational structure. The contractor shall identify, based on the CWBS, a hierarchy of key program Events, Accomplishment, Criteria and supporting efforts that define the HSIN Program. Each program Event, Accomplishment and Criteria shall have specific entrance and exit criteria.

The contractor shall develop and maintain an Integrated Master Schedule (IMS) developed by logically networking detailed program activities. The schedule shall contain the contract IMP events and milestones, accomplishments, criteria, and activities from contract award to the completion of the contract. The contractor shall ensure schedule integration with its subcontractors and shall verify and ensure the validity of the subcontractors' schedule data, including demonstrating effective methods for incorporating schedule data from subcontractors into the contractor's IMS.

The contractor shall participate in the Integrated Baseline Review within 90 calendar days after Option 4 award. The contractor shall also participate in an IBR within 90 calendar days whenever a major task order modification has been awarded. The objective of the integrated baseline review is for the Government and the contractor to jointly assess areas, such as the Contractor's planning, to ensure complete coverage of the statement of work, logical scheduling of the work activities, resources, and identification of inherent risks.

4.5.1.3 Subcontract Management

The contractor shall update the Subcontract Management Plan for planning and oversight of the HSIN program subcontractors. The subcontract program manager will provide programmatic direction and oversight to the subcontractor.

4.5.1.4 Configuration Management

The contractor shall update the Configuration Management Plan (CMP). The contractor shall update the Data Management Plan. Configuration Management personnel will provide technical

and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, audit and verify compliance with specified requirements.

4.5.1.5 Program Quality Assurance

The contractor shall update the Program Quality Plan to identify the appropriate quality assurance activities, methods, and tools for the HSIN NextGen program. The Quality Assurance personnel will perform the activities in accordance with the Program Quality Plan and QASP:

- Monitor program activities, as described in the QASP,
- Perform work product inspections, including review of deliverables,
- Audit activities and products against their documented processes, specifications, standards, and requirements
- Witness tests,
- Monitor quality activities of subcontractors,
- Manage the quality of products received from suppliers,
- Ensure that corrective or preventive action taken to eliminate the causes of actual or potential non-conformities is appropriate for scope of the problem and the associated risks,
- Report the results of quality assurance activities, and

Assist the Government in quality activity, upon request.

4.5.1.6 Program Reviews

The contractor shall conduct program reviews to assess program status. The contractor shall develop and deliver agendas prior to the conduct of customer program review meetings. Program reviews shall identify program risks and issues supporting course-correction planning. The contractor shall prepare minutes that detail the review.

4.5.1.7 Performance Measures

The contractor shall update and continue support performance measures collection and reporting.

4.5.2 HSIN NextGen O&M Support

4.5.2.1 Program Management

The contractor shall operate and maintain HSIN NextGen, which includes the Common Operating Picture (COP) application and, services, tools and associated Oracle database. The O&M support shall provide:

- Personnel, equipment, and materials necessary to provide Help Desk Services [excluding GFE provided Help Desk tools: e.g. 866 help desk number, help desk email, Remedy Ticketing Solution and CISCO call centers with associated hardware] to include the associated hardware and software licenses, their currency and upgrades as required, and all other maintenance documentation and support agreements that will enable complete Operations & Maintenance (O&M) support at all levels.
- System Monitoring (on-site or remote capability utilizing an approved network performance monitoring tool).
- Capture system and mission performance metrics and provide reporting versus SLA

Attachment J-1

- Support development of, modification to, and execution of all O&M related SLA
- Support and maintenance of approved interfaces with other systems and subsystems
- Support to Configuration Management Process
- Preventative Maintenance on hardware, software per a defined schedule
- Corrective maintenance as required to include patch management
- System security vulnerability monitoring and proactive management of hardware and software security enhancements
- Support to Certification and Accreditation activities
- Development, test, and release of Engineering Change Requests (ECR)
- Over the phone training support for users and close interaction with Organization Change and Training Team to address user training needs
- Highly trained Surge Staffing (all tiers) in direct support of National Security Special Events and National Level Exercises or incidents that require a coordinated national response (i.e. Presidential elections, TOPOFF-5, Hurricanes etc.).

4.5.2.2 Help Desk Services

The contractor shall maintain a Help Desk providing 24x7x365 services to the HSIN NextGen user community. The contractor shall provide phone based level 1 support for customer requests for service, user training via phone communications, reports of incidents through a Help Desk responsible for end-to-end call and problems management. The contractor shall track and measure average speed to answer.

4.5.2.3 Tier 2 – System Administration

The contractor shall provide Tier 2 - System Administration staff to perform system monitoring, system and application maintenance, new site creation and site modifications and upgrades as captured within the Change Management automated processing tool and approved by the Change Control Board (CCB), problem detection and correction, and backup/recovery. The Tier 2 - System Administration staff will also be responsible for minor bug fixes and patches and conduct system security vulnerability scans.

4.5.2.4 Tier 3 – Infrastructure & Network Services

The contractor shall provide Tier 3 staff to install or integrate requested and approved hardware and software modifications, baseline Engineering Change Packages (ECP) and implement enhancements approved by the HSIN NextGen PMO and HSIN NextGen CCB, and test/implement major patches or fixes that may be required. The Tier 3 staff will also work directly with the Spiral 1, 2 and 4 IPT to assume responsibility for all system functional improvements once these improvements have been approved by DHS and moved to production. Tier 3 staff will also provide system security support to include enhancements, corrections and fixes to ensure the highest level of security across HSIN NextGen.

5.0 PERFORMANCE STANDARDS

Section 13 of this PWS contains the detailed performance standards associated with the activities defined as performance requirements in the previous section. In addition, Section 14 provides a cross reference from this document (PWS) to the Statement Of Objectives, Functional Requirements, and the Contract Work Breakdown Structure.

6.0 INCENTIVES

There are currently no defined incentives for this program.

7.0 DELIVERABLES AND DELIVERY SCHEDULE

The following table lists outputs from the performance identified in this document. Also identified is a reference to the PWS paragraph and the date of submission. The contractor shall provide electronic copies of each deliverable. Electronic copies shall be delivered via email attachment or other media by mutual agreement of the Government and Contractor. The electronic copies shall be compatible with MS Office 2003 or other applications as appropriate and mutually agreed to by the Government and Contractor. The contractor shall use best commercial practice for formatting deliverables under this contract. All of the Government's comments on deliverables shall be incorporated in the succeeding version or the contractor shall demonstrate to the Government's satisfaction why such comments should not be incorporated.

DELIVERABLE AND MILESTONE SCHEDULE			
CDRL	Title	PWS Reference	Date of Submission
0001	Spiral 1 – HSIN-CS	4.1.2	30 days after contract award
0002	Spiral 2 – HSIN NextGen Requirements 2.X IV&V Delivery	4.1.3	240 days after contract award (8 months)
0003	Spiral 2 – HSIN NextGen Requirements 2.X IOC	4.1.3	365 days after contract award (12 months)
0004	Spiral 3 – HSIN NextGen Requirements 2.X MOC	4.2.2	480 days after contract award (16 months)
0005	Spiral 4 – HSIN NextGen Requirements 3.X FOC	4.1.4, 4.2.3	540 days after contract award (18 months)
0006	Integrated Baseline Reviews (IBRs)	4.1.1.2, 4.2.1.2, 4.3.1.2, 4.4.1.2, 4.5.1.2	90 days after contract award
0007	Earned Value Reports	4.1.1.2, 4.2.1.2, 4.3.1.2, 4.4.1.2, 4.5.1.2	Monthly, after PMB established
0008	IT Security Plan	4.1.1.1.4	30 days after contract award
0009	IT Security Accreditation	4.1.1.1.4	180 days after contract award (6 months)
0010	Contractor Personnel – Background Investigation	11.0	30 days before the start date of the contract or 30 days prior to entry on duty
0011	Contractor Personnel – Terminations/Resignations	11.0	5 days after occurrence
0012	Program Plan	4.1.1.1.1	LAW IMS

Attachment J-1

DELIVERABLE AND MILESTONE SCHEDULE			
CDRL	Title	PWS Reference	Date of Submission
0013	Integrated Master Plan (IMP)	4.1.1.2, 4.2.1.2, 4.3.1.2, 4.4.1.2, 4.5.1.2	At IBR
0014	Integrated Master Schedule (IMS)	4.1.1.2, 4.2.1.2, 4.3.1.2, 4.4.1.2, 4.5.1.2	At IBR
0015	Subcontractor Management Plan	4.1.1.3, 4.2.1.3, 4.3.1.3, 4.4.1.3, 4.5.1.3	IAW IMS
0016	Configuration Management Plan	4.1.1.4, 4.2.1.4, 4.3.1.4, 4.4.1.4, 4.5.1.4	IAW IMS
0017	Program Quality Plan	4.1.1.5, 4.2.1.5, 4.3.1.5, 4.4.1.5, 4.5.1.5	IAW IMS
0018	Quality Assurance Surveillance Plan	4.1.1.1.7	IAW IMS, jointly developed with DHS input
0019	Master Test and Evaluation Plan	4.1.1.1.5	IAW IMS
0020	Software Development Plan	4.1.1.1.6	IAW IMS
0021	Transition Plan Draft	4.1.5.1	3 days after contract award
0022	Transition Plan Final	4.1.5.1	15 days after contract award
0023	Program Review Agenda, Contents, and Minutes	4.1.1.6, 4.2.1.6, 4.3.1.6, 4.4.1.6, 4.5.1.6	IAW IMS
0024	HSIN NextGen System Specification	4.1.3.2, 4.2.3.2	IAW IMS
0025	HSIN NextGen System Design Document	4.1.3.2, 4.2.3.2	IAW IMS
0026	HSIN NextGen Interface Requirement Specification	4.1.3.2, 4.2.3.2	IAW IMS
0027	HSIN NextGen Interface Design Document	4.1.3.3, 4.2.3.3	IAW IMS
0028	Technical Review Agenda, Contents, and Minutes	4.1.2.5, 4.1.3.2, 4.1.3.3, 4.1.3.5, 4.1.4.2, 4.2.3.3, 4.2.3.5	IAW IMS
0029	Installation Plans	4.1.2.7.1, 4.1.3.7.1, 4.2.3.7.1	IAW IMS
0030	Installation Drawings	4.1.2.7.1.2, 4.1.3.7.1.2, 4.2.3.7.1.2	IAW IMS
0031	Training Plan	4.1.2.6.2, 4.1.3.6.2, 4.1.4.6.2, 4.2.3.6.2	IAW IMS
0032	Training Materials	4.1.2.6.2, 4.1.3.6.2, 4.1.4.6.2, 4.2.2.2.1, 4.2.3.6.2	IAW IMS
0033	Organizational Change Communication Plan	4.1.2.6.1, 4.1.3.6.1, 4.1.4.6.1, 4.2.2.2.1, 4.2.3.6.1	IAW IMS
0034	Stakeholder Assessment Reports	4.1.2.6.1, 4.1.3.6.1, 4.1.4.6.1, 4.2.2.2.1, 4.2.3.6.1	IAW IMS

8.0 GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION

The DHS will provide, at no cost to the Contractor, when required and authorized by the contract:

- Workspace and furnishings at the designated DHS work sites for staff employees who are assigned by the contractor to the fulfillment of the HSIN contract;
- Government forms, publications and documents, except those offered for sale to the public;
- Access to computers, laptops, common-use software, data-access services, communications networks, and other resources owned or leased and operated by the DHS as appropriate for the completion of the Contractor's responsibilities;
- Required facility and network security access credentials and management of such credentials for use on DHS sites and networks;
- Help Desk tools, (e.g. 866 help desk number, help desk email, Remedy, Ticketing Solution and CISCO call centers with associated hardware)

9.0 PLACE OF PERFORMANCE

The primary place of performance for the HSIN NextGen task order contractor shall be at the contractor's Oakton Virginia facility, 10455 White Granite Drive, Suite 400. The Oakton facility is within fifty miles of the DHS Office of Operations Coordination (OPS) at the Nebraska Avenue Complex (NAC) in NW Washington DC. HSIN NextGen system build activities shall be conducted at the DHS Data Centers (to be determined) and HSIN NextGen testing tasks may require periods of travel to one or more of the DHS HSIN NextGen stakeholder offices located in the continental United States, United States territories, and internationally. The HSIN Next Generation System shall be physically hosted at no less than two geographically-separated DHS Data Centers, which include Government owned, Government operated, and contractor owned and contractor operated. The locations of these geographically separated data centers shall be at the sole discretion of DHS. Contractors will be provided the necessary physical and remote access.

9.1 Travel Requirements

The contractor shall comply with the guidance in FAR 31.205-46 using the regulations specified below:

- Federal Travel Regulations (FTR) - prescribed by the General Services Administration, for travel in the contiguous United States.
- Joint Travel Regulations (JTR), Volume 2, DoD Civilian Personnel, Appendix A. prescribed by the Department of Defense, for travel in Alaska, Hawaii, and outlying areas of the United States.
- Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas", prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

Prior to any long distance travel, the contractor shall prepare a Travel Authorization Request for Government review and COTR approval. The contractor shall use only the minimum number of

Attachment J-1

travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

Requests for travel approval shall contain:

- Date, time and points of departure
- Destination, time and dates of arrival
- Name of each contractor employee and position title
- Include a description of the travel proposed including a statement as to purpose
- Identify the Task Order number
- Identify the CLIN(s) associated with the travel
- Be submitted in advance of the travel with sufficient time to permit review and approval.

10.0 PERIOD OF PERFORMANCE

This PWS covers the task order's basic and four option performance periods. The task order's basic period of performance shall be from the effective date of the task order award through the task order month 12 (one year). Beyond the base period, there are four one-year option periods. Taken together with the base period and option periods, the task order term may last for a total period not to exceed five years. Periods of Task Order Performance to begin upon date of task order award.

Period of Performance	
Base Period	365 calendar days
Option Year 1	365 calendar days after Base period
Option Year 2	365 calendar days after Option period
Option Year 3	365 calendar days after Option period
Option Year 4	365 calendar days after Option period

11.0 SECURITY

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

The contractors shall comply DHS Management Directive (MD) 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information, MD 4300.1 Information Technology Systems Security, and the DHS Sensitive Systems Handbooks.

Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnect service agreements.

Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality,

Attachment J-1

integrity, and availability for the two networks. ISAs shall be signed by both DAAs or by the officials designated by the DAA.

Contractor employees (to include applicants, temporaries, part-time and replacement employees) requiring access to sensitive information, shall undergo a position sensitivity analysis based on the duties, outlined in the Position Designation Determination (PDD) for Contractor Personnel, each individual will perform on the contract. Prospective Contractor employees shall submit the required forms to OSI through the COTR no less than thirty (30) days before the start date of the contract or thirty (30) days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor.

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

When sensitive government information is processed on DHS telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed and adhere to the procedures governing such data as outlined in "DHS IT Security Program – Publication DHS MD 4300.Pub".

All Contractor employees using DHS automated systems or processing DHS sensitive data shall receive Security Awareness Training.

Contractors involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of DHS, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. Contractors with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

The Contractor shall ensure that requirements are allocated in the functional requirements and system design documents to security requirements are based on the DHS policy, NIST standards and applicable legislation and regulatory requirements.

The Contractor shall ensure that all aspects of data security requirements (i.e. confidentiality, integrity, and availability) are included in the functional requirements and system design, and ensure that they meet the minimum requirements as set forth in the DHS Sensitive Systems Handbook and policies and procedures.

The platform must be implemented in a data center that meets the DHS Extranet Security requirements as specified in the DHS 4300A.

12.0 QUALITY ASSURANCE SURVEILLANCE PLAN

The contractor will assist the Government in developing a Quality Assurance Surveillance Plan with measures defined in Section 13 of this document.

HOMELAND SECURITY INFORMATION NETWORK (HSIN)

FUNCTIONAL REQUIREMENTS DOCUMENT (FRD)

Version 5.0



Submitted:

11 March 2008

Developed for:

DHS/Office of Operations Coordination (OPS)

HSIN 2.X (Basis for Procurement – Must be hosted in 3.X Solution)

<i>HSIN 3.X (New Development)</i>

Table of Contents

1	INTRODUCTION	1
1.1	Purpose	1
1.1.1	Mission	1
1.1.2	Scope	1
1.1.3	Vision	2
1.1.4	HSIN Description	2
1.1.5	HSIN Functional Objectives	3
1.2	Project Description	3
1.3	Assumptions and Constraints	4
1.3.1	Assumptions	4
1.3.2	Constraints	4
1.4	Interfaces to External Systems	4
1.5	Points of Contact	5
1.6	Document References	5
1.6.1	Government Sources	5
1.6.2	Non-Government Sources	7
1.6.3	Statutes and Regulations	7
2	FUNCTIONAL REQUIREMENTS	9
2.1	Service-Oriented Architecture (SOA)	9
2.1.1	Service Discovery	10
2.1.2	Enterprise Service Management (ESM)	11
2.1.3	Machine-to-Machine (M2M) Messaging	11
2.1.4	Mediation	11
2.1.5	Content Discovery and Delivery (CDD)	12
2.2	Information Management	13
2.2.1	Content Management	13
2.2.1.1	Content Type	15
2.2.1.2	Search and Discovery	17
2.2.1.3	Personalization/Customization	17
2.2.1.4	Content Subscriptions	18
2.2.2	User Management	19
2.2.2.1	Role-Based Access and Role Definition	20
2.2.3	Access Management	20
2.3	Collaboration and Communication	21
2.3.1	Collaboration	21
2.3.1.1	Alerts, Notifications, and Announcements	22
2.3.1.2	User Community Directory	25
2.3.1.3	Instant Messaging (IM)	26
2.3.1.4	Discussion Boards	27
2.3.1.5	Feedback	28
2.3.1.6	Workflow Management	29
2.4	Situational Awareness	30
2.4.1	Visualization	30
2.4.1.1	Viewing Environment	30
2.4.1.2	Geospatial Information System (GIS) Mapping	31

3 NON-BUSINESS REQUIREMENTS 32

3.1 Security / Information Assurance..... 32

3.1.1 Identity Management – Authentication and Authorization..... 33

3.1.2 Password Management 34

3.1.3 Encryption..... 35

3.1.4 Audit Trail..... 35

3.1.5 Reporting 36

3.2 Infrastructure 37

3.2.1 Availability, Reliability, and Maintainability 38

3.2.1.1 Availability..... 38

3.2.1.2 Reliability..... 39

3.2.1.3 Maintainability 39

3.2.2 Survivability..... 39

3.2.3 Performance 40

3.2.4 Scalability 40

3.2.5 Data Retention 40

3.2.6 Usability..... 41

3.3 Interoperability / Integration 42

3.4 Regulations and Compliance..... 43

3.4.1 Legal Compliance..... 43

3.4.2 HSIN Third-Party Rule..... 44

3.4.3 Protection of Privacy and Proprietary Information..... 44

3.4.4 Accessibility..... 45

3.5 Quality Measurement and Monitoring 49

3.5.1 User and Usage Metrics 49

3.5.2 System Health Metrics..... 50

3.5.3 Content Metrics..... 50

4 REQUIREMENTS TRACEABILITY MATRIX..... 52

APPENDIX A: SOURCES 81

APPENDIX B: GLOSSARY..... 83

List of Tables

Table 1. Requirements Traceability Matrix..... 52

Table 32. Glossary of Terms 83

List of Figures

Figure 1. HSIN Next Generation System Requirements Structure..... 2

Figure 2. HSIN Next Generation System Context Diagram..... 5

Figure 3. HSIN Next Generation Information Sharing Overview 10

1 INTRODUCTION

3 1.1 Purpose

4 The purpose of this Functional Requirements Document (FRD) is to define and outline the known
5 services and functional requirements for the next generation Homeland Security Information Network
6 (HSIN). The update enhances the current HSIN implementation.

7
8 Information presented with an italic typeface in a bulleted list represents functionality (or a non-business
9 requirement) that is completely new to HSIN. Information that is non-italicized in a bulleted list
10 represents existing functionality of the HSIN system. Appendix A provides a list of acronyms used in this
11 FRD. Appendix B identifies additional sources which may be of use when reviewing this document.
12 Appendix C presents a glossary of many of the key terms used in this document. Some acronyms will be
13 found spelled out as a footnote, rather than the original text. This was done on a limited basis to preserve
14 the formal citation of a document.

16 1.1.1 Mission

17 The mission of the HSIN Next Generation System is to provide a secure and trusted national platform for
18 information sharing and collaboration between Federal, State, Local, Tribal, Territorial, Private Sector
19 and International partners engaged in preventing, protecting from, responding to and recovering from all
20 threats, hazards and incidents within the authority of the Department of Homeland Security (DHS).
21

22 1.1.2 Scope

23 The HSIN Next Generation System is a national sharing and collaboration platform that provides and/or
24 serves as a conduit to Sensitive but Unclassified (SBU) data and analysis regarding people, places, things,
25 events, resources and activities lawfully owned, maintained by and shared in a multi-directional, trusted
26 and secure environment. DHS and other domestic and international users, who are in mission partnership
27 with DHS for the purpose of supporting missions to prevent, protect from, respond to and recover from all
28 threats, hazards and incidents included within the official scope of DHS authority.

29
30 HSIN Next Generation development includes the design, development, integration and test, and
31 implementation of a multi-level secure Open Architecture system. Figure 1 provides a pictorial view of
32 the structure of this FRD.
33

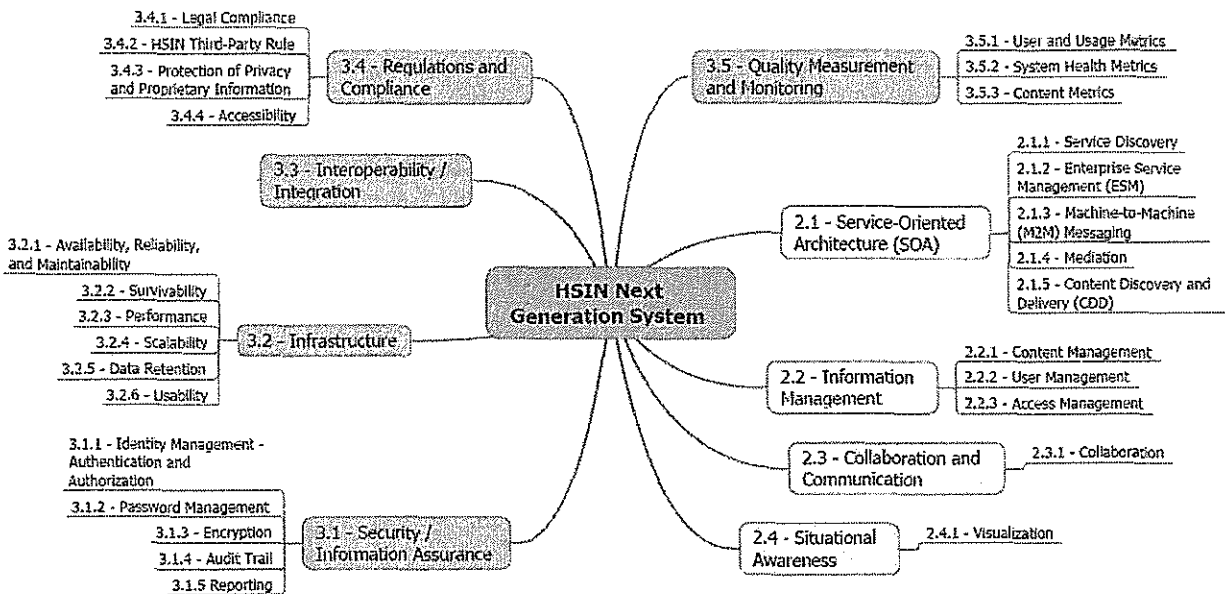


Figure 1. HSIN Next Generation System Requirements Structure

1.1.3 Vision

The vision of the DHS Office of Operations Coordination (OPS) Chief Information Officer (CIO) is for HSIN Next Generation to be the Homeland Security community's information sharing tool of choice for protecting, preventing, responding to, and recovering from terrorist attacks and natural and man-made disasters.

In its end state, the HSIN Next Generation System is envisioned to provide to members of the Homeland Security Community relevant and actionable information that will support them in executing their responsibilities across the entire spectrum of Homeland Security operations. More specifically, the goal is "to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system" as stated by Homeland Security Presidential Directive (HSPD) 5 (referenced as "HSPD-5" hereafter).

1.1.4 HSIN Description

The current HSIN is a primary communication and collaboration system that supports the unified effort to prevent and deter terrorist attacks, and prepare for and respond to any natural or man-made disaster. The HSIN system provides a means to plan, coordinate, collaborate, execute, report, analyze, and promote situational awareness. HSIN acquisition objectives are outlined in the HSIN Program Wide Acquisition Plan (AP) include:

- Providing a common, interoperable information technology (IT) architecture for gathering, fusing, analyzing, and reporting all threats, all hazards information to the U.S. Homeland.
- Hosting the DHS National Operations Center (NOC) to provide leaders and stakeholders with timely, accurate, relevant, and highly integrated all-source information to enhance operational situational awareness and actionable decision making.

63 HSIN supports DHS executions under the Homeland Security Act (HSA) of 2002, HSPD-5, DHS
64 Strategic Plan, and DHS Objectives.
65

66 **1.1.5 HSIN Functional Objectives**

67 The primary HSIN functional objectives are as follows:
68

- 69 • Establish a robust national information sharing and collaboration system in support of the
70 counter terrorism and emergency response missions, ensuring timely and reliable access to and
71 use of information.
- 72 • Provide key leadership, planners and community stakeholders at all levels of government
73 with the best possible information and situation awareness for planning, coordinating, and
74 conducting operations related to the prevention of crises, and responding to, mitigating, and
75 recovering from the effects of crises.
- 76 • Provide a system with a secure, integrated architecture that is cross-platform with all Federal,
77 State, Local, Tribal, Territorial, Private Sector and International partners.
- 78 • Provide authorized access to data stores, shared services (i.e. federated searches), near real-
79 time collaboration, accessible information, systematic information gathering, and dissemination.
- 80 • Provide a standards-based architecture to enable the private sector to interact and share
81 information on critical infrastructure and key resources with government organizations.
82

83 **1.2 Project Description**

84 DHS OPS enables strategic decision-making and operations through National-level contingency planning
85 and incident coordination, situational awareness and operational assessments, and information sharing
86 and subject matter expertise. By taking these actions, OPS enhances mission effectiveness and unity of
87 effort for all threats/all-hazards Homeland Security operations.
88

89 OPS CIO is currently managing the development, implementation, and program execution of two major
90 investments, HSIN and DHS NOC Common Operational Picture (COP), both of which are used in the
91 DHS OPS NOC.
92

93 HSIN provides a common, interoperable IT architecture for gathering, fusing, analyzing, and reporting
94 information and threats to the U.S. Homeland. This is achieved by ensuring timely and accurate
95 dissemination of relevant information to Homeland Security stakeholders.
96

97 HSIN is currently connecting Community of Interest (COI) members from law enforcement agencies,
98 emergency management and first responder agencies, intelligence agencies, private sector infrastructure
99 stakeholders, DHS component organizations, and international partners. Access rights to the system will
100 be determined by the user's COI-vetted classification, as well as their role-based privileges for services
101 and content. HSIN Next Generation will continue to increase functionality, access levels and
102 infrastructure, increasing community and user trust, utility and utilization.
103

104 The HSIN Next Generation System will improve sharing of timely, validated, protected, and actionable
105 all threats/all-hazards information. The HSIN Next Generation System will promote more rapid and
106 effective interchange and coordination among the DHS enterprise and Federal, State, Local, Tribal,
107 Territorial, Private Sector and International partners, thus ensuring effective multi-directional sharing of
108 information, as described below.

109

110 **1.3 Assumptions and Constraints**

111 **1.3.1 Assumptions**

- 112 • The HSIN Next Generation System will draw upon the existing HSIN system and
113 capabilities, rather than be a complete infrastructure replacement.
- 114 • The solution that meets these requirements will be a combination of Government Off-the-
115 Shelf (GOTS) and Commercial Off-the-Shelf (COTS) hardware, firmware, and software
116 components.
- 117 • The HSIN Next Generation System must be resilient and adaptable as threats change,
118 technologies evolve and information needs shift.
119

120 **1.3.2 Constraints**

- 121 • The HSIN Next Generation System must incorporate *all* of the existing functionality of the
122 HSIN 2.x system (as denoted in Table 1, the Requirements Traceability Matrix, beginning on
123 page 52), in addition to the completely new functionality for the 3.x system as defined herein.
- 124 • The HSIN Next Generation System implementation must require no installation of any client-
125 side software.
- 126 • The HSIN Next Generation System implementation must be entirely web browser-based.
- 127 • Users accessing HSIN, except users accessing HSIN via the Internet, must use OneNET,
128 unless a waiver is obtained from the DHS CIO.
- 129 • The HSIN Next Generation System must provide load balancing between production sites
130 and application servers.
- 131 • The HSIN Next Generation System must support a data replication/data mirroring capability
132 to enable concurrency of information between the production sites.
- 133 • The HSIN Next Generation System must comply with all DHS policies, legalities, and
134 standards as described herein.
- 135 • The HSIN Next Generation System does not include building an email system.
- 136 • The HSIN Next Generation program does not have any control of the user operating
137 environment.
138

139 **1.4 Interfaces to External Systems**

140 The HSIN Next Generation System context diagram (see Figure 2 on page 5) provides a visual depiction
141 of the system, its external interfaces, and its users. System interfaces will be compliant with the
142 Information Sharing Environment (ISE) Implementation Plan. There will be a variety of usage
143 agreements that may be required. These may be in the form of End-User License Agreements (EULAs),
144 which will become more critical as looser coupling occurs via the Service-Oriented Architecture (SOA)
145 structure, or a more formal Interface Security Agreement (ISA) with attendant Service Level Agreement
146 (SLA).
147

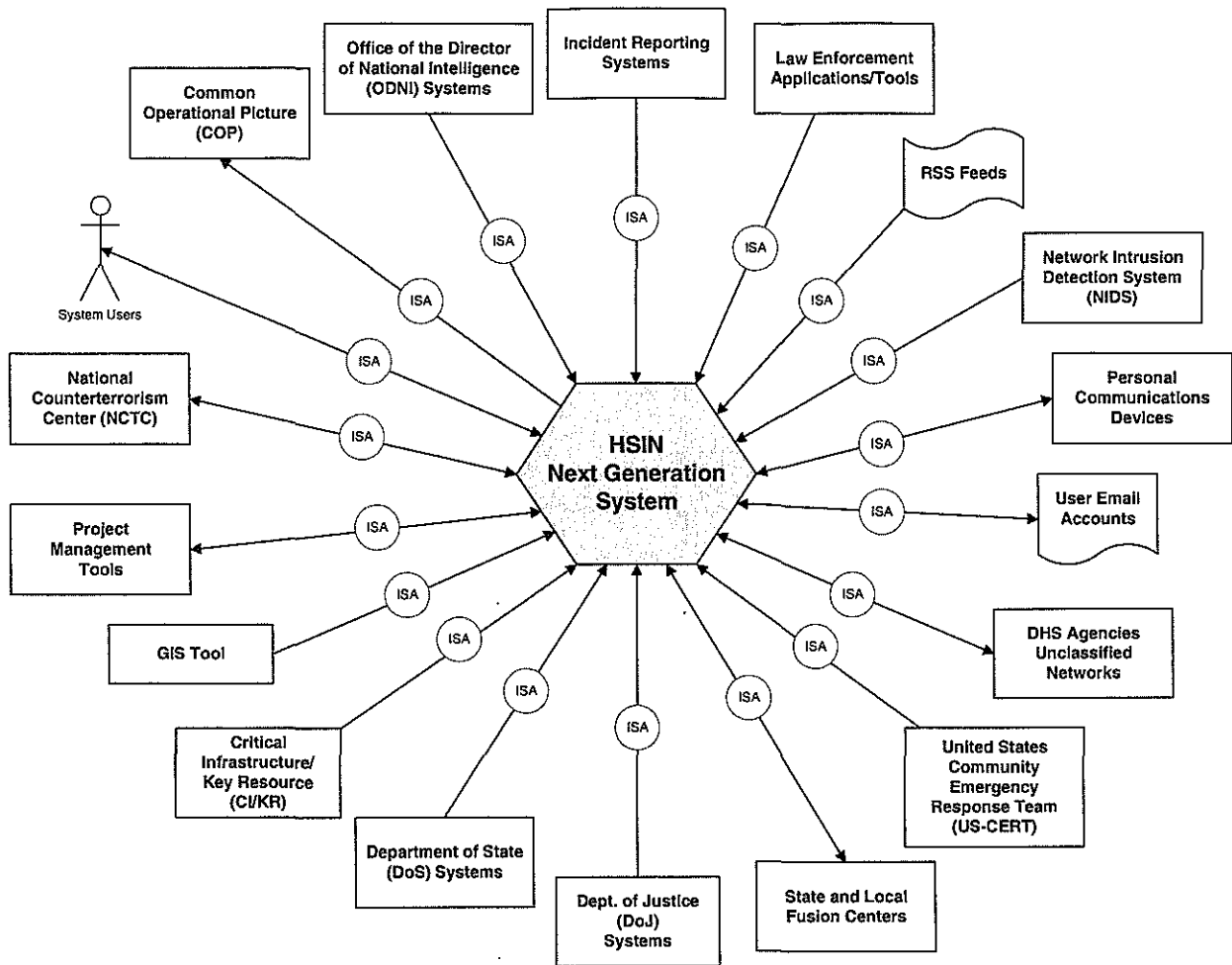


Figure 2. HSIN Next Generation System Context Diagram

148

149

150

1.5 Points of Contact

152

1.6 Document References

154 The reference materials used in the preparation of this document are as cited in subsections 1.6.1 through
155 1.6.3 below.

156

1.6.1 Government Sources

158 Executive Office of the President of the United States, Office of Management and Budget (OMB),
159 OMB Circular A-11, *Preparation and Submission of Budget Estimates*, 3 July 2001

160 Program Manager, Information Sharing Environment (PM-ISE), *Information Sharing Environment*
161 *Implementation Plan*, November 2006

162 U.S. Department of Commerce, Technology Administration, National Institute of Standards and
163 Technology (NIST), Information Technology Library (ITL), Federal Information Processing

- 164 Standards Publication 140-2 (FIPS PUB 140-2), *Security Requirements for Cryptographic*
165 *Modules*, 25 May 2001 (supersedes FIPS PUB 140-1, 11 January 1994)
- 166 U.S. Department of Commerce, Technology Administration, NIST, Information Technology Library
167 (ITL), FIPS PUB 197, *Advanced Encryption Standard (AES)*, 26 November 2001
- 168 U.S. Department of Commerce, Technology Administration, NIST, ITL, FIPS PUB 199, *Standards*
169 *for Security Categorization of Federal Information and Information Systems*, February 2004
- 170 U.S. Department of Commerce, Technology Administration, NIST, ITL, FIPS PUB 201, *Personal*
171 *Identity Verification (PIV) of Federal Employees and Contractors*, March 2006
- 172 U.S. Department of Commerce, Technology Administration, NIST, NIST Special Publication 800-53,
173 *Recommended Security Controls for Federal Information Systems*, February 2005
- 174 U.S. Department of Commerce, Technology Administration, NIST, NIST Special Publication 800-60,
175 *Guide for Mapping Types of Information and Information Systems to Security Categories*,
176 Version 2.0, June 2004
- 177 U.S. Department of Defense, 5015.2-STD,¹*Electronic Records Management Software Applications*
178 *Design Criteria Standard*, 25 April 2007
- 179 U.S. Department of Defense, Directive 5240.1, *DoD Intelligence Activities*, 25 April 1988
- 180 U.S. Department of Homeland Security, *DHS Portal Standards*, Draft 16 December 2007
- 181 U.S. Department of Homeland Security, *DHS Service Oriented Architecture – Technical Framework*,
182 12 February 2007
- 183 U.S. Department of Homeland Security, Homeland Security Operations Center (HSOC), *Operational*
184 *Requirements Document for the Homeland Security Information Network*, Draft Version 0.9, 21
185 August 2007
- 186 U.S. Department of Homeland Security, HSOC, *Homeland Security Information Network, Baseline 2*
187 *System Requirements Specification*, Version 1.0, 1 February 2006
- 188 U.S. Department of Homeland Security, Information Technology Security Program Publication, *DHS*
189 *4300B, National Security Systems Handbook*, Version 4.3, 30 September 2007
- 190 U.S. Department of Homeland Security, Information Technology Security Program Publication, *DHS*
191 *Sensitive Systems Policy Directive 4300A*, Version 5.5, 30 September 2007
- 192 U.S. Department of Homeland Security, Information Technology Security Program Publication,
193 *Secure Baseline Configuration Guidelines*, 31 May 2007
- 194 U.S. Department of Homeland Security, Management Directive System, *Privacy Act Compliance*,
195 MD 0470.1, 27 January 2003
- 196 U.S. Department of Homeland Security, Management Directive System, *Safeguarding Sensitive But*
197 *Unclassified (For Official Use Only) Information*, MD 11042.1, 6 January 2005
- 198 U.S. Department of Homeland Security, Management Directive System, *Section 508 Program*
199 *Management Office & Electronic and Information Technology Accessibility*, MD 4010.2, 26
200 October 2005 (establishes policy regarding Electronic and Information Technology accessibility
201 for DHS employees and customers with disabilities)
- 202 U.S. Department of Homeland Security, Office of Operations Coordination, *Assessment of the Policy*
203 *and Strategy Framework for the HSIN*, 25 October 2006

¹ “STD” stands for “Standard.”

204 U.S. Department of Homeland Security, Office of the Chief Information Officer (OCIO), *Homeland*
205 *Security Enterprise Architecture (HLS EA) – Target Enterprise*, February 2007

206 U.S. Department of Homeland Security, Operations Directorate National Operations Center, *Privacy*
207 *Impact Assessment for the Homeland Security Information Network (HSIN) Communities of*
208 *Interest (COIs)*, 22 June 2007
209

210 **1.6.2 Non-Government Sources**

211 International Organization for Standardization, International Standard ISO 15489-1, *Information and*
212 *Documentation, Records Management, Part 1: General*, September 2001

213 International Organization for Standardization, International Standard ISO 15489-2, *Information and*
214 *Documentation, Records Management, Part 2: Guidelines*, October 2001

215 International Organization for Standardization, International Standard 23950, *Information and*
216 *Documentation, Information Retrieval (Z39.50), Application Service Definition and Protocol*
217 *Specification*, 1998 (this standard defines a client/server protocol for searching and retrieving
218 information from remote computer databases; its provisions are also covered by ANSI/NISO
219 Z39.50, 2003)²

220 Java Community Process, JSR-000168,³ *Portlet Specification, Version 1.0*, 27 October 2003 (defines
221 a set of Application Programming Interfaces [APIs] for portal computing addressing the areas of
222 aggregation, personalization, presentation, and security for enabling interoperability between
223 portlets and portals)

224 Java Community Process, JSR-170/283, *Content Repository API for Java (JCR)*, Version 1 was
225 issued as JSR-170 on 24 April 2006; Version 2 was issued as JSR-283 on 10 September 2007
226 (JSR-170/283 is a specification defining a Java platform API for accessing content repositories in
227 a uniform manner)

228 OASIS Technical Committee, OpenDocument Format (ODF) International Organization for
229 Standardization/International Electrotechnical Commission (ISO/IEC) 26300, *OASIS Open*
230 *Document Format for Office Applications (OpenDocument)*, OpenDocument Version 1.0 was
231 approved 3 May 3 2006; Version 1.1 was approved 19 October 2006; Version 1.2 was expected
232 by October 2007 (defines file formats for electronic office documents such as spreadsheets,
233 charts, presentations, and word processing documents)

234 Open GIS⁴ Consortium Inc., OpenGIS Project Document OGC 03-008r2, *Web Notification Service*,
235 Version 0.1.0, 21 April 2003

236 Universal Description Discovery and Integration (UDDI) Specification Technical Committee, *UDDI*
237 *Specification Committee Draft, Version 3.0.2*, 19 October 2004 (describes the Web services, data
238 structures, and behaviors of all instances of a UDDI registry)
239

240 **1.6.3 Statutes and Regulations**

241 5 United States Code (U.S.C). 552a, *The Privacy Act of 1974*, as amended (regarding records
242 maintained on individuals)

243 5 U.S.C. 552b, *The Freedom of Information Act*, 4 July 1966, as amended in 2002 (regarding public
244 information such as agency rules, opinions, orders, records, and proceedings)

² “ANSI/NISO” stands for “American National Standards Institute/National Information Standards Organization.”

³ “JSR” stands for “Java Specification Request.”

⁴ “GIS” stands for “Geodata Interoperability Specification.”

- 245 Public Law 105-220, *Workforce Investment Act of 1998*, 7 August 1998 (consolidates, coordinates,
246 and improves employment, training, literacy, and vocational rehabilitation programs in the United
247 States)
- 248 National Archives and Records Administration, Office of the Federal Register, Code of Federal
249 Regulations (CFR) Title 28 Part 23, *Criminal Intelligence Systems Operating Policies*
- 250 Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act
251 of 1998 (P.L. 105-220)⁵, *Electronic and Information Technology Accessibility Requirements for*
252 *Federal Departments and Agencies*, 7 August 1998
- 253 The White House, Executive Order 12333, *United States Intelligence Activities*, 4 December 1981
254 (amended by Executive Order 13355)
- 255 The White House, Executive Order 13355, *Strengthened Management of the Intelligence Community*,
256 27 August 2004
- 257 The White House, Office of the Press Secretary, Homeland Security Presidential Directive 5
258 (HSPD-5), *Management of Domestic Incidents*, 28 February 2003
- 259 The White House, Office of the Press Secretary, Homeland Security Presidential Directive 12
260 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and*
261 *Contractors*, 27 August 2004
262

⁵ "P.L." stands for "Public Law."

263 2 FUNCTIONAL REQUIREMENTS

264

265 2.1 Service-Oriented Architecture (SOA)

266 The HSIN Next Generation System will promote interoperability between DHS enterprise and Federal,
267 State, Local, Tribal, Territorial, Private Sector and International partners through an SOA. The HSIN
268 Next Generation SOA objective is intended to define a set of capabilities that can be satisfied with
269 commercially available products, open standards and include the following enterprise core services:
270 Enterprise Service Management (ESM), Content Discovery and Delivery (CDD), Machine-to-Machine
271 (M2M) Messaging, and Service Discovery.

272

273 The HSIN Next Generation SOA framework will provide the infrastructure required to support the
274 development of web services to promote the sharing of data that is of value to organizations supporting
275 the mission of securing the homeland. The HSIN Next Generation SOA framework includes the Core
276 Enterprise Services described above, but will also incorporate provisioning of services to support and
277 encourage the development and use of services for use with external system communication.

278

279 The HSIN Next Generation System architecture will require an open system approach, which employs
280 modular design tenets, uses widely supported and consensus based standards for its key interfaces and is
281 subject to independent validation and verification (IV&V) tests to ensure the openness of its key
282 interfaces.

283

284 The Operational View 1 (OV-1) diagram (refer to Figure 3 on page 10) illustrates the HSIN Next
285 Generation operating environment. HSIN Next Generation facilitates information sharing among Federal,
286 State, Local, Tribal, Territorial, Private Sector and International partners by providing a wide range of
287 services for each to use in accomplishing their respective missions. Additionally, HSIN capabilities will
288 be extended to federated users who are authorized users of other networks, but whose credentials will be
289 accepted for access to HSIN information. The following definitions are used to clarify the types of users
290 and services.

291

292 • **Core HSIN Next Generation System Users:** These are users whose accounts are maintained
293 by the HSIN Next Generation System.

294 • **Federated Users:** These are users whose accounts are maintained elsewhere, but whose
295 credentials are recognized and honored by the HSIN Next Generation System's security/access
296 policy.

297 • **HSIN Next Generation System Services:** Services available to all HSIN users through the
298 HSIN Next Generation System.
299

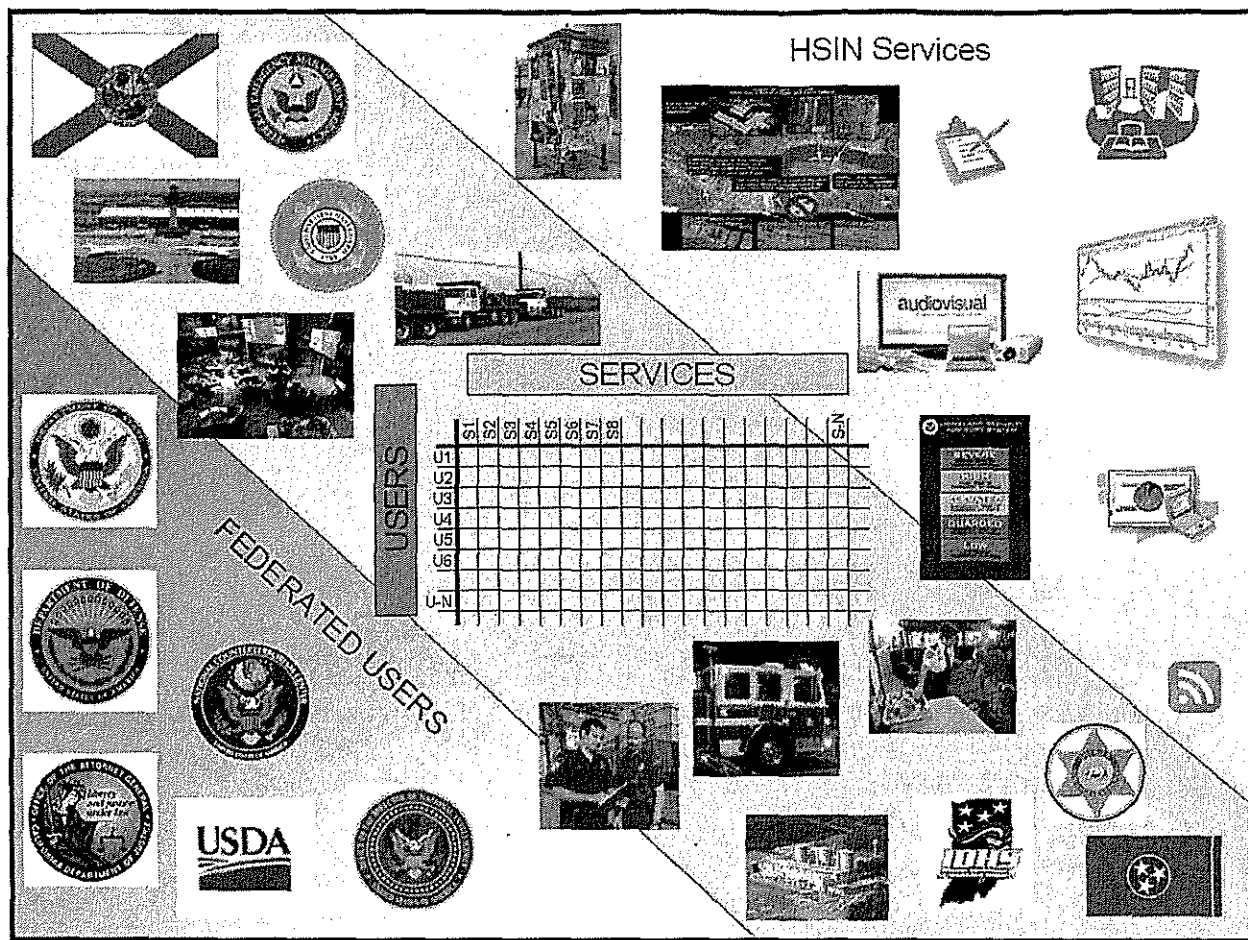


Figure 3. HSIN Next Generation Information Sharing Overview

The SOA requirements for the HSIN Next Generation System are listed below:

- The HSIN Next Generation System shall use SOA to assure the interoperability of collaborative systems and the ability to seamlessly share data.
- The HSIN Next Generation System shall comply with the DHS SOA Framework as outlined in, DHS Service Oriented Architecture – Technical Framework, 12 February 2007.
- The HSIN Next Generation System shall comply with the Service Discovery Standards of the DHS Enterprise Portal Standards List, including Simple Object Access Protocol (SOAP).
- The HSIN Next Generation System shall comply with the Information Sharing Environment Implementation Plan, November 2006.

2.1.1 Service Discovery

A key component of the HSIN Next Generation System SOA framework will be a searchable repository of services that provides an asset management capability for services within DHS and supports the full life-cycle of services and service artifacts. Service Discovery allows service providers to publish/advertise service specifications, metadata, and service accessibility to the entire community. Service Discovery also allows service consumers to discover information as advertised by providers.

- 320
321 The service discovery requirements for the HSIN Next Generation System are listed below:
322
323
 - 324 • *The HSIN Next Generation System shall be able to discover, identify and use services that are external to HSIN Next Generation System.*
 - 325 • *The HSIN Next Generation System SOA framework shall incorporate a searchable repository of services that provides an asset management capability for services within DHS.*
 - 326 • *The HSIN Next Generation System shall conform to the UDDI V3.0.2 standard, including Service Discovery specification for support of the SOA framework.*
 - 327 • *The HSIN Next Generation System shall comply with the Service Discovery Standards of the DHS Enterprise Portal Standards List, including UDDI.*

328
329
330
331

332 **2.1.2 Enterprise Service Management (ESM)**

333 The ESM capability collects information to support monitoring and management of all web services
334 within the HSIN Next Generation system. To accomplish this objective, the ESM capability provides the
335 ability to measure Service Level Metrics with an SLA, is aware of the situational status of services, and
336 provides service status information to external consumers such as the DHS Infrastructure Services
337 Management Center.

338
339 The ESM requirements for the HSIN Next Generation System are listed below:
340

- 341
 - 342 • *The HSIN Next Generation System ESM capability shall collect information to support monitoring and management of web services within the HSIN Next Generation System.*
 - 343 • *The HSIN Next Generation System ESM capability within the HSIN Next Generation System shall interface with the DHS infrastructure toolset.*

344
345

346 **2.1.3 Machine-to-Machine (M2M) Messaging**

347 The use of M2M Messaging will provide the HSIN Next Generation System with the infrastructure to
348 establish and sustain a reliable bridge between multiple organizations for the interoperable sharing of
349 data.

350
351 The M2M Messaging requirements for the HSIN Next Generation System are listed below:
352

- 353
 - 354 • *The HSIN Next Generation System Machine-to-Machine Messaging capability shall allow DHS software applications to interoperate in order to perform synchronous and asynchronous messaging.*
 - 355 • *The HSIN Next Generation System Machine-to-Machine Messaging capability shall allow other agency's software applications to interoperate in order to perform synchronous and asynchronous messaging.*

356
357
358
359

360 **2.1.4 Mediation**

361 The HSIN Next Generation System Mediation capability provides the infrastructure to integrate data
362 providers seamlessly with data consumers and other data providers. The focus of this integration is to
363 provide the capability to translate schemas and orchestrate interactions between web services into a

364 workflow supporting HSIN stakeholder missions. This capability will provide DHS with the
365 infrastructure to translate messages that allows the sharing of data between multiple organizations.
366

367 The mediation requirements for the HSIN Next Generation System are listed below:
368

- 369 • *The HSIN Next Generation System Mediation capability shall support data format*
370 *transformations in compliance with the National Information Exchange Model (NIEM).*
- 371 • *The HSIN Next Generation System Mediation capability shall support rules-based data*
372 *routing.*
- 373 • *The HSIN Next Generation System Mediation capability shall support orchestration of web*
374 *services.*
375

376 **2.1.5 Content Discovery and Delivery (CDD)**

377 The HSIN Next Generation System CDD capability will provide a fast response method of information
378 transport. This CDD capability facilitates the movement of content around the enterprise for rapid access,
379 enterprise federated alerts and transactional messaging capabilities. This system capability will also
380 incorporate enterprise subscription and publishing capabilities and mediation-enabling services to
381 facilitate disaster recovery efforts.
382

383 This CDD capability may include, but is not limited to, the establishment of publish/subscribe channels in
384 which users receive content published over a predefined channel. It may also encompass the capability to
385 provide a distributed content cache (i.e., the capability for transparent pull of content from regional
386 locations during user requests to support responsiveness). The CDD provides Content Staging data
387 replication and forward staging solutions into the HSIN Next Generation System. This functionality
388 supports responsiveness and provides guaranteed reliable delivery in accordance with assigned handling
389 instructions, configurable bandwidth use, and transfer scheduling.
390

391 The CDD requirements for the HSIN Next Generation System are listed below:
392

- 393 • The HSIN Next Generation System shall incorporate a CDD capability.
- 394 • The HSIN Next Generation System shall provide for performing federated searches for
395 enterprise content across federated search-enabled SBU data sources.
- 396 • The HSIN Next Generation System shall provide for indexing the search-enabled enterprise
397 content.
- 398 • *The HSIN Next Generation System shall provide for searching other federated content*
399 *repositories across SBU classifications.*
- 400 • *The HSIN Next Generation System shall provide for automatically indexing external content.*
- 401 • *The HSIN Next Generation System shall provide for establishing catalogs of tagged*
402 *information.*
- 403 • *The HSIN Next Generation System shall provide for searching these established catalogs of*
404 *tagged information.*
- 405 • *The HSIN Next Generation System shall provide for migrating COI-specific data sources to*
406 *support federated search, saving for reuse, archiving, and de-confliction.*

- 407 • *The HSIN Next Generation System shall be able to discover, identify and use content that is*
408 *resident external to HSIN Next Generation System.*
409

410 **2.2 Information Management**

411 **2.2.1 Content Management**

412 A primary function of the HSIN Next Generation System is to serve as a central point of information
413 sharing and collaboration across agencies and components within and outside of the federal government.
414 The ability to create, protect, and manage content is of utmost importance. Content Management is the
415 collection and dissemination of either raw or processed data for the operational use of COI members and
416 for use by the various analytical COIs.

417
418 In support of critical situations and emergencies that would require high-volume information processing
419 the HSIN Next Generation System's content management capabilities must support bulk content
420 management operations such as upload and download. Integrated content metadata extraction is needed
421 to ease content organization within the HSIN Next Generation System environment for all content
422 operation transactions, and bulk content operation transactions.

423
424 The general content management requirements for the HSIN Next Generation System are listed below:

- 425
- 426 • The HSIN Next Generation System shall provide capabilities to allow information gathered at
427 the all levels to be processed, analyzed, disseminated, and integrated with information gathered at
428 the all other levels.
 - 429 • The HSIN Next Generation System shall provide a content management system that allows
430 the user to create, update, publish, translate, archive and retrieve accessible content.
 - 431 • The HSIN Next Generation System shall provide multiple logical repositories such that user
432 access can be restricted to an individual Agency/Unit repository.
 - 433 • *The HSIN Next Generation System shall provide the user with the ability to distinguish new*
434 *data, changed data, and unchanged data. (For example, the system will distinguish changed*
435 *content within a file, document, or other content piece).*
 - 436 • *The HSIN Next Generation System shall provide visual indications of changed or new*
437 *content.*
 - 438 • *The HSIN Next Generation System shall support the logical storage of and ability to easily*
439 *visually distinguish content that is hierarchically (parent-child) related.*
 - 440 • *The HSIN Next Generation System shall allow users to create and remove content folders as*
441 *needed for content organization.*
 - 442 • *The HSIN Next Generation System shall be capable of accessing content which is stored in*
443 *external repositories or systems.*
 - 444 • *The HSIN Next Generation System shall allow the user to "tag" content for access.*
 - 445 • *The HSIN Next Generation System shall display content based on user privilege.*
 - 446 • *The HSIN Next Generation System shall allow end-user to be able to redact or sanitize data*
447 *for public use and distribute to all communities that need the data.*

- 448 • The HSIN Next Generation System shall provide the capability to remove content from view
449 or access.
- 450 • *The HSIN Next Generation System shall provide the author/data provider with the ability to*
451 *set content validity time.*
- 452 • *The HSIN Next Generation System shall maintain a record of retention schedules and*
453 *removal schedules.*
- 454 • The HSIN Next Generation System shall provide check-in/check-out control for each piece of
455 content stored in the content repository, for controlled information provisioning.
- 456 • The HSIN Next Generation System shall provide version management capabilities to keep
457 track of different versions of the same information with their revisions and renditions.
- 458 • *The HSIN Next Generation System shall provide “dynamic linking” capabilities to maintain*
459 *link integrity.*
- 460 • *The HSIN Next Generation System shall provide “dynamic linking” capabilities to identify*
461 *inactive links.*
- 462 • The HSIN Next Generation System shall support bulk content management operations such
463 as upload, download and remove.
- 464 • *The HSIN Next Generation System shall provide the capability to segregate content based*
465 *upon individual community governance preferences.*
- 466 • *The HSIN Next Generation System shall be capable of handling Protected Critical*
467 *Infrastructure Information (PCII) data.*
- 468 • *The HSIN Next Generation System shall be certified to handle PCII data.*
- 469 • *The HSIN Next Generation System shall provide end-users with the ability to execute*
470 *Freedom of Information Act (FOIA) requests.*
- 471 • *The HSIN Next Generation System shall only provide the FOIA requestor with the content*
472 *that the Agency “owns.”*
- 473 • *The HSIN Next Generation System shall permanently “tag” all content with originating*
474 *identifying information, including author and agency, which enables*
475 *permanent/continuous/persistent ownership of all content.*
- 476 • *The HSIN Next Generation System shall “tag” all content to track individuals what have*
477 *downloaded a particular content piece.*
- 478 • *The HSIN Next Generation System shall allow content owners to “tag” all content with*
479 *accessibility information, which enables Section 508 compliance of all content.*
- 480 • *The HSIN Next Generation System shall provide the capability to “tag” content with*
481 *handling procedures for each piece of content (i.e., how long to store and where to store).*
- 482 • *The HSIN Next Generation System shall allow content to be saved to a user-defined subject.*
- 483 • *The HSIN Next Generation System shall allow content to be retrieved by a user-defined*
484 *subject.*
- 485 • *The HSIN Next Generation System shall allow the author/agency that introduced the content*
486 *into the system to retain all rights over any content they “publish.”*

- 487 • *The HSIN Next Generation System shall provide the ability to use analytical tools on content*
488 *for the purposes of analyzing for patterns.*
- 489 • *The HSIN Next Generation System shall provide the ability for user-defined content*
490 *attributes.*
- 491 • *The HSIN Next Generation System shall provide the ability to search and link across portals*
492 *for content containing an attribute.*
- 493 • *The HSIN Next Generation System shall allow content submitters to choose to prevent the*
494 *content from being saved onto other user's computers.*
- 495 • *The HSIN Next Generation System shall allow content submitters to choose to prevent the*
496 *content from being copied.*
- 497 • *The HSIN Next Generation system shall provide users with spell-check capabilities so that*
498 *the spelling of text entered in free-text field can be checked before submission.*
- 499 • *The HSIN Next Generation System shall comply with the Content Management Standards of*
500 *the DHS Enterprise Portal Standards List, including:*
 - 501 – *DoD 5015.2-STD, Design Criteria Standard for Electronic Records Management*
502 *Software Applications*
 - 503 – *OASIS OpenDocument, Version 1.x*
 - 504 – *ISO 15489 (Parts 1 and 2)*
 - 505 – *JSR 170/283*
506

507 **2.2.1.1 Content Type**

508 The HSIN Next Generation System will be able to support a diverse array of content types on its content
509 management platform and many different types of industry sensitive information. The HSIN Next
510 Generation System should enable users to create, share, and edit simple and rich digital content.
511

512 The content type requirements for the HSIN Next Generation System are listed below:
513

- 514 • *The HSIN Next Generation System shall support, but not limited to, the following various*
515 *content types, for capture classification, attachment to workflows, editing, printing, and*
516 *managing as:*
 - 517 – *Microsoft Office suite (Word, Excel, PowerPoint, Project, Access, Publisher, InfoPath,*
518 *and Visio)*
 - 519 – *Websites*
 - 520 – *eXtensible Markup Language (XML) / HyperText Markup Language (HTML) / eXtensible*
521 *Stylesheet Language Transformation (XSLT) / Cascading Style Sheet (CSS)*
 - 522 – *Portable Document Format (PDF)*
 - 523 – *Tagged Image File Format (TIFF)*
 - 524 – *Bitmap (BMP)*
 - 525 – *Joint Photographic Experts Group (JPEG)*
 - 526 – *Portable Network Graphic (PNG)*

- 527 – *Email, including archive formats (Microsoft Outlook and Lotus Notes)*
- 528 – *Email attachments*
- 529 – *Geospatial documentation/data*
- 530 – *Databases (Structured Query Language [SQL], Oracle, Microsoft Access)*
- 531 – *WinZip*
- 532 – *Adobe Page Maker*
- 533 – *Adobe Photoshop*
- 534 – *Rich Media*
- 535 – *Adobe animation (e.g. Flash, Shockwave)*
- 536 – *Streaming video*
- 537 – *Workflow tools*
- 538 – *Faxes routed through electronic gateways*
- 539 – *Others as may be determined by the government*
- 540 • *The HSIN Next Generation System shall support National Oceanic and Atmospheric*
541 *Administration (NOAA) Vessel Monitoring System (VMS) data.*
- 542 • *The HSIN Next Generation System shall provide protection of information in accordance*
543 *with its characteristics, down to individual content components in documents.*
- 544 • *The HSIN Next Generation System shall provide a means of compressing content.*
- 545 • *The HSIN Next Generation System shall provide a means of tagging and ingesting external*
546 *emails and attachments directly to the system repository.*
- 547 • *The HSIN Next Generation System shall provide a means of maintaining the original format*
548 *of the external emails and attachments so they can be copied back into the originating*
549 *environment.*
- 550 • *The HSIN Next Generation System shall provide selective inclusion/exclusion of external*
551 *email attachments and multipart emails and attachments for capture into the system repository.*
- 552 • *The HSIN Next Generation System shall provide an ability to capture external email heading.*
- 553 • *The HSIN Next Generation System shall provide the ability to save email in .msg format.*
- 554 • *The HSIN Next Generation System shall provide capability for tagging content using*
555 *metadata.*
- 556 • *The HSIN Next Generation System shall provide the user the ability to define metadata*
557 *categories.*
- 558 • *The HSIN Next Generation System shall retain all metadata associated with any piece of*
559 *information during its entire life-cycle.*
- 560 • *The HSIN Next Generation System shall enable users to create, share, and edit simple and*
561 *rich digital content including any tagging necessary for accessibility (Section 508 compliance).*
562

563 **2.2.1.2 Search and Discovery**

564 Search is a critical cornerstone to the information exchange and sharing objectives of the HSIN Next
565 Generation System. To meet the needs of information retrieval from across disparate agencies,
566 communities, and sources, the HSIN Next Generation System must employ a uniform federated search
567 interface that can issue broad reaching flexible queries, and results-merging and ranking capabilities.
568 While not all data sources might be local to the HSIN Next Generation System, all data featured in the
569 HSIN Next Generation System should be indexed for ease of search.

570
571 The search and discovery requirements for the HSIN Next Generation System are listed below:
572

- 573 • The HSIN Next Generation System shall provide federated search engine capability based on
574 user access privileges.
- 575 • *The HSIN Next Generation System shall provide all applicable search result titles and*
576 *classification levels, regardless of user access privilege.*
- 577 • *The HSIN Next Generation System shall display a point of contact (POC) for search results*
578 *the user does not have privileges to access.*
- 579 • *The HSIN Next Generation System shall provide the ability and require that the user select to*
580 *have their document returned in search results if the searcher does not have access otherwise.*
581 *NOTE: The default for every posting shall be to NOT be searchable by non-privileged users*
- 582 • The HSIN Next Generation System shall provide capability to query systems of record.
- 583 • The HSIN Next Generation System shall provide capability to unambiguously index
584 information.
- 585 • The HSIN Next Generation System shall provide capability to display search results.
- 586 • *The HSIN Next Generation System shall provide capability to export search results.*
- 587 • The HSIN Next Generation System shall perform crawler-type indexing for enhanced search
588 (e.g., Google desktop).
- 589 • *The HSIN Next Generation System shall comply with the Search Standards of the DHS*
590 *Enterprise Portal Standards List, including ISO 23950:1998, Information Retrieval (Z39.50).*
- 591 • *The HSIN Next Generation System shall allow the end-users to select any content from a*
592 *search for use directly through the browser or for downloading onto their personal computer*
593 *(PC).*
- 594 • *The HSIN Next Generation System shall allow users to search on specific file formats.*
- 595 • *The HSIN Next Generation System shall allow users to search on specific validity dates.*
- 596 • *The HSIN Next Generation System shall allow users to search based on alternative text for*
597 *images and visual file formats.*
- 598 • *The HSIN Next Generation System shall allow users to search on metadata associated with*
599 *content.*

600
601 **2.2.1.3 Personalization/Customization**

602 Due to extensive reach of the HSIN Next Generation System into various levels among Federal, State,
603 Local, Tribal, Territorial, Private Sector and International partners, it is imperative that the HSIN Next
604 Generation System be adaptable to each user communities' needs in terms of functionality and user

605 experience. The need for customization can come from perspectives of various levels of agencies and
606 users. Not all of the HSIN Next Generation System features are used in the same manner or context
607 across communities that have unique missions or processes.
608

609 Personalization will significantly influence the customization capabilities of the HSIN Next Generation
610 System. The HSIN Next Generation System is expected to be a completely dynamic system, which will
611 use operating procedures, to be defined by administrators, to build pages based on such things as a user's
612 logins and items previously viewed to intelligently decide what to show on a page.
613

614 The customization requirements for the HSIN Next Generation System are listed below:
615

- 616 • The HSIN Next Generation System shall support personalization.
- 617 • The HSIN Next Generation System shall provide the ability to customize on a per device
618 basis.
- 619 • The HSIN Next Generation System shall allow users to choose a customized set of links
620 available to them.
- 621 • The HSIN Next Generation System shall allow users to customize their homepage.
- 622 • The HSIN Next Generation System shall allow the user to configure display of system
623 components available to them.
- 624 • The HSIN Next Generation System shall provide the ability to select content from multiple
625 communities and configure display per their preference.
- 626 • The HSIN Next Generation System shall allow integration of common components from
627 multiple communities (e.g., single calendar for all events across all user access areas).
- 628 • The HSIN Next Generation System shall use operating procedures to dynamically customize
629 the user experience.
- 630 • *The HSIN Next Generation System shall use the end-user's cookie setting choices as part of*
631 *each user's profile.*
- 632 • The HSIN Next Generation System shall allow users to create home pages containing portlets
633 within the HSIN Next Generation framework.
- 634 • *The HSIN Next Generation System shall enable users to tag all content as necessary for*
635 *accessibility (Section 508 compliance).*
- 636 • *The HSIN Next Generation System shall comply with the personalization standards of the*
637 *Enterprise Portal Standards List, including:*
 - 638 – *HTML 4.x*
 - 639 – *Portlets/Webparts – JSR 168*
 - 640 – *Asynchronous JavaScript and XML (AJAX)*
641

642 **2.2.1.4 Content Subscriptions**

643 The HSIN Next Generation System will offer the ability for all users to configure individual Really
644 Simple Syndication (RSS) feed lists. Through this list, users may subscribe to content updates from
645 various syndications for objects, events, and sources. The aggregation of this information should be
646 presented in a uniform setting for all HSIN Next Generation System users.

- 647
648 The content subscription requirement for the HSIN Next Generation System is listed below:
649
650
- The HSIN Next Generation System shall provide content subscription capabilities.
 - The HSIN Next Generation System shall provide the ability to configure individual RSS Feed lists.
- 651
652
653

654 **2.2.2 User Management**

655 The HSIN Next Generation System's administrators and approved users will have the ability to manage
656 users and account settings. Maintaining and managing the HSIN Next Generation System repository of
657 users is critical to the security and integrity of the system. HSIN will have basic user management and
658 assignment capabilities. HSIN Next Generation member managers will be able to define, create, modify,
659 delete and add users.

660 The user management requirements for the HSIN Next Generation System are listed below:

- The HSIN Next Generation System shall provide registration to admit a new user into the system.
 - *The HSIN Next Generation System shall provide registration to admit new users into the system in bulk.*
 - *The HSIN Next Generation System shall use agency active directories in support of managing users.*
 - *The HSIN Next Generation System shall enforce user acceptance of an approved access agreement to gain access to the System for the first time.*
 - *The HSIN Next Generation system shall enforce user acceptance of an approved access agreement to gain access to the system at account revalidation.*
 - *The HSIN Next Generation system shall support the automatic creation/maintenance of accounts with appropriate role attributes defined by a Security Assertion Markup Language (SAML) assertion.*
 - *The HSIN Next Generation system shall provide the capability for users to establish user groups by individual users or by specifying user metadata.*
 - *The HSIN Next Generation system shall provide the capability for users to share groups with other users.*
 - *The HSIN Next Generation System shall allow the assignment of security levels to approved users or groups of users.*
 - *The HSIN Next Generation System shall provide a workflow capability to manage the user management process.*
 - *The HSIN Next Generation System shall provide an emergency workflow process to give access in bulk without having to go through the standard workflow process.*
 - *These accounts shall be tagged as "Special" and shall be deactivated after a predetermined time period.*
- 661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688

689 **2.2.2.1 Role-Based Access and Role Definition**

690 The assignment of roles is critical to the HSIN Next Generation System. Role assignment and privileges
691 within the HSIN Next Generation System will dictate user access to specific areas and content. The
692 system should also flag users for removal based on their defined roles.

693
694 The role-based access and role definition requirements for the HSIN Next Generation System are listed
695 below:

- 696
697 • The HSIN Next Generation System shall support roles in the user repository.
- 698 • The HSIN Next Generation System shall provide role-based access control across all
699 templates, content, processes, and repositories for:
 - 700 – Individual users
 - 701 – Groups of users
 - 702 – Individual directories/domains
 - 703 – Subdirectories
 - 704 – Sites
- 705 • *The HSIN Next Generation System shall assign content access privileges to roles in the user*
706 *repository.*
- 707 • The HSIN Next Generation System shall assign users to roles in the user repository.
- 708 • *The HSIN Next Generation System shall be capable of assigning a user to multiple roles.*
- 709 • *The HSIN Next Generation System shall be capable of assigning a user to multiple roles on a*
710 *temporary basis.*
- 711 • *The HSIN Next Generation System shall assign role access requirements to a single piece of*
712 *content in the user repository.*
- 713 • *The HSIN Next Generation System shall define role access requirements to a collection of*
714 *content in the user repository.*
- 715 • *The HSIN Next Generation System shall have the ability to define role access requirements in*
716 *a single operation to a collection of content.*
- 717 • *The HSIN Next Generation System shall have the ability to define role access requirements in*
718 *a single operation to a collection of services.*
- 719 • *The HSIN Next Generation System shall have the ability to define groups of collections role*
720 *access requirements in a single operation.*
- 721 • *The HSIN Next Generation System shall have the ability to remove temporary role*
722 *assignments after a predefined period of time automatically.*
723

724 **2.2.3 Access Management**

725 Users will be provided access to the HSIN Next Generation System content based on their role and
726 mission within the community. This should include HSIN Next Generation System COI, pages, services
727 (such as applications), and content.

- 728 • *The HSIN Next Generation System shall allow the establishment of discrete access rights for*
729 *all content, including custom content and functions.*

- 730 • *The HSIN Next Generation System shall provide security levels that can be set by the system*
731 *approved users (i.e., users granted some system administrative privileges, usually on a temporary*
732 *basis).*
- 733 • *The HSIN Next Generation System shall allow the assignment of security levels and*
734 *temporary privileges to approved roles to access approved content to which the end-user already*
735 *has access (e.g., delegate rights downstream).*
- 736 • The HSIN Next Generation System shall allow approved end-users to have temporary
737 privileges.
- 738 • *The HSIN Next Generation System shall provide the ability for approved roles to override*
739 *access controls to release/unlock content.*
- 740 • *The HSIN Next Generation System shall ensure that the end-user cannot use the system in*
741 *any way to identify the presence of content to which they are unauthorized.*
- 742 • The HSIN Next Generation System shall restrict search and reporting access rights based on a
743 discrete role or privilege.
- 744 • The HSIN Next Generation System shall restrict content editing access rights, based on a
745 discrete role or privilege.
- 746 • The HSIN Next Generation System shall support the restriction to content print access rights,
747 based on a discrete role or privilege.
- 748 • The HSIN Next Generation System shall restrict content view only access rights, based on a
749 discrete role or privilege.
- 750 • The HSIN Next Generation System shall restrict content metadata view only access rights,
751 based on a discrete role or privilege.
- 752 • The HSIN Next Generation System shall restrict content delete access rights, based on a
753 discrete role or privilege.
- 754 • The HSIN Next Generation System shall restrict content workflow access rights, based on a
755 discrete role or privilege.
- 756 • *The HSIN Next Generation System shall allow approved users to transfer ownership of*
757 *content allocated to users who may have left the organization.*
758

759 **2.3 Collaboration and Communication**

760 **2.3.1 Collaboration**

761 The HSIN Next Generation System will maximize the quality and accessibility of content by allowing
762 end-users to enforce standard production workflows, by providing effective tools for organizing,
763 categorizing and scheduling content. Collaboration is a primary requirement of the HSIN Next Generation
764 System, consisting of two or more persons working together to support the mission. This consists of real-
765 time communications, collaborating through discussion boards, Instant Messaging (IM) and other means
766 of communicating with other users.
767

768 The HSIN Next Generation System should be designed with “presence technology” in mind. Presence
769 technology makes collaboration possible wherever and whenever users are online. Providing this
770 technology to such things as IM makes real-time collaboration effortless and intuitive. A driver with a
771 GPS-enabled device is an example of presence technology. The driver can be tracked and sent messages

772 warning about traffic delays and suggesting alternate routes. Presence technology is an integral part of
773 third generation (3G) wireless networks, and is being employed across a wide variety of communication
774 devices, including cell phones, laptop computers, personal digital assistants (PDAs), television sets, and
775 pagers.

776
777 The HSIN Next Generation System must provide comprehensive web-based meeting capabilities that
778 allow users from various jurisdictions to attend and participate. This must include the ability for multiple
779 users to view presentation data of any visual and/or audio type presented in real-time. The common
780 practices in this capability area dictates the functions for administration of presentation, screen
781 publishing, attendance tracking, question sharing, and various other support functions that enable
782 interactive information presentation for virtual meetings.

783
784 The general collaboration requirements for the HSIN Next Generation System are listed below:

- 785
786 • The HSIN Next Generation System shall provide joint, simultaneous and controlled
787 information sharing capabilities as defined by roles.
- 788 • The HSIN Next Generation System shall support industry best practices for device presence
789 sensing capabilities whenever and wherever possible.
- 790 • *The HSIN Next Generation System shall provide online meeting support capabilities.*
- 791 • *The HSIN Next Generation System shall provide virtual whiteboard capabilities.*
- 792 • *The HSIN Next Generation System shall allow the end-users to post content in multiple*
793 *locations, in one transaction (federated posting). (Note: The intent of this requirement is not to*
794 *duplicate content).*
- 795 • The HSIN Next Generation System shall provide a community calendar feature that enables
796 users to view and log related timelines and schedules.
- 797 • The HSIN Next Generation System shall allow users to add events to external personal
798 calendar tools.
- 799 • The HSIN Next Generation System shall provide polling capabilities.
- 800 • The HSIN Next Generation System shall provide survey capabilities.
- 801 • *The HSIN Next Generation System shall compartmentalize Internet protocols for seamlessly*
802 *sharing real-time video information.*
- 803 • *The HSIN Next Generation System shall synchronize Internet protocols for seamlessly*
804 *sharing real-time video information.*
- 805 • *The HSIN Next Generation System shall provide an email gateway.*
- 806 • *The HSIN Next Generation System shall allow multiple user edit of content.*
807

808 **2.3.1.1 Alerts, Notifications, and Announcements**

809 The HSIN Next Generation System must have the ability to send alerts, notifications and post public
810 announcements by an automated event or manual triggers to what would be a dynamically configurable
811 set of HSIN end-users through multiple mediums. Mediums may include, but is not limited to, web
812 portal, email, Short Message Service (SMS), and Wireless Application Protocol (WAP).

813

814 The alert, notification, and announcement requirements for the HSIN Next Generation System are listed
815 below:

- 816
- 817 • The HSIN Next Generation System shall have the ability to process real-time alerts,
818 notifications, and announcements.
- 819 • The HSIN Next Generation System shall allow approved users to send alerts regarding any
820 type of announcements.
- 821 • The HSIN Next Generation System shall allow approved users to send alerts, notifications,
822 and announcements to individual users or groups of users.
- 823 • *The HSIN Next Generation System shall allow for personal creation of "alert groups" as well*
824 *as administrator groups for all users with specified permissions.*
- 825 • *The HSIN Next Generation system shall provide end users with the subject (or other*
826 *indicator) of the content referenced in a notification or alert.*
- 827 • *The HSIN Next Generation System shall support incoming messages, enabling interactive*
828 *responses to alerts, notifications, and announcements.*
- 829 • *The HSIN Next Generation System shall provide the recipients with a brief description of why*
830 *the alert, notification, or announcements was sent, as entered by the author.*
- 831 • *The HSIN Next Generation System shall allow end-users to report receiving an alert,*
832 *notification, or announcement in error and request to opt out any future related alerts.*
- 833 • *The HSIN Next Generation System shall capture and record when a user reports that they*
834 *received an alert, notification, or announcement in error, for later analysis.*
- 835 • *The HSIN Next Generation system shall allow end-users to view all of the alerts,*
836 *notifications, and announcements they have received.*
- 837 • *The HSIN Next Generation System shall allow users to view alerts, notifications, and*
838 *announcements they have sent.*
- 839 • *The HSIN Next Generation System shall be able to store, recall, and display all sent alerts,*
840 *notifications, and announcements, including their footers and any metadata.*
- 841 • *The HSIN Next Generation System shall allow a user to view the name of the alert,*
842 *notification, or announcement sender for all of the alerts they have received.*
- 843 • *The HSIN Next Generation System shall provide receipt confirmation capabilities for alerts,*
844 *notifications, and announcements.*
- 845 • *The HSIN Next Generation System shall allow for senders of view alerts, notifications, and*
846 *announcements to track and print reports of acknowledgement.*
- 847 • *The HSIN Next Generation System shall allow approved users to view the names of recipients*
848 *who have opened their intended view alerts, notifications, and announcements for supported alert*
849 *types.*
- 850 • *The HSIN Next Generation System shall allow approved users to set priorities for view alerts,*
851 *notifications, and announcements.*
- 852 • *The HSIN Next Generation system shall allow end users to use a content keyword in order to*
853 *define automated content alerts, notifications, and announcements.*

- 854 • *The HSIN Next Generation system shall provide alerts, notifications and announcements of*
855 *new content based on content metadata fields.*
- 856 • *The HSIN Next Generation System shall allow end-users to set the preferences, without help*
857 *desk intervention, for which communication medium they will receive view alerts, notifications,*
858 *and announcements.*
- 859 • *The HSIN Next Generation System shall allow view alerts, notifications, and announcements*
860 *to be displayable on the homepage.*
- 861 • *The HSIN Next Generation System shall comply with the Alerts / Warnings / Notification*
862 *Standards of the DHS Enterprise Portal Standards List, including:*
 - 863 – *Web Notification Service (WNS) 0.1.0 in accordance with the OpenGIS Web Notification*
864 *Service discussion paper*
 - 865 – *Common Alerting Protocol (CAP), V1.x*
866

Content Alerts, Notifications, and Announcements

869 In addition to the ability for all HSIN Next Generation System users to receive triggered alerts,
870 notifications, and announcements, the system must provide the capability to customize a subscription
871 service for alerts, notifications, and announcements to any object or event at a granular level in the HSIN
872 Next Generation System. Syndication of all content and events within the HSIN Next Generation System
873 is necessary to enable the information feed aggregation feature. An example would be a new file upload
874 of a certain type that is posted to a specific community that triggers an email notification to authorized
875 persons of interest.

876
877 The content alert, notification, and announcement requirements for the HSIN Next Generation System are
878 listed below:

- 880 • *The HSIN Next Generation System shall provide end-users the ability to navigate directly to*
881 *the content that is referenced in the view alert, notification, or announcement.*
- 882 • *The HSIN Next Generation System shall provide the ability to update alerts, notifications,*
883 *and announcements.*
- 884 • *The HSIN Next Generation System shall provide the ability to remove alerts, notifications,*
885 *and announcements.*
886

Alerting Warning System (AWS)

887
888
889 The projected number of cross-agency users that HSIN targets to support and integrate into the network
890 places the HSIN Next Generation System in a unique strategic position to be the single centralized point
891 of critical information dissemination with time-sensitivity (as required by HSPD-5). Federal Emergency
892 Management Agency (FEMA) initiated the Integrated Public Alert and Warning System (IPAWS) from
893 Executive Order 13407, making it the Nation's next generation public communications and warning
894 capability. To support the mission to improve reliability, security and accessibility of public alerts and
895 warnings, the HSIN Next Generation System will integrate with IPAWS.
896

897 The Alerting Warning System requirements for the HSIN Next Generation System are listed below:

- 898 • *The HSIN Next Generation System shall support the IPAWS requirements for alerting.*
899

- 900 • *The HSIN Next Generation System shall integrate with the DHS chosen alerting tool.*
- 901 • *The HSIN Next Generation System shall require approved users to provide a brief*
902 *explanation of why they are sending the alert.*
- 903 • *The HSIN Next Generation System shall require approved users to select a pre-defined footer*
904 *when entering alerts.*
- 905 • *The HSIN Next Generation System shall allow approved users to send alerts to multiple*
906 *communication medium and device including email and SMS.*
- 907 • *The HSIN Next Generation System shall allow end-users to receive alerts via multiple*
908 *communication mediums, including email and SMS.*
- 909 • *The HSIN Next Generation System shall allow approved users to override the end-users*
910 *defined communication medium preferences, on a per alert basis.*
- 911 • *The HSIN Next Generation System shall truncate messages sent via SMS at 60 characters.*
912 *The remaining message shall be sent via email.*
- 913 • *The HSIN Next Generation System shall allow approved users to send alerts that are only*
914 *available to the user through the web portal, which will send an external notification of the*
915 *waiting alert.*
- 916 • *The HSIN Next Generation System shall be capable of handling alerts at different priority*
917 *levels.*
918

919 **2.3.1.2 User Community Directory**

920 The HSIN Next Generation System must allow COIs to maintain a local user community directory
921 drawing relevant user contact information based on dynamic COI membership accounts. This
922 information would be statically displayed and available for authorized users to obtain.
923

924 The user community directory requirements for the HSIN Next Generation System are listed below:
925

- 926 • *The HSIN Next Generation System shall provide a User Community Directory containing an*
927 *interactive contact database which is inclusive of all community users.*
- 928 • *The HSIN Next Generation System shall allow the User Community Directory to be*
929 *searchable as permissions allow.*
- 930 • *The HSIN Next Generation System shall provide User Community Directory functionality to*
931 *integrate with Instant Messaging functions.*
- 932 • *The HSIN Next Generation System shall provide User Community Directory functionality to*
933 *provide management of lists (subscription, create, edit, delete) by user and/or role.*
- 934 • *The HSIN Next Generation System shall provide User Community Directory functionality to*
935 *integrate with other services of HSIN.*
- 936 • *The HSIN Next Generation System shall allow export of the User Community Directory as*
937 *permissions allow.*
- 938 • *The HSIN Next Generation System shall allow users of an approved role to omit the User*
939 *Community Directory from display and access.*
- 940 • *The HSIN Next Generation System shall provide end-users the ability to share contact*
941 *information with other end-users.*

- 942 • *The HSIN Next Generation System shall provide end-users the ability to choose which*
943 *contact information to share with other end-users within their COI.*
- 944 • *The HSIN Next Generation System shall provide end-users the ability to choose which*
945 *contact information to share with other end-users outside of their COI.*
- 946 • *The HSIN Next Generation System shall provide authorized users the ability to create contact*
947 *lists.*
- 948 • *The HSIN Next Generation System shall provide authorized users the ability to save contact*
949 *lists.*
- 950 • *The HSIN Next Generation System shall provide authorized users the ability to update*
951 *contact lists they have created when authorized.*
- 952 • *The HSIN Next Generation System shall provide authorized users the ability to share contact*
953 *lists they created with other users when authorized.*
- 954 • *The HSIN Next Generation System shall provide authorized users the ability to remove*
955 *contact lists.*
956

957 **2.3.1.3 Instant Messaging (IM)**

958 The HSIN Next Generation System will provide an IM application.

959

960 The IM requirements for the HSIN Next Generation System are listed below:

961

- 962 • The HSIN Next Generation System shall provide real-time IM capability with presence
963 sensing.
- 964 • *The HSIN Next Generation System shall allow IM by user title or name.*
- 965 • The HSIN Next Generation System shall allow end-users to perform searches on IM sessions.
- 966 • The HSIN Next Generation System shall allow the end-users to have multiple IM windows
967 open at the same time.
- 968 • The HSIN Next Generation System shall allow the end-users to cut and paste text from or
969 into an IM session.
- 970 • The HSIN Next Generation System shall allow the end-users to print a discussion or dialogue
971 from an IM.
- 972 • The HSIN Next Generation System shall record and retain all user communication via IM.
- 973 • The HSIN Next Generation System shall provide file transfer via IM.
- 974 • The HSIN Next Generation System shall encrypt text-based messaging in accordance with
975 NIST standards.
- 976 • The HSIN Next Generation System shall allow end-users to create both persistent and
977 temporary chat rooms.
- 978 • *The HSIN Next Generation System Instant Messaging software clients shall meet all Section*
979 *508 Software (1194.21) provisions.*
- 980 • *The HSIN Next Generation System shall comply with the Instant Messaging Standards of the*
981 *DHS Enterprise Portal Standards List, including:*

- 982 – *Hypertext Transfer Protocol Secure (HTTPS)*
- 983 – *Hypertext Transfer Protocol (HTTP)*
- 984 – *HyperText Markup Language (HTML)*
- 985 – *Multimedia Internet Message Extension (MIME)*
- 986 – *Session Initiation Protocol (SIP)*
- 987 – *Real-Time Protocol (RTP)*
- 988 – *eXtensible Messaging and Presence Protocol (XMPP)*
- 989 – *Internet Relay Chat (IRC)*

990

991 **2.3.1.4 Discussion Boards**

992 The HSIN Next Generation System will provide a web forum function for all HSIN Next Generation
993 System COIs. All HSIN Next Generation communities must be able to create their own discussion
994 boards that are managed by COI administrators or approved users, who should be able to edit and remove
995 threads and moderate community users. As part of the overall solution to information assurance, the
996 threaded discussion will also carry the feature of discussion archival per all legal requirements of certain
997 HSIN Next Generation System participating agencies.

998

999 The discussion board requirements for the HSIN Next Generation System are listed below:

1000

1001

- The HSIN Next Generation System shall provide Discussion Board capabilities.

1002

- The HSIN Next Generation System shall provide threaded discussion capabilities.

1003

- *The HSIN Next Generation System shall archive threaded discussions for not less than five years in accordance with minimum legal requirements of certain HSIN Next Generation System participating agencies.*

1004

1005

1006

- The HSIN Next Generation System shall allow end-users to create new discussions as needed.

1007

1008

- The HSIN Next Generation System shall allow authorized end-users to participate in existing discussions as role/permissions allow.

1009

1010

- The HSIN Next Generation System shall allow end-users to filter discussion threads by thread attributes (e.g. topic, date).

1011

1012

- The HSIN Next Generation System shall allow authorized end-users to remove discussion threads.

1013

1014

- The HSIN Next Generation System shall allow end-users to update discussion threads.

1015

- *The HSIN Next Generation System shall provide capabilities for archiving discussion threads.*

1016

1017

- *The HSIN Next Generation System shall allow for the end-users to post something on multiple discussion boards in one transaction (federated posting).*

1018

1019

- *The HSIN Next Generation System Discussion Boards shall meet all Section 508 provisions for web content.*

1020

1021 • *The HSIN Next Generation System shall comply with the Message Board Standards of the*
1022 *DHS Enterprise Portal Standards List, including:*

1023 – *T120*

1024 – *T123*

1025

1026 **2.3.1.5 Feedback**

1027 The feedback functionality within the HSIN Next Generation System is required to play a major role in
1028 the upkeep and maintenance of the HSIN Next Generation System usability and end-user relationships.
1029 This feedback feature must account for a process that involves a two-tier response system where all HSIN
1030 Next Generation System user feedback is vetted by the immediate COI administrators or approved users
1031 before being escalated to the HSIN Next Generation System Program Management level. The
1032 functionality of the feedback feature will be based on the system's integrated content management and
1033 workflow capabilities.

1034

1035 The scope of the feedback feature must include, but not be limited to, the following types:

1036

1037 • Change requests

1038 • Service requests

1039 • New functionality

1040 • Bug fix

1041 • Training request

1042 • General comments

1043

1044 To support the handling of various types of feedback filtered through the HSIN Next Generation System,
1045 it must provide workflow actions and status reporting for all authorized HSIN Next Generation System
1046 end-user groups involved in the resolution process. At various intervals of events and status changes, the
1047 HSIN Next Generation System shall automatically notify feedback stakeholders of those changes and
1048 feedback responses.

1049

1050 The feedback requirements for the HSIN Next Generation System are listed below:

1051

1052 • *The HSIN Next Generation System shall provide a feedback workflow form.*

1053 • *The HSIN Next Generation System shall ensure that the receipt of Feedback Forms shall be*
1054 *subject to role based access.*

1055 • *The HSIN Next Generation System shall allow end-users to manage and respond to feedback.*

1056 • *The HSIN Next Generation System shall allow users to assign a numeric rating to document*
1057 *content, events, tools, and applications.*

1058 • *The HSIN Next Generation System shall allow users to filter by the assigned numeric rating.*

1059 • *The HSIN Next Generation System shall provide social book marking for users to view the*
1060 *internal and external web pages most popular with other users.*

1061 • *The HSIN Next Generation System forms shall allow people using assistive technology to*
1062 *access the information, field elements, and functionality required for completion and submission*
1063 *of the form, including all directions and cues.*

1064

1065 **2.3.1.6 Workflow Management**

1066 The HSIN Next Generation System will facilitate the automation of processes involving combinations of
1067 human and machine based activities; particularly those involving IT applications and tools.

1068
1069 To facilitate information exchange and collaboration between its end-users from various jurisdictions, the
1070 HSIN Next Generation System must be able to automate content processing transactions between users
1071 and/or communities that have established formal manual handling processes. Potential tasks and
1072 activities that would require automation support include, though not limited to, information submission,
1073 vetting, and validation.

1074
1075 The HSIN Next Generation System will be able to tag data with its source (author or agency). This
1076 original source tag will remain intact regardless of where the data may travel.

1077
1078 The HSIN Next Generation System will provide support for information exchange and tracking and the
1079 ability to capture and track community task lists. This function must entail the ability to track task list
1080 item details and the individuals assigned to the task, and report on task status and percentage complete
1081 when changed either manually or automatically due to a work flow. The task list must also enable HSIN
1082 Next Generation System COIs to prioritize a comprehensive list based on a set of attributes that can be
1083 sorted within a display.

1084
1085 The workflow management requirements for the HSIN Next Generation System are listed below:

- 1086
- 1087 • *The HSIN Next Generation System shall provide workflow model capabilities for routing,*
1088 *action and closure.*
 - 1089 • *The HSIN Next Generation System shall provide the users with a visualization and textual*
1090 *equivalent of the process and organization structures within a workflow.*
 - 1091 • *The HSIN Next Generation System will provide the users with reminders, deadlines, business*
1092 *rules and other common functionalities associated with workflows.*
 - 1093 • *The HSIN Next Generation System shall provide monitoring and documentation of workflow*
1094 *process status, routing and outcomes.*
 - 1095 • *The HSIN Next Generation System shall provide transactional support at COI level in line*
1096 *with COI business operations surrounding:*
 - 1097 – *Information Submission*
 - 1098 – *Information Vetting*
 - 1099 – *Information Validation*
 - 1100 • *The HSIN Next Generation System shall provide a task list capability that is integrated with*
1101 *the work flow capabilities.*
 - 1102 • *The HSIN Next Generation System shall provide users with accessible online form creation.*
 - 1103 • *The HSIN Next Generation System shall provide users the ability to save task lists.*
 - 1104 • *The HSIN Next Generation System shall provide users the ability to update task lists.*
 - 1105 • *The Next Generation System shall provide users the ability to remove task lists they have*
1106 *created when authorized.*

- 1107 • *The HSIN Next Generation System shall provide users the ability to remove a task from task*
1108 *lists.*
- 1109 • *The HSIN Next Generation System shall provide users the ability to share task lists they*
1110 *created with other users when authorized.*
- 1111 • *The HSIN Next Generation System shall comply with the Business Process / Workflow*
1112 *Standards of the DHS Enterprise Portal Standards List, including Web Services for Business*
1113 *Process Execution Language (WS-BPEL) V2.x.*
1114

1115 **2.4 Situational Awareness**

1116 **2.4.1 Visualization**

1117 Data visualization is the use of interactive, visual representations of abstract and non-abstract data to
1118 provide for decision support and situational awareness. Visualization provides user interactivity and
1119 dynamic visual representation. The user can modify the visualization in real-time, thus affording
1120 perception of patterns and structural relations in the abstract data in question.
1121

1122 The HSIN Next Generation System will support visualization tools to view data in graphical, geospatial
1123 and temporal views. It is the intent of DHS to implement geospatial, graphical, statistical, relational and
1124 temporal visualization tools as integrated components supporting an information design. These tools
1125 should provide the ability to visually display situational data in a geospatial manner and the ability to
1126 layer multiple types of situational data within the same graphical presentation.
1127

1128 The visualization requirements for the HSIN Next Generation System are listed below:
1129

- 1130 • The HSIN Next Generation System shall display or provide access to situational data in a
1131 geospatial, tabular, graphic, or textual manner.
- 1132 • The HSIN Next Generation System shall support graphical visualization tools.
- 1133 • The HSIN Next Generation System shall support geospatial visualization tools.
- 1134 • The HSIN Next Generation System shall support temporal view visualization tools.
- 1135 • *The HSIN Next Generation System shall comply with the Geospatial Standards of the DHS*
1136 *Enterprise Portal Standards List, including:*
 - 1137 – *Web Map Service (WMS) 1.1.1*
 - 1138 – *Web Terrain Service (WTS) 0.5*
 - 1139 – *Information Systems eXtensible Markup Language (IS XML)*
 - 1140 – *XML for Image and Map Annotation (XIMA v0.4)*
 - 1141 – *Wireless Communication Service (WCS) 1.0*
 - 1142 – *Web Feature Service (WFS) 1.0*
1143

1144 **2.4.1.1 Viewing Environment**

1145 The HSIN Next Generation System will provide an information and exchange environment to share and
1146 collaborate on data with multiple users. Users will be able to log into, navigate and edit data in the

1147 environment. The viewing environment will support users working collaboratively on documents and
1148 data.

1149

1150 The viewing environment requirements for the HSIN Next Generation System are listed below:

1151

1152 • The HSIN Next Generation System shall allow the end-users to filter on the source of data to
1153 block if needed (such as a spam filter).

1154 • *The HSIN Next Generation System shall provide a homepage upon user logon.*

1155 • The HSIN Next Generation System shall support the integration of visualization views into
1156 applications and information.

1157 • The HSIN Next Generation System shall provide navigation and controls on visualization
1158 views.

1159 • The HSIN Next Generation System shall allow users to select elements on visualization
1160 views.

1161 • The HSIN Next Generation System shall always display the current DHS national threat level
1162 and provide severity color codes for incident data analysis and display, in all views.
1163

1164 **2.4.1.2 Geospatial Information System (GIS) Mapping**

1165 DHS Preparedness Directorate commissioned the development of a geospatial-intelligence decision-
1166 support tool that maps real-time situation awareness information. The HSIN Next Generation System
1167 must support data gathering and data merging functions that supply data layers to, at a minimum, the
1168 DHS mandated GIS tool map intelligence.

1169

1170 The GIS mapping environment requirements for the HSIN Next Generation System are listed below:

1171

1172 • *The HSIN Next Generation System shall be compliant with the Homeland Security Geospatial
1173 Information Infrastructure (GII).*

1174 • *The HSIN Next Generation System shall be designed in accordance with the DHS geospatial
1175 data model.*

1176 • The HSIN Next Generation System shall allow end-users to use the display/map to create
1177 boundaries for data sharing.

1178 • *The HSIN Next Generation System shall allow end-users to use a map to set the duration of
1179 displayed data.*

1180 • *The HSIN Next Generation System shall allow users to view a notification that data is about
1181 to expire.*

1182 • *The HSIN Next Generation System shall allow end-users to use the map to mark data for
1183 analysis.*

1184 • *The HSIN Next Generation System shall allow end-users to recall data displayed on the map.*

1185 • *The HSIN Next Generation System shall allow import and export of GIS layers.*

1186 • The HSIN Next Generation System must provide GIS Mapping Common Service.
1187

1188 **3 NON-BUSINESS REQUIREMENTS**

1189

1190 **3.1 Security / Information Assurance**

1191 The overall security objective of the HSIN Next Generation System is to ensure adequate protection of
1192 the Sensitive but Unclassified category of information shared and transmitted through the HSIN Next
1193 Generation System as mandated by DHS through policy guidance such as DHS Management Directive
1194 (MD) 4300A, DHS Secure Baseline Configuration Guidelines, and NIST Special Publication 800-53.
1195 While HSIN must conform to established technical security requirements, it must also achieve its mission
1196 goals of enabling and promoting information sharing among cross-component users by making data
1197 available for access to authorized personnel.

1198
1199 The general information assurance/security requirements for the HSIN Next Generation System are listed
1200 below:

- 1201
- 1202 • The HSIN Next Generation System shall comply with the security operating principles
1203 mandated in DHS MD 4300A.
 - 1204 • The HSIN Next Generation System shall provide network security monitoring capabilities in
1205 accordance with DHS MD 4300A.
 - 1206 • The HSIN Next Generation System shall provide intrusion detections capabilities in
1207 accordance with DHS MD 4300A.
 - 1208 • The HSIN Next Generation System shall comply with the Certification and Accreditation
1209 (C&A) policy in accordance with DHS MD 4300A.
 - 1210 • The HSIN Next Generation System shall provide an alert when suspicious users login.
 - 1211 • The HSIN Next Generation System shall provide an alert when users login from a suspicious
1212 Internet Protocol (IP) address.
 - 1213 • The HSIN Next Generation System shall block logins from IP addresses on block list.
 - 1214 • The HSIN Next Generation System shall provide virus protection capabilities in accordance
1215 with DHS MD 4300A.
 - 1216 • The HSIN Next Generation System shall meet the FIPS PUB 199 rating of “High” for all
1217 categories.
 - 1218 • The HSIN Next Generation System shall provide compartmentalized security in support of
1219 SBU information.
 - 1220 • The HSIN Next Generation System shall support multi-level security for compartmentalizing,
1221 labeling, and identifying multiple types of data classification.
 - 1222 • The HSIN Next Generation System shall provide access control across all templates, content,
1223 processes, and repositories for:
 - 1224 – Individual users
 - 1225 – Groups of users
 - 1226 – Individual directories/domains
 - 1227 – Subdirectories

- 1228 – Sites
- 1229 • The HSIN Next Generation System shall provide authorized users the ability to provide /
1230 revoke all privileges from a specified group or selected user(s).
- 1231 • The HSIN Next Generation System shall be able to prevent “expired” content from being
1232 viewed after the specified date and time.
- 1233 **Note:** While posting data to the system, a user can set a date and time at which the data will no
1234 longer be available for use, because it will be removed from the system at that time.
- 1235 • *The HSIN Next Generation System shall protect data against unauthorized access,
1236 modification, and withholding.*
- 1237 • The HSIN Next Generation System shall identify the source of the original document and the
1238 source of any changes.
1239

1240 **3.1.1 Identity Management – Authentication and Authorization**

1241 As part of the overall HSIN Next Generation System security objective, identity management must
1242 provide a comprehensive, process-oriented approach to the consolidation of identity data and deployment
1243 across the DHS enterprise and Federal, State, Local, Tribal, Territorial, Private Sector and International
1244 partners. Authentication and authorization processes and standards are included in this objective.
1245

1246 Authorization of the HSIN Next Generation System end-users should be comprised of user management
1247 functions that support the definitions of user communities, roles, and related system privileges. Access
1248 control within the system must be designed to enforce the principle of least privilege in accordance to
1249 user type and security level. The HSIN Next Generation System controls must be designed to ensure that
1250 each user is authenticated before access is permitted.
1251

1252 The authentication and authorization requirements for the HSIN Next Generation System are listed
1253 below:
1254

- 1255 • The HSIN Next Generation System shall provide the capabilities to authenticate the identity
1256 of users accessing the system.
- 1257 • The HSIN Next Generation System shall use E-Authentication to authenticate the identity of
1258 users accessing the system.
- 1259 • The HSIN Next Generation System shall provide authentication capabilities in accordance
1260 with DHS MD 4300A.
- 1261 • *The HSIN Next Generation System shall complete user authentication using HSPD-12
1262 guidance.*
- 1263 • *The HSIN Next Generation System shall leverage the HSPD-12 compliant, DHS Single Sign-
1264 On (SSO) defined authentication methodology.*
- 1265 • The HSIN Next Generation System shall store user authentication credentials in the user
1266 repository.
- 1267 • The HSIN Next Generation System shall only transmit user authentication credentials in an
1268 encrypted form.
- 1269 • The HSIN Next Generation System shall ensure that all remote devices and external systems
1270 use NIST-compliant authentication mechanisms when accessing system resources.

- 1271 • The HSIN Next Generation System shall provide control of access to system resources
1272 (content, registries and repositories).
- 1273 • The HSIN Next Generation System shall indicate requested access is denied if roles,
1274 securities, and policies are not met.
- 1275 • The HSIN Next Generation System shall grant a user access to system content only if the user
1276 has been authorized to access the content.
- 1277 • The HSIN Next Generation System shall enforce the principle of least privilege in accordance
1278 with user type and security level.
- 1279 • The HSIN Next Generation System shall provide a time out capability.
- 1280 • *The HSIN Next Generation System shall notify the user and give sufficient time (30 seconds)*
1281 *to indicate more time is required.*
- 1282 • The HSIN Next Generation System shall control interactions between users and content to
1283 ensure confidentiality.
- 1284 • The HSIN Next Generation System processes (i.e., workflows) shall run as a defined
1285 username and associated role.
- 1286 • The HSIN Next Generation System shall not be dependant on hard-coded usernames
1287 (usernames shall not indicate the role of the user).
- 1288 • The HSIN Next Generation System shall share user identification/authentication functionality
1289 with all services.
- 1290 • *The HSIN Next Generation System shall be PKI-enabled⁶ to support access by individual*
1291 *users with valid PKI certificates in accordance with FIPS PUB 201 and HSPD-12.*
- 1292 • *The HSIN Next Generation System shall provide alternate credential (certificate or token)*
1293 *association process.*
- 1294 Note: These credentials must be verified and validated by HSIN Next Generation System in
1295 accordance with the credential issuer policies.
- 1296 • *The HSIN Next Generation System shall provide two factor authentication as defined by*
1297 *OMB M06-16 and DHS MD 4300A.*
1298

1299 **3.1.2 Password Management**

1300 The HSIN Next Generation System will have a robust password management system. The password
1301 management system will allow system administrators to operate, regulate and maintain the passwords of
1302 all HSIN Next Generation System users. The password management system will allow for automated
1303 password management such as expiration notices and password renewal ability. The Password
1304 Management capability will comply with the DHS MD 4300A.
1305

1306 The password management requirements for the HSIN Next Generation System are listed below:
1307

- 1308 • The HSIN Next Generation System shall provide user/user group password management
1309 capabilities.

⁶ "PKI" stands for "Public Key Infrastructure."

- 1310 • The HSIN Next Generation System shall provide username and password management
1311 facilities such that:
- 1312 – User name length are enforced
- 1313 – Password length and composition are enforced
- 1314 – Password changes are enforced after defined periods
- 1315 – Password changes are enforced after first use, in accordance with DHS MD 4300A
- 1316 • *The HSIN Next Generation System shall provide an interactive mechanism to automatically
1317 reset a forgotten or lost password or associated newly issued alternate credential (certificate or
1318 token) without going through the help desk.*
- 1319 • *The HSIN Next Generation System shall allow Service/Agency level policy option to disable
1320 username and password credentials after alternate credential (certificate or token) association is
1321 performed on account.*
- 1322 • The HSIN Next Generation System shall provide an automatic mechanism for alerting users
1323 of their password expiration.
- 1324 • The HSIN Next Generation System shall allow self provisioning of passwords.
1325

1326 **3.1.3 Encryption**

1327 The HSIN Next Generation System encryption will provide secure and private communications between
1328 users. The encryption will be used on prescribed applications to ensure the integrity of the data
1329 transmitted through the system.

1330 The encryption requirements for the HSIN Next Generation System are listed below:
1331

- 1332
- 1333 • The HSIN Next Generation System shall be capable of encrypting content.
- 1334 • The HSIN Next Generation System shall be capable of managing encrypted content.
- 1335 • *The HSIN Next Generation System shall use only Advanced Encryption Standard (AES)
1336 algorithms that have been validated under FIPS PUB 140-2 or National Security Agency (NSA)
1337 Type 2 or Type 1 encryption for protecting sensitive information.*
- 1338 • The HSIN Next Generation System shall use only cryptographic modules that have been
1339 validated in accordance with FIPS PUB 140-2.
- 1340 • The HSIN Next Generation System shall use the AES in accordance with FIPS PUB 197.
1341

1342 **3.1.4 Audit Trail**

1343 Each user of the HSIN Next Generation System is to be individually accountable for his or her actions
1344 while using the system. System auditing tools will provide the ability to track a user's activities. Audit
1345 trails maintain a record of system activity by system or application processes by individual user activity.
1346

1347 The HSIN Next Generation System will collect, store and distribute operating requests to repudiate
1348 content registries and repositories. The audit process will allow for transaction accounting and review of
1349 all content and user activity. This capability enables an authorized user to follow a user/content
1350 throughout the session. Examples include; download activity, page view activity, tool usage, session
1351 durations and contributions.

1352

1353 The audit trail requirements for the HSIN Next Generation System are listed below:

1354

1355 • *The HSIN Next Generation System shall provide security audit capabilities as stated in DHS*
1356 *MD 4300A.*

1357 • *The HSIN Next Generation System shall be able to audit all user activity.*

1358 • *The HSIN Next Generation System shall be able to audit all administrative activity.*

1359 • *The HSIN Next Generation System shall have the ability to track which users have accessed*
1360 *selected content material.*

1361 • *The HSIN next Generation System shall provide the capability for intelligence analysis of*
1362 *audit records.*

1363 • *The HSIN Next Generation System shall provide an auditing mechanism that can handle*
1364 *process flows across multiple services.*

1365 • *The HSIN Next Generation System shall provide an end-to-end audit trail of all services*
1366 *accessed across the business processes.*

1367 • *The HSIN Next Generation System shall provide account audits to include entry points.*

1368 • *The HSIN Next Generation System shall be able to audit all of the changes made to any*
1369 *portal content accessed through the system.*

1370 • *The HSIN Next Generation System shall allow the end-users to refuse any or all cookies*
1371 *without affecting the basic usability of the system.*

1372 • *The HSIN Next Generation System shall provide authorized users the ability to retrieve and*
1373 *review system audit logs.*

1374 • *The HSIN Next Generation System shall provide an audit history for the posting of all content*
1375 *to the system.*

1376 • *The HSIN Next Generation System shall retain audit logs as required in subsection 3.2.5,*
1377 *Data Retention.*

1378

1379 **3.1.5 Reporting**

1380 The reporting requirements for the HSIN Next Generation System are listed below:

1381

1382 • *The HSIN Next Generation System shall allow authorized end-users to build complex or*
1383 *simple system queries.*

1384 • *The HSIN Next Generation System shall have the capability to store a report generation*
1385 *query and presentation templates for repeated execution.*

1386 • *The HSIN Next Generation System shall restrict access to saved report queries to approved*
1387 *users or groups of users.*

1388 • *The HSIN Next Generation System shall have the ability to generate and view a report of*
1389 *content based on metadata elements.*

1390 • *The HSIN Next Generation System shall allow the user to access the content directly from the*
1391 *report.*

- 1392 • *The HSIN Next Generation System shall be capable of integrating with external commercial*
1393 *reporting tools that allow analysis and representation of results graphically.*
- 1394 • *The HSIN Next Generation System shall provide configurable reporting functions to end-*
1395 *users across all repositories with forms of content that can be restricted by security and access*
1396 *rights.*
- 1397 • *The HSIN Next Generation System shall provide the report design capability for users to*
1398 *create and build customized reports.*
- 1399 • *The HSIN Next Generation System shall allow end-users to add graphs, bitmaps or tables to*
1400 *the reports.*
- 1401 • *The HSIN Next Generation System shall allow for sharing of reports among a specified*
1402 *workgroup, user(s) or all system.*
- 1403 • *The HSIN Next Generation System shall allow previewing of a report before printing.*
- 1404 • *The HSIN Next Generation System shall allow for batch scheduling of reports.*
- 1405 • *The HSIN Next Generation System shall automatically attach reports and distribute via each*
1406 *to specified end-users.*
- 1407 • *The HSIN Next Generation System shall report on all data (users, privileges, metadata*
1408 *schemas, workflows, reports, queries, versions, etc)..*
- 1409 • *The HSIN Next Generation System shall provide an ad-hoc reporting facility to allow users to*
1410 *specify parameters and produce reports based on the contents of any selection of the information*
1411 *made available by any portals.*
- 1412 • *The HSIN Next Generation System shall allow end-users to add text equivalents for graphs,*
1413 *bitmaps including row, column and table header tags to tables to reports.*
1414

1415 **3.2 Infrastructure**

1416 The HSIN Next Generation System infrastructure will be built to support the mission needs of DHS and
1417 the COIs. The infrastructure must support availability, reliability, maintainability and survivability
1418 performance requirements. To ensure greater stability and recovery in the event of an incident the HSIN
1419 Next Generation System infrastructure will be redundant and geographically diverse between the primary
1420 and backup sites.
1421

1422 The HSIN Next Generation System infrastructure will consist of heterogeneous, distributed resources
1423 based on COTS hardware and software components. Within the context of this document the
1424 infrastructure includes physical components required to host and facilitate communication between users
1425 of the software components. Infrastructure also includes providing the resources to host applications
1426 developed for HSIN Next Generation users.
1427

1428 The infrastructure requirements for the HSIN Next Generation System are listed below:
1429

- 1430 • *The HSIN Next Generation System shall have an enhanced backup/restore mechanism which*
1431 *will allow the restoration of all system components.*
- 1432 • *The HSIN Next Generation System shall be physically hosted at DHS Data Center, which*
1433 *include Government owner, Government operated, and contractor owned and contractor operated,*

1434 at no less than two geographically-separated data centers. (The locations of these geographically-
1435 separated data centers shall be at the sole discretion of DHS).

1436 • The HSIN Next Generation System shall provide an Open API capability.

1437 • The HSIN Next Generation System shall provide a database interface capability.

1438 • *HSIN Next Generation System shall deliver a developed and tested low bandwidth version of*
1439 *the Next Generation HSIN System.*
1440

1441 **3.2.1 Availability, Reliability, and Maintainability**

1442 Operational availability of minimal essential sustained and survivable mission capability for the HSIN
1443 Next Generation System is a primary factor in the performance criteria. The systems must be available
1444 and at all times, including when the national infrastructure is stressed or degraded and shall support full
1445 capability during Continuity of Operation Plan (COOP) Plan conditions. Therefore, it is essential that the
1446 Next Generation System exhibit high, measurable availability and reliability, and consistent performance.
1447

1448 **3.2.1.1 Availability**

1449 HSIN is considered operational when users can successfully log-on to any COI site, access the COP, and
1450 can collaborate and communicate via one or more of the following methods: instant messaging, alerts,
1451 and discussion groups. The following definitions provide additional details regarding the severity of
1452 outages that impact operational availability. These definitions are currently used to categorize HSIN
1453 system severity levels.
1454

1455 **Catastrophic Failure:** An incident that causes total loss of all HSIN services. Users are prevented from
1456 performing tasks necessary for mission critical operations. Failure requires immediate resolution as the
1457 complete system cannot be used until the repair has been made.

1458 **Failure:** An incident that causes total loss of functionality for one of the HSIN services and severely
1459 affects system use. The problem is of a time-sensitive nature. While it does not cause a complete work
1460 stoppage, no workaround is available and operational activities can only continue in a restricted fashion.
1461 Alternatively, it may be a "critical failure" for which a customer-acceptable workaround exists.

1462 **Issue:** An incident during which the system is operational but one or more components are operating
1463 differently than expected. It does not result in a failure, but causes the system to produce incorrect,
1464 incomplete, or inconsistent results, or impairs system usability.

1465 **Incident:** A defect that causes system degradation or loss of non-critical business functionality. This
1466 includes degradation of expected system response times for a particular tool to the extent that operational
1467 activities suffer. The defect does not cause a failure or impair usability, and the desired processing results
1468 are easily obtained by working around the defect.

1469 **Routine Problem:** A problem that is commonly resolved within the span of a Help Desk call or quickly
1470 resolved following the call. If there is a defect, it is the result of non-conformance to a standard, related
1471 to the aesthetics of the system, or a request for an enhancement. A defect at this level may be deferred or
1472 even ignored at the discretion of DHS. It can be resolved in a future system update or not at all.
1473

1474 The availability requirements for the HSIN Next Generation System are listed below:

1475 • *The HSIN Next Generation System shall meet an operational availability of 99.99%*
1476 *throughout the calendar year.*
1477
1478

1479 **3.2.1.2 Reliability**

1480 The HSIN infrastructure will maintain reliability during peak demand or periods of stress. Vendors have
1481 the flexibility to distribute the HSIN Next Generation System load across sites; however, this peak
1482 volume demand (or multiple national level events) does *not* in any way alleviate the system's reliability
1483 requirements.

1484
1485 The reliability requirements for the HSIN Next Generation System are listed below:

- 1486
1487 • The HSIN Next Generation System shall function such that failure or removal of any
1488 component or item in the system does not cause a failure to any other component(s) or item(s).

1489
1490 **3.2.1.3 Maintainability**

1491 Maintenance and support concepts and requirements need to be developed and established as early as
1492 possible during system design and development, including accessibility, diagnostics, repair, and sparing
1493 for all maintenance levels. Maintenance includes Operational and Depot Levels, with Intermediate Level
1494 Maintenance included, if applicable. Requirements for manpower factors that impact system design, such
1495 as maintenance ratios, will be identified during an early phase.

1496
1497 Repair and maintenance criteria need to be established for all applicable levels in terms of time, accuracy,
1498 built-in-test, testability, availability, reliability, maintainability, support equipment requirements
1499 (including automatic test equipment), and manpower skills, knowledge and abilities. Software
1500 maintenance includes, but may not be limited to, source, maintainability, recoverability coding, and
1501 transition planning. Life-cycle cost will play a key role, and support/maintenance concepts will
1502 incorporate a balance between readiness and life-cycle cost.

1503
1504 The maintainability requirements for the HSIN Next Generation System are listed below:

- 1505
1506 • The HSIN Next Generation System shall be configured to allow the removing, repairing, and
1507 replacing equipment without the need to remove additional system equipment.
- 1508 • The HSIN Next Generation System shall allow tool and application updating without a
1509 change of infrastructure.

1510
1511 **3.2.2 Survivability**

1512 The HSIN Next Generation System will remain operational during and following a system or
1513 environmental disturbance. This requires resources reconstituted in time or failover in place.

1514
1515 The survivability requirements for the HSIN Next Generation System are listed below:

- 1516
1517 • *The HSIN Next Generation System shall exhibit failover redundant data systems within 60*
1518 *seconds of a component failure with no loss of stored data.*
- 1519 • The HSIN Next Generation System shall maintain COOP functionality in support of a
1520 minimum of three concurrent national level events.

1521

1522 **3.2.3 Performance**

1523 The HSIN Next Generation System performance requirements describe the functional capability and user
1524 capacity of the system. The capabilities and user capacity help define characteristics of the system that
1525 support the mission and other major functional areas.

1526
1527 The performance requirements for the HSIN Next Generation System are listed below:
1528

1529 **Note:** The time requirements below do not consider network latency, due to that being dependent upon
1530 the users connection and is out of the systems control.

- 1531
- 1532 • *The HSIN Next Generation System shall distribute and/or support the distribution of key*
1533 *information to the end-users within 30 minutes of request for key information.*
 - 1534 • *The HSIN Next Generation System shall update posted content with changes within (1)*
1535 *minute of being posted by the end- user.*
 - 1536 • *The HSIN Next Generation System shall have a page render time of (10) seconds.*
 - 1537 • The HSIN Next Generation System shall provide search results in (15) seconds.
 - 1538 • The HSIN Next Generation System shall process user login in (10) seconds.
 - 1539 • The HSIN Next Generation System shall make available content within one (1) minute of
1540 being posted by the end-user.
 - 1541 • The HSIN Next Generation System shall make available decisions within fifteen (15) minutes
1542 of being entered by a user. (**Note:** A decision is defined as any communication to the user in the
1543 form of alerts, files, reports, or other content types).
 - 1544 • The HSIN Next Generation System shall provide synchronous services to consumers at the
1545 time that they are requested (i.e., the services must be up and running).
1546

1547 **3.2.4 Scalability**

1548 The HSIN Next Generation will be designed to facilitate consistent and graceful expansion. The system
1549 will be capable of maintaining momentum on Federal, State, Local, Tribal, Territorial, Private Sector and
1550 International partners subscription expansion.

1551
1552 The scalability requirements for the HSIN Next Generation System are listed below:
1553

- 1554 • The HSIN Next Generation System shall be able to sustain normal DHS operations during
1555 three concurrent national level events.
- 1556 • *The HSIN Next Generation System shall support at least two million unique user accounts.*
- 1557 • *The HSIN Next Generation System shall support at least 120,000 concurrent, active users.*
1558

1559 **3.2.5 Data Retention**

1560 The OPS Records Manager is working HSIN Program Management personnel to request records
1561 disposition schedules and coordination of those schedules with the National Archives and Records
1562 Administration (NARA) for the HSIN Next Generation System. In accordance with the signed Privacy
1563 Impact Assessment (PIA), dated 22 June 2007, the HSIN Next Generation System will operate in
1564 accordance with NARA guidance.

1565
1566 The general data retention requirements, based on current guidance, for the HSIN Next Generation
1567 System are listed below:

- 1568 • *The HSIN Next Generation System shall retain audit logs on-line for 90 days.*
- 1570 • *The HSIN Next Generation System shall retain audit logs off-line for 7 years.*
- 1571 • *The HSIN Next Generation System shall retain data in accordance with the retention*
1572 *schedules of each community, not to exceed on-line retention beyond 90 days and off-line*
1573 *retention beyond 7 years.*
- 1574 • *The HSIN Next Generation System shall provide the capability for content to be tagged for*
1575 *review, based on content metadata fields.*
- 1576 • *The HSIN Next Generation system shall provide the capability for content to be tagged for*
1577 *retention, based on content metadata fields.*
- 1578 • *The HSIN Next Generation system shall provide the capability for content to be tagged for*
1579 *disposition, based on content metadata fields.*
- 1580

1581 **3.2.6 Usability**

1582 The HSIN Next Generation System interfaces and functions will be designed for ease-of-use at all levels.
1583 All functionality and toolsets offered through the HSIN Next Generation system will be accessible to all
1584 users.

1585
1586 The usability requirements for the HSIN Next Generation System are listed below:

- 1587 • The HSIN Next Generation System shall provide page identification at the top of each page
1588 within the portal.
- 1589 • The HSIN Next Generation System shall provide “breadcrumbs” during system navigation to
1590 allow users to track where they are in the system hierarchy at all times.
- 1591 • The HSIN Next Generation System navigational breadcrumbs shall be active hyperlinks to
1592 facilitate navigation between pages.
- 1593 • The HSIN Next Generation System shall be display-configurable to allow for different
1594 resolutions on user workstation desktops.
- 1595 • The HSIN Next Generation System shall be display-configurable to allow for use preferences
1596 for fonts and colors on user workstation desktops.
- 1597 • The HSIN Next Generation System shall provide detailed context-sensitive error messages.
- 1598 • The HSIN Next Generation System shall provide an easily recognizable logout button to
1599 enable a quick and graceful exit from the system.
- 1600 • The HSIN Next Generation System shall provide HSIN online user guides.
- 1601 • The HSIN Next Generation System shall provide tutorials, context sensitive help files (web-
1602 based/indexed/searchable), user guide (printable), feedback mechanisms, password reset process,
1603 and Frequently Asked Questions (FAQs).
- 1604 • The HSIN Next Generation System shall provide a system Help page.
- 1605 • The HSIN Next Generation System shall provide administrative tools.
- 1606

- 1607 • The HSIN Next Generation System shall provide a link to the homepage that is available to
1608 the user at all times.
- 1609 • The HSIN Next Generation System shall provide a context-sensitive help link that is
1610 available to the user at all times.
- 1611 • *The HSIN Next Generation System shall allow users to view author of each page/community/
1612 portal.*
- 1613 • The HSIN Next Generation System shall allow users to create communities/events
1614 automatically.
1615

1616 3.3 Interoperability / Integration

1617 The HSIN Next Generation system will be the hub connecting the DHS community and their information
1618 sharing networks and applications for all Federal, State, Local, Tribal, Territorial, Private Sector and
1619 International partners engaged in preventing, protecting from, responding to and recovering from all
1620 threats, hazards and incidents within the authority of DHS. Interoperability and system integration is a
1621 key component to the realization of such a connection. There are several allied networks and programs
1622 that serve, support, or leverage HSIN for the COIs.

1623 The interoperability/integration requirements for the HSIN Next Generation System are listed below:
1624

- 1625 • *The HSIN Next Generation System shall be interoperable with all DHS agencies SBU
1626 networks, at the same security level or below.*
- 1627 • *The HSIN Next Generation System shall be interoperable with the U.S. Community
1628 Emergency Response Team.*
- 1629 • The HSIN Next Generation System shall serve as a host platform to the COP application.
- 1630 • The HSIN Next Generation System shall provide data to the COP application.
- 1631 • The HSIN Next Generation System shall be interoperable with Department of Justice (DoJ)
1632 systems that provide information sharing that aligns with HSIN objectives.
- 1633 • The HSIN Next Generation System shall be interoperable with the National Infrastructure
1634 Coordination Center (NICC) systems that provide information sharing that aligns with HSIN
1635 objectives.
1636
- 1637 • The HSIN Next Generation System shall be interoperable with the NPPD systems that
1638 provide information sharing that aligns with HSIN objectives.
- 1639 • *The HSIN Next Generation System shall support Security Assertions Markup Language
1640 (SAML) 2.0 in order to interoperate with other systems.*
- 1641 • The HSIN Next Generation System shall be interoperable with systems of other Federal
1642 agencies that share the same technology standards as HSIN.
- 1643 • The HSIN Next Generation System shall be capable of sharing situational data with a GIS
1644 tool.
- 1645 • *The HSIN Next Generation System shall provide workflow capability for disparate HSIN
1646 communities to submit and vet data.*
- 1647 • The HSIN Next Generation System shall be accessible from any encryption-capable web
1648 browser.

- 1649 • The HSIN Next Generation System shall be Internet Protocol, version 6 (IPv6)
1650 compatible/compliant.
- 1651 • The HSIN Next Generation System shall allow all authorized users to log onto the system
1652 from any internet-accessible computer.
- 1653 • The HSIN Next Generation System shall use a communication channel to interoperate with
1654 external systems. The channel shall be independent of the technology used by either system.
- 1655 • *The HSIN Next Generation System shall be able to provide data to Homeland Secure Data
1656 Network (HSDN).*
- 1657 • *The HSIN Next Generation System shall provide a way to assure external systems and users
1658 that it is authentically the HSIN Next Generation System.*
- 1659 • *The HSIN Next Generation System shall comply with the Electronic Mail Server Standards of
1660 the DHS Enterprise Portal Standards List.*
- 1661 • *The HSIN Next Generation System shall comply with the Web Server Standards of the DHS
1662 Enterprise Portal Standards List.*
- 1663 • *The HSIN Next Generation System shall comply with the Application Server Standards of the
1664 DHS Enterprise Portal Standards List.*
- 1665 • *The HSIN Next Generation System shall comply with the Database Access Service Standards
1666 of the DHS Enterprise Portal Standards List.*
- 1667 • *The HSIN Next Generation System shall comply with the Security Standards of the DHS
1668 Enterprise Portal Standards List.*
1669

1670 **3.4 Regulations and Compliance**

1671 Information coordination referred below includes information gathering, processing, dissemination,
1672 sharing and archiving and all other record management practices involving information maintained and
1673 exchanged through the HSIN Next Generation System.

1674
1675 The regulation and compliance requirement for the HSIN Next Generation System is listed below:

- 1676
1677 • *The HSIN Next Generation System shall be compliant with the Code of Federal Regulations
1678 (CFR) Part 23.*
- 1679 • *The HSIN Next Generation System shall be compliant with the Homeland Security Enterprise
1680 Architecture (HLS EA), February 2007.*
- 1681 • *The HSIN Next Generation System hardware or software shall be compliant with the HLS EA
1682 Technical Reference Model (TRM) Standards and Products Profile.*
- 1683 • *The HSIN Next Generation System shall be compliant with the Assessment of The Policy and
1684 Strategy Framework for the HSIN, dated 25 October 2006.*
1685

1686 **3.4.1 Legal Compliance**

1687 The HSIN Next Generation System users involved in the information coordination process discussed
1688 below are subject to the Federal, State, Local, Tribal, Territorial, Private Sector and International
1689 government information management, privacy, public disclosure (or “sunshine”) statutes and regulations
1690 of their jurisdictions. Compliance with all applicable laws and regulations is a non-delegable

1691 responsibility of individual users and the agencies to which they belong. Some representative examples
1692 of the types of statutes and regulations applicable include, but are not limited to: 5 U.S.C. Part 552, The
1693 Freedom of Information Act; 5 U.S.C. Part 552b, The Privacy Act of 1974 (as amended); 28 C.F.R. Part
1694 23, Criminal Intelligence System Operating Policies; Executive Order 12333, United States Intelligence
1695 Activities, amended by Executive Order 13355 27 Aug 04; and DoD 5240.1, DoD Intelligence Activities
1696 that Affect United States Persons. These laws and regulations are only applicable to the extent that they
1697 apply to a particular agency, entity or individual using the HSIN Next Generation.
1698

1699 The HSIN Next Generation System communities provided for the exclusive use of the Sector
1700 Coordinating Councils (SCCs) and their designees may only be used for purposes authorized by the
1701 United States Government in conjunction with the SCC, which serves as exclusive proprietary owner and
1702 steward of the information residing within those HSIN Next Generation System communities. The
1703 Government may monitor and audit the usage of the SCC communities to ensure the security of the
1704 network and to prevent its use for any purpose that constitutes a violation of law. Use of SCC HSIN Next
1705 Generation System communities and the information contained therein is governed by the procedures and
1706 requirements of the respective SCCs.
1707

1708 **3.4.2 HSIN Third-Party Rule**

1709 Information reported or posted by a Federal, State, Local, Tribal, Territorial, Private Sector and
1710 International partners may be coordinated among the applicable communities to which it was reported or
1711 posted, but remains in the "custody and exclusive control" of the source submitter. Such information is
1712 subject to limitations on use/dissemination imposed by the reporting/posting source privacy and
1713 information release requirements imposed by law or regulatory policy.
1714

1715 The HSIN Third-Party Rule requirement for the HSIN Next Generation System is listed below:

- 1716 • *The HSIN Next Generation System shall release data among sectors upon receipt of an*
1717 *indication that the data owner (such as a COI) has deemed it releasable.*
1718
1719

1720 **3.4.3 Protection of Privacy and Proprietary Information**

1721 Other than the Federal, State, Local, Tribal, Territorial, Private Sector and International partner users that
1722 are directly subject to the privacy and information requirements imposed by the laws and policies of their
1723 jurisdictions, no HSIN Next Generation System user shall be afforded access to privacy or proprietary
1724 record information obtained within the HSIN Next Generation System. Private sector information which
1725 may be proprietary or otherwise sensitive will be managed in compliance with all security and
1726 safeguarding provisions imposed by law and/or as agreed upon between the applicable private sector
1727 entities and the source agency.
1728

1729 The HSIN Next Generation System will enable users to indicate whether the information contains any
1730 personally identifiable information. All data assets and information exchanges that contain personally
1731 identifiable information will be submitted to the DHS Privacy Office for review and approval for privacy
1732 compliance, including the Privacy Act, E-Government Act, Homeland Security Act, and DHS Privacy
1733 Policies prior to inclusion in HSIN.
1734

1735 The Protection of Privacy and Proprietary Information requirement for the HSIN Next Generation System
1736 is listed below:

- 1737 • *The HSIN Next Generation System shall provide protection for privacy or proprietary record*
1738 *information obtained within the system from unauthorized users.*
1739

- 1740 • The HSIN Next Generation System shall audit the actual use of Personally Identifiable
1741 Information (PII) to demonstrate compliance with all of the applicable principles and privacy
1742 protection requirements.
- 1743 • *The HSIN Next Generation System shall comply with the Federal Information Security*
1744 *Management Act (FISMA).*
- 1745 • *The HSIN Next Generation System shall comply with the National Institute of Standards and*
1746 *Technology (NIST) FIPS.*
- 1747 • *The HSIN Next Generation System shall comply with the E-Government Act of 2002.*
- 1748 • *The HSIN Next Generation System shall comply with the OMB Circular A-11.*
- 1749 • *The HSIN Next Generation System shall comply with the NIST 800-60.*
- 1750 • *The HSIN Next Generation System shall comply with the Code of Federal Regulations 6 CFR*
1751 *Part 5, Subpart B, Privacy Act.*
- 1752 • *The HSIN Next Generation System shall comply with DHS Management Directive (MD)*
1753 *0470.1.*
- 1754 • *The HSIN Next Generation System shall be able to identify Personally Identifiable*
1755 *Information (PII) either through automated means or through user action.*
- 1756 • *The HSIN Next Generation System shall be able to identify by both by specific user and*
1757 *user groups who has accessed, amended, distributed, or deleted each piece of PII.*
- 1758 • *The HSIN Next Generation System shall be able to lock user accounts, if privacy*
1759 *training has not been completed within one year.*
- 1760 • *The HSIN Next Generation System shall be able to track who and when the inclusion of*
1761 *new datasets that contain PII was approved.*
1762

1763 **Disclaimer:** The compliance policies and rules concerning information coordination are not intended to
1764 create or confer any right, privilege or benefit to any private person including any person in litigation with
1765 the United States or any agency or individual using the HSIN Next Generation System.
1766

1767 **3.4.4 Accessibility**

1768 Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended, requires that when Federal agencies
1769 develop, procure, maintain or use electronic and information technology (EIT), they must ensure that it is
1770 accessible to people with disabilities. Federal employees and members of the public who have disabilities
1771 must have access to and use of information and services that are comparable to the access and use
1772 available to non-disabled Federal employees and members of the public.
1773

1774 The accessibility requirements for the HSIN Next Generation System were derived from the DHS MD
1775 4010.2, Section 508 Program Management Office & Electronic and Information Technology
1776 Accessibility, dated 26 October 2005.
1777

1778 The accessibility requirements for the HSIN Next Generation System are listed below:
1779

1780 DHS has identified the following applicable standards from the Electronic and Information
1781 Technology Accessibility Standards (Section 508) *36 CFR 1194.31*: Functional Performance Criteria

- 1782 • *The HSIN Next Generation System shall provide at least one mode of operation and*
1783 *information retrieval that does not require user vision, or support for assistive technology used*
1784 *by people who are blind or visually impaired shall be provided.*
- 1785 *Note: This includes full keyboard-only access for all functions of the system.*
- 1786 • *The HSIN Next Generation System shall provide at least one mode of operation and*
1787 *information retrieval that does not require visual acuity greater than 20/70 that must be in audio*
1788 *and enlarged print output working together or independently, or support for assistive technology*
1789 *used by people who are visually impaired shall be provided.*
- 1790 • *The HSIN Next Generation System shall provide at least one mode of operation and*
1791 *information retrieval that does not require user hearing, or support for assistive technology used*
1792 *by people who are deaf or hard of hearing.*
- 1793 • *The HSIN Next Generation System shall provide, where audio information is important for*
1794 *the use of the product, at least one mode of operation and information retrieval in an enhanced*
1795 *auditory fashion, or support for assistive hearing devices.*
- 1796 • *The HSIN Next Generation System shall provide at least one mode of operation and*
1797 *information retrieval that does not require user speech, or support for assistive technology used*
1798 *by people with disabilities.*
- 1799 • *The HSIN Next Generation System shall provide at least one mode of operation and*
1800 *information retrieval that does not require fine motor control or simultaneous actions and that is*
1801 *operable with limited reach and strength.*
- 1802 • *The HSIN Next Generation System shall provide support for assistive technology such as*
1803 *tracking focus, providing user-controlled keyboard or automatic navigation (focus control) to*
1804 *updated content, to ensure the updated information is available to users who are blind or have*
1805 *low vision disabilities comparable to access by users without disabilities.*
- 1806
- 1807 DHS has identified the following applicable standards from the Electronic and Information
1808 Technology Accessibility Standards (Section 508) 36 CFR 1194.22: Web-based intranet and internet
1809 information and applications
- 1810 • *The HSIN Next Generation System shall present a text equivalent for every non-text element*
1811 *(e.g., via "alt", "longdesc", or in element content).*
- 1812 • *The HSIN Next Generation System shall support the capabilities to synchronize equivalent*
1813 *alternatives for any multimedia presentation with the presentation.*
- 1814 *Note: All Web-based multimedia must also comply with the item 5 ("Video and Multimedia*
1815 *Technical Requirements") of the matrix in the MD 4010.2 Section 508 Program Management*
1816 *Office & Electronic and Information Technology.*
- 1817 • *The HSIN Next Generation System shall present Web pages such that all information*
1818 *conveyed with color is also available without color, for example from context or markup.*
- 1819 • *The HSIN Next Generation System shall provide the ability to organize documents so they are*
1820 *readable without requiring an associated style-sheet.*
- 1821 • *The HSIN Next Generation System shall present data tables in such a way that identifies the*
1822 *row and column headers for data tables.*

- 1823 • *The HSIN Next Generation System shall present markup to associate data cells and header*
1824 *cells for data tables that have two or more logical levels of row or column headers.*
- 1825 • *The HSIN Next Generation System shall provide the ability to title all frames with text that*
1826 *facilitates frame identification and navigation.*
- 1827 • *The HSIN Next Generation System shall support the ability for all pages to be designed to*
1828 *avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55Hz.*
- 1829 • *The HSIN Next Generation System shall use a standard interface that is accessible to both*
1830 *users with and without disabilities with rare exception.*
- 1831 *Note: Upon rare exception with DHS approval, providing a text-only page with equivalent*
1832 *information or functionality may be permitted to make a web site accessible, when accessibility*
1833 *and conformance of this requirement cannot be accomplished in any other way.*
- 1834 • *The HSIN Next Generation System shall ensure that the content of the text only page shall be*
1835 *updated whenever the primary page changes.*
- 1836 • *The HSIN Next Generation System shall provide the capabilities for the information provided*
1837 *by the script to be identified with functional text that can be read by assistive technology.*
- 1838 • *The HSIN Next Generation System shall allow users to use assistive technology to access the*
1839 *information, field elements, and functionality required for completion and submission of*
1840 *electronic forms that are designed to be competed on-line, including all directions and cues.*
- 1841 • *The HSIN Next Generation System shall provide a method that permits users to skip*
1842 *repetitive navigation links.*

1843

1844 DHS has identified the following applicable standards from the Electronic and Information
1845 Technology Accessibility Standards (Section 508) 36 CFR 1194.41: *Information, Documentation,*
1846 *and support*

- 1847 • *The HSIN Next Generation System shall provide Web-based (HTML) product training, support*
1848 *and help documentation to the end users identified in 36 CFR 1194.31 (Functional Performance*
1849 *Criteria) of the MD 4010.2 Section 508 Program Management Office & Electronic and*
1850 *Information Technology, which must comply with the 36 CFR 1194.22 (Web-based Technical*
1851 *Requirements) of the MD 4010.2 Section 508 Program Management Office & Electronic and*
1852 *Information Technology.*
- 1853 • *The HSIN Next Generation System shall provide support services for products that accommodate*
1854 *the communication needs of end-users with disabilities.*

1855

1856 DHS has identified the following applicable standards from the Electronic and Information
1857 Technology Accessibility Standards (Section 508) 36 CFR 1194.21: *Software Applications and*
1858 *operating systems*

- 1859 • *The HSIN Next Generation System shall support the ability for product functions to be executable*
1860 *from a keyboard where the function itself or the result of performing a function can be discerned*
1861 *textually.*
- 1862 • *The HSIN Next Generation System shall provide/use applications that do not disrupt or disable*
1863 *activated features of other products that are identified as accessibility features, where those*
1864 *features are developed and documented according to industry standards.*

- 1865
- 1866
- 1867
- 1868
- *The HSIN Next Generation System shall provide/use applications that do not disrupt or disable activated features of any operating system that are identified as accessibility features where the application programming interface for those accessibility features has been documented by the manufacturer of the operating system and is available to the product developer.*
- 1869
- 1870
- *The HSIN Next Generation System shall provide a well defined on-screen indication of the current focus that moves among interactive interface elements as the input focus changes.*
- 1871
- 1872
- 1873
- *The HSIN Next Generation System shall provide a well defined on-screen indication of the current focus that is programmatically exposed so that assistive technology can track focus and focus changes.*
- 1874
- 1875
- *The HSIN Next Generation System shall provide sufficient information about the user interface including the identity, operation and state of the element to assistant technology.*
- 1876
- 1877
- *The HSIN Next Generation System shall provide the information conveyed by images representing program elements in text.*
- 1878
- 1879
- 1880
- *The HSIN Next Generation System shall provide a consistent assigned meaning of images throughout an application's performance, when bitmap images are used to identify controls, status indicators, or other programmatic elements.*
- 1881
- 1882
- 1883
- *The HSIN Next Generation System shall provide textual information through operating system functions for displaying text, which includes text content, text input caret location, and text attributes at a minimum.*
- 1884
- 1885
- *The HSIN Next Generation System shall provide applications that do not override user selected contrast and color selections and other individual display attributes.*
- 1886
- 1887
- *The HSIN Next generation System shall display animation in at least one non-animated presentation mode at the option of the user.*
- 1888
- 1889
- *The HSIN Next generation System shall convey information that indicates an action, prompts a response, or distinguishes a visual element, without the use of color coding.*
- 1890
- 1891
- 1892
- *The HSIN Next Generation System shall provide a variety of color selections capable of producing a range of contrast levels, for use when a product permits users to adjust color and contrast settings.*
- 1893
- 1894
- *The HSIN Next Generation System shall not use flashing or blinking text, objects or other elements having flash or blink frequency greater than 2 Hz and Lower than 55 Hz.*
- 1895
- 1896
- 1897
- DHS has identified the following applicable standards from the Electronic and Information Technology Accessibility Standards (Section 508) 36 CFR 1194.24: *Video and multimedia products.*
- 1898
- 1899
- 1900
- *The HSIN Next Generation System shall provide the ability for open or closed caption for any multimedia, regardless of format that contain speech or other audio information necessary for the comprehension of the content.*
- 1901
- 1902
- 1903
- Note: For the purposes of this requirement, closed or open captioning will mean the inclusion of synchronized equivalent text embedded within a presentation that permits user selectable controls to turn the feature on-off unless permanent.*
- 1904
- 1905
- 1906
- *The HSIN Next Generation System shall support audio described for any multimedia, regardless of format that contain speech or other audio information necessary for the comprehension of the content.*

- 1907
1908
1909
- *The HSIN Next Generation System shall allow the end-users to select the display or presentation of alternate text presentation or audio descriptions, unless permanent.*

1910 **3.5 Quality Measurement and Monitoring**

1911 The HSIN Next Generation System will be able to monitor and evaluate its effectiveness to satisfy user
1912 needs. The system will capture and generate meaningful reports of statistical metrics. These reports will
1913 be dynamic and configurable and shall be accessible to all authorized users. Formal systemic measures of
1914 usage, health and content will be an integral component of the HSIN Next Generation System.

1915
1916 The quality measurement and monitoring requirements for the HSIN Next Generation System are listed
1917 below:

- 1918
1919
1920
- The HSIN Next Generation System shall provide measurement, storage, and reporting of usage, health and content statistics on a periodic basis as specified by an authorized user.
 - *The HSIN Next Generation System shall provide metrics on demand, when requested by an authorized user.*
 - The HSIN Next Generation System shall generate detailed statistical reports.
 - *The HSIN Next Generation System shall time-tag all portal transactions.*
 - The HSIN Next Generation System shall provide statistics concerning portal usage.
 - The HSIN Next Generation System shall provide a dashboard for metrics.
 - *The HSIN Next Generation System shall provide business intelligence or other tools to graphically depict metrics.*
- 1921
1922
1923
1924
1925
1926
1927
1928

1929

1930 **3.5.1 User and Usage Metrics**

1931 User and usage metrics characterize how the end-users are interacting with the HSIN Next Generation
1932 System.

1933
1934 The user and usage metrics requirements for the HSIN Next Generation System are listed below:

- 1935
1936
1937
- The HSIN Next Generation System shall provide user metrics defining the number, type, specific permissions granted and current state of user accounts.
 - The HSIN Next Generation System shall track these metrics to provide snapshots of the health and activity of the system's user base.
 - The HSIN Next Generation System shall provide usage metrics to track the number of documents created, the number and percentage of documents shared, and the number and percentage of documents unused.
 - The HSIN Next Generation System shall provide daily average unique user metric.
 - The HSIN Next Generation System shall provide number of users metric.
 - *The HSIN Next Generation System shall provide user and usage metrics, which will be available to owners or administrators directly on the page.*
- 1938
1939
1940
1941
1942
1943
1944
1945
1946
1947

1948 **3.5.2 System Health Metrics**

1949 System health metrics will describe and characterize the operational state of the HSIN Next Generation
1950 System.

1951
1952 The system health metrics requirements for the HSIN Next Generation System are listed below:

- 1953
- 1954 • The HSIN Next Generation System's health metrics shall be tailored to allow system
1955 administrators to quickly discern any significant degradation of the system's infrastructure.
- 1956 • The HSIN Next Generation System's health metrics shall record and make available the
1957 unplanned system downtime in hours for any of the services provided by the HSIN Next
1958 Generation System.
- 1959 • The HSIN Next Generation System's health metrics shall record and make available the
1960 average number of hours to resolve emergency service requests for any of the services provided
1961 by the HSIN Next Generation System.
- 1962 • The HSIN Next Generation System shall provide system health metrics including uptime,
1963 downtime, data throughput, number of concurrent users, throughput rates and mean time between
1964 failures.
1965

1966 **3.5.3 Content Metrics**

1967 The HSIN Next Generation System will track metrics related to the subscription and access of the
1968 system's informational content. Tracking content metrics will enable system administrators to detect
1969 trends in content usage to enhance throughput for high- traffic areas.

1970
1971 The content metrics requirements for the HSIN Next Generation System are listed below:

- 1972
- 1973 • The HSIN Next Generation System shall provide content metrics describing what content is
1974 being accessed, how frequently the content is accessed and which users are accessing the content.
- 1975 • The HSIN Next Generation System shall measure the number of documents generated.
- 1976 • *The HSIN Next Generation System shall measure the number and percentage of documents*
1977 *shared.*
- 1978 • *The HSIN Next Generation System shall allow the setting of an unused document metric*
1979 *(days since last access).*
- 1980 • The HSIN Next Generation System shall measure the number and percentage of documents
1981 meeting the criteria of the unused document metric.
- 1982 • The HSIN Next Generation System shall report the number and percentage of documents
1983 meeting the criteria of the unused document metric.
- 1984 • The HSIN Next Generation System shall measure the number and percentage of documents
1985 blocked.
- 1986 • *The HSIN Next Generation shall measure the number of reports generated and disseminated*
1987 *by defined categories (e.g., COI, state, region, etc)..*
- 1988 • The HSIN Next Generation shall measure the number of Critical Infrastructure/Key Resource
1989 (CI/KR) sector assessments completed for the year by Intelligence and Analysis (I&A's)
1990 Homeland Infrastructure Threat and Risk Analysis Center (HITRAC).

- 1991 • The HSIN Next Generation System shall time-tag all data transactions.
- 1992 • The HSIN Next Generation System shall provide the amount of data storage metric.
- 1993 • The HSIN Next Generation System shall provide number of files metric.
- 1994 • The HSIN Next Generation System shall provide number of folders metric.
- 1995 • The HSIN Next Generation System shall provide content size metric.
- 1996

2003 **Appendix A: SOURCES**

- 2004
- 2005 The White House, *National Strategy for Information Sharing – Successes and Challenges In*
- 2006 *Improving Terrorism-Related Information Sharing*, October 2007
- 2007 U.S. Department of Commerce, *Federal Information Processing Standards Publication 140-2 (FIPS*
- 2008 *PUB 140-2): Security Requirements for Cryptographic Modules*, 11 January 1994
- 2009 U.S. Department of Homeland Security, “*Demo Week*,” 10-14 December 2007
- 2010 U.S. Department of Homeland Security, *DHS/OPS TOPOFF 4 Corrective Action Tracker*
- 2011 U.S. Department of Homeland Security, DHS Enterprise Architecture Center of Excellence
- 2012 (EACOE), *HSPD-12 Credentialing Program and Infrastructure*, 17 July 2007 (Microsoft
- 2013 PowerPoint slide presentation)
- 2014 U.S. Department of Homeland Security, DHS EACOE, *Immigration and Customs Enforcement*,
- 2015 November 2007 (Microsoft PowerPoint slide presentation)
- 2016 U.S. Department of Homeland Security, DHS EACOE, *Single Sign-On Project*, July 2007 (Microsoft
- 2017 PowerPoint slide presentation)
- 2018 U.S. Department of Homeland Security, *The Department of Homeland Security Acquisition*
- 2019 *Regulation (HSAR)*, 01 June 2006
- 2020 U.S. Department of Homeland Security, *The Department of Homeland Security (DHS) Internet*
- 2021 *Protocol Version 6 (IPv6) Transition Plan*, Version 1.0 (Draft), February 2007
- 2022 U.S. Department of Homeland Security, Enterprise Data Management Office, OCIO, *Data*
- 2023 *Management Portfolio*, 11 February 2007
- 2024 U.S. Department of Homeland Security, Homeland Security Information Network-Critical Sectors
- 2025 (HSIN-CS), *HSIN-CS Operations & Maintenance Statement of Work (SOW)*, 28 September 2007
- 2026 U.S. Department of Homeland Security, Homeland Security Information Network-Intel (HSIN-Intel),
- 2027 *HSIN-Intel Technical Requirements September 2007*, 09 October 2007
- 2028 U.S. Department of Homeland Security, Homeland Security Information Network Program
- 2029 Management Office (PMO), *Acquisition Program Baseline (APB) for Homeland Security*
- 2030 *Information Network (HSIN)*, Version 1.0, 28 June 2006
- 2031 U.S. Department of Homeland Security, Homeland Security Information Network Program
- 2032 Management Office (PMO), *Account Management System (AMS) Use Case*, Version 5.0, 12
- 2033 October 2007
- 2034 U.S. Department of Homeland Security, Homeland Security Information Network Program
- 2035 Management Office (PMO), *Alerts and Notification Use Case*, Version 3.0, 11 October 2007
- 2036 U.S. Department of Homeland Security, Homeland Security Information Network Program
- 2037 Management Office (PMO), *Automatic Data Ingest*, Version 1.5, 31 August 2007
- 2038 U.S. Department of Homeland Security, Homeland Security Information Network Program
- 2039 Management Office (PMO), *Bulk User Management*, Version 4.0, 12 October 2007
- 2040 U.S. Department of Homeland Security, Homeland Security Information Network Program
- 2041 Management Office (PMO), *CS Private Sectors Integration Use Case*, Version 2.0, 04 October
- 2042 2007

- 2043 U.S. Department of Homeland Security, Homeland Security Information Network Program
2044 Management Office (PMO), *Discussion Board Enhancements Use Case*, Version 1.5, 29 August
2045 2007
- 2046 U.S. Department of Homeland Security, Homeland Security Information Network Program
2047 Management Office (PMO), *Document Library Navigation Use Case*, Version 3.0, 11 October
2048 2007
- 2049 U.S. Department of Homeland Security, Homeland Security Information Network Program
2050 Management Office (PMO), *Document Management Use Case*, Version 3.0, 11 October 2007
- 2051 U.S. Department of Homeland Security, Homeland Security Information Network Program
2052 Management Office (PMO), *Feedback Mechanism Use Case*, Version 5.0, 12 October 2007
- 2053 U.S. Department of Homeland Security, Homeland Security Information Network Program
2054 Management Office (PMO), *File Sharing via Chat Use Case*, Version 1.5, 30 August 2007
- 2055 U.S. Department of Homeland Security, Homeland Security Information Network Program
2056 Management Office (PMO), *Integrated Persistent Chat Use Case*, Version 3.0, 12 October 2007
- 2057 U.S. Department of Homeland Security, Homeland Security Information Network Program
2058 Management Office (PMO), *Online Meetings Use Case*, Version 3.0, 11 October 2007
- 2059 U.S. Department of Homeland Security, Homeland Security Information Network Program
2060 Management Office (PMO), *Password Security Use Case*, Version 5.0, 12 October 2007
- 2061 U.S. Department of Homeland Security, Homeland Security Information Network Program
2062 Management Office (PMO), *Search Enhancements Use Case*, Version 3.0, 14 September 2007
- 2063 U.S. Department of Homeland Security, Homeland Security Information Network Program
2064 Management Office (PMO), *Standard Document Naming Convention Use Case*, Version 2.0, 12
2065 October 2007
- 2066 U.S. Department of Homeland Security, Homeland Security Information Network Program
2067 Management Office (PMO), *User and Jabber Directory Use Case*, Version 2.0, 12 October 2007
- 2068 U.S. Department of Homeland Security, Homeland Security Information Network Program
2069 Management Office (PMO), *Virtual Whiteboard Use Case*, Version 3.0, 11 October 2007
- 2070 U.S. Department of Homeland Security, Office of the Chief Information Officer (OCIO), *Enterprise
2071 Transition Strategy*, February 2007
- 2072 U.S. Department of Homeland Security, Office of the Chief Information Officer (OCIO), *System Life
2073 Cycle Guide*, Version 0.9, 14 December 2007
- 2074 U.S. Department of Justice, Office of Chief Information Officer, *Service Provider Requirements:
2075 Application Requirements for the Identity Federation Support*, Version 0.1, November 2007
- 2076 U.S. Department of Justice, Office of Chief Information Officer, *Law Enforcement Information
2077 Sharing Program Federated Identity Trusted Broker Pilot: Identity Provider Integration
2078 Overview - SAML*, Version 3.6, 2007
- 2079 U.S. Department of Justice, Office of Chief Information Officer, *Law Enforcement Information
2080 Sharing Program Federated Identity Trusted Broker Pilot: Service Provider Integration
2081 Overview - SAML*, Version 3.6, 2007
- 2082 "Utopia" Discussion with Theresa Phillips, 7 November 2007
- 2083

2084

Appendix B: GLOSSARY

2085

Table 2 below provides a list of defined terms pertinent to this document.

Table 2. Glossary of Terms	
Term	Definition
Alert	An alert is an incoming message sent to a user via another user, an automated response to an event, or a manual trigger. An alert will display a brief description as to why it appeared or why it was sent and will ask the user to either; confirm the alert was received or respond to the alert as described in the message. Approved users may send alerts to individual users or entire communities regarding announcements or other information.
Analysis	Analysis is the verification by evaluation using mathematical representation, experience, charts, graphs, circuit diagrams, data reduction, and/or representative data. Analysis also includes the verification of requirements under conditions (simulated or modeled) where the results are derived from the analysis of the results produced by the model.
Announcement	Announcements are notices that affect most or all users. An announcement is typically sent to all users via email, preferred medium, or posted on a common space such as a homepage or specific announcements section so that it can be easily communicated to everyone. Alerts or notifications may be sent to notify users that an announcement was released.
Architecture	Architecture refers to the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.
Assumption	An assumption is the notion that the information, standard, or requirement is generally understood or thought true. Assumptions are not tested and may not have a 100 percent chance of occurring.
Audit Trail	An audit trail is an electronic record showing who has accessed a computer system and what operations they have performed during a given period of time. Audit trails are useful both for maintaining security and for recovering lost transactions. Audit records typically result from activities such as transactions or communications by individual people, systems, accounts, or other entities. In information or communications security, information audit means a chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. Each user of the HSIN Next Generation System will be individually accountable for their actions while using the system through the integration of auditing tools.
Authentication	Authentication refers to the process of identifying an individual, usually based on a username and password. In a security context, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who they claim to be, but making no distinctions concerning the specific access rights of the individual. The HSIN Next Generation System will enforce two-factor authentication.
Authorization	Authorization is the process of granting or denying user access to a specific network resource. Most computer security systems are based on a two-step process. The first stage is authentication, which ensures that a user is who they claim to be. The second stage is authorization, which allows the user access to various resources based on the user's identity. The HSIN Next Generation System will allow single sign-on authorization (including applications and other portals) once a user is successfully authenticated.

Table 2. Glossary of Terms	
Term	Definition
Availability	<p>Availability is a system design and associated implementation protocol that ensures a certain absolute degree of operational continuity during a given measurement period. Availability refers to the ability of the user community to access the system, whether to submit new work, update, or remove existing work, or collect the results of previous work. If a user cannot access the system, it is said to be unavailable. Generally, the term "downtime" is used to refer to periods when a system is unavailable.</p> <p>The HSIN Next Generation System target operational availability is 99.99%.</p>
Cascading Style Sheet (CSS)	<p>In web development, Cascading Style Sheet is a style sheet language used to describe the presentation of a document written in a markup language. Its most common application is to style web pages written in HTML, but the language can be applied to any kind of XML document.</p> <p>CSS is used to help readers of web pages to define colors, fonts, layout, and other aspects of document presentation. It is designed primarily to enable the separation of document content (written in HTML, or a similar markup language) from document presentation (written in CSS). This separation can improve content accessibility, provide more flexibility and control in presentation characteristics, and reduce complexity and repetition in structural content.</p>
Catastrophic Failure	<p>Catastrophic failure refers to any incident that causes total loss of HSIN or its tools (e.g. Portal, Instant Messaging, AMS, databases, and mapping). Users are prevented from performing tasks necessary for mission critical operations. Failure requires immediate resolution as the complete system cannot be used until the repair has been made.</p>
Collaboration	<p>Collaboration is a structured, recursive process where two or more people work together toward a common goal (typically an intellectual endeavor that is creative in nature) by sharing knowledge, learning and building consensus.</p> <p>Collaboration is a primary component of the HSIN Next Generation System. Its architecture and functionality will encourage multiple persons working together to support the mission. This will consist of real-time communications, collaborating through discussion boards, Instant Messaging, and other innovative means of communicating with other system users.</p>
Communities of Interest (COI)	<p>Communities of interest refers to groups of collaborative users who require a shared vocabulary to exchange information in pursuit of common goals, interests, and business objectives (per the <i>National Information Exchange Model [NIEM] CONOPS</i>, October 2004).</p>
Constraint	<p>A constraint is a bound that specifies an acceptable minimum or maximum condition or requirement and are conditions outside the control of the project that limit the design or other alternatives.</p>
Content Discovery and Delivery (CDD)	<p>Within an SOA framework, CDD refers to a generally-available, searchable index of media files and other content to help users locate content on a web-enabled system.</p> <p>The HSIN Next Generation System CDD capability will provide a smart-cache method of information transport. This CDD capability facilitates the movement of content around the enterprise for rapid access, enterprise federated alerts, and transactional messaging capabilities.</p>
Context Diagram	<p>A Context diagram is the highest level view of a system. Context diagrams are typically used to display how a system interoperates at a very high level or how systems operate and interact logically. The system context diagram is a necessary tool in developing a baseline interaction between systems and actors, actors and system, or systems and</p>

Table 2. Glossary of Terms	
Term	Definition
	systems. Context diagrams show the interactions between a system and other actors with which the system is designed to face.
Data Retention	Data retention refers to the determining the retention period and archival requirements for each identifiable data entity. For historical data, it refers to determining the frequency of access and the type of data to be accessed. Data retention might also include any known backup or archiving requirements that would contribute significant network traffic (e.g., the need to implement a distributed backup from a central site).
Demonstration	Demonstration is the verification by operation, movement, and/or adjustment of the item under specific conditions to perform the design functions without recoding of quantitative data. Demonstration is typically considered the least restrictive of the verification methods.
Discussion Board	A discussion board is an Internet-based forum usually dedicated to a specific interest group. It is sometime called a bulletin board or interactive message board. The HSIN Next Generation System will provide a web forum function that enables the creation of private discussion boards. These discussion boards will be managed by administrators (or other approved users) who will be able to edit and delete threads and moderate community users. As part of the overall solution to information assurance, the threaded discussion will also feature discussion archival.
Download	To 'download' is the ability for HSIN users to be able to receive/transfer data from the HSIN Next Generation System and save/copy it to a local source, such as the user's desktop. For example, "Downloading a video from HSIN NextGen" means that a video that is currently hosted on the system is saved onto the user's local desktop, and can be accessed from the user's machine without having to be logged onto the HSIN NextGen system.
Encryption	Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text. There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption.
Enterprise Architecture (EA)	Enterprise Architecture is a strategic information asset base that defines the mission, the information required to perform the mission, and the technologies necessary to perform the mission. It also encompasses the transitional processes for implementing new technologies in response to changing mission needs (per the Federal CIO Council).
Enterprise Service Management (ESM)	Within an SOA framework, ESM refers the set of systems used to manage large numbers of remote intelligent devices via a variety of communication mechanisms. Within HSIN Next Generation, the ESM capability collects information to support monitoring and management of web services and monitoring of COI developed web services.
Functional Requirements	In systems engineering, a functional requirement defines the desired operational characteristic of a software system (or one of its components). A function is described as a set of inputs, the system behavior and outputs. Functional requirements describe what the system, process, or product/service must do in order to fulfill the related business requirement(s). Functional requirements are typically supported by non-business which are requirements that specify criteria that can be used to assess the general operational characteristics of

Table 2. Glossary of Terms	
Term	Definition
	<p>a system, rather than their specific behaviors (e.g., performance, scalability, security and usability).</p> <p>Requirements must be clear, correct, unambiguous, specific, achievable and verifiable.</p>
Homepage	<p>The homepage is the page a user arrives at after logging into a system. It serves as a point of entry to the rest of the website or system and displays user specific information and links. The homepage may also be known as the "landing page," because it is the page a user "lands" on or is re-directed to after successful login.</p> <p>In HSIN Next Generation System, users will customize the display and content of their homepage.</p>
Incident	<p>An incident is any action or defect that causes system degradation or loss of non-critical business functionality. This includes degradation of expected system response times for a particular tool to the extent that operational activities suffer. The defect does not cause a failure or impair usability, and the desired processing results are easily obtained by working around the defect.</p>
Information Management	<p>Information management refers to the collection and management of information from one or more sources and the distribution of that information to one or more audiences. This sometimes involves those who have a stake in, or a right to that information. Management means the organization of and control over the structure, processing and delivery of information.</p> <p>For the specific mission purposes of the HSIN Next Generation System, content management is the collection and dissemination of either raw or processed data for the operational use of COI members and the various analytical COIs. The HSIN Next Generation System's content management capabilities will support bulk content management operations such as upload and download. Integrated content metadata extraction is required to ease content organization within the HSIN Next Generation System environment for all content (including bulk content) operational transactions.</p>
Information Technology (IT)	<p>Information technology refers to any equipment, or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the executive agency. This includes equipment used by a Component directly, or used by a contractor under a contract with the Component, which (a) requires the use of such equipment; or (b) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.</p> <p>The term "IT" also includes computers, ancillary equipment, infrastructure, software, firmware, services (including support services), and related resources.</p>
Infrastructure (system-specific)	<p>Infrastructure refers to the basic, underlying framework and features of any automated system. The term infrastructure typically includes the component system installations that form the basis of any operational system. Infrastructure also encompasses the basic support services for computing as well—particularly national networks.</p> <p>The HSIN Next Generation System's infrastructure will inherently support all of its defined availability, reliability, maintainability, and survivability performance requirements. To ensure greater stability and recovery in the event of an incident, the system's infrastructure will be redundant and geographically diverse between the primary and backup sites.</p>

Table 2. Glossary of Terms	
Term	Definition
Inspection	Inspection is the verification by examination of the item, reviewing descriptive documentation, and comparing the appropriate characteristics with a predetermined standard to determine conformance to requirements without the use of special laboratory equipment or procedures.
Instant Messaging (IM)	<p>Instant messaging is a form of real-time communication between two or more people based on typed text. The text is conveyed via computers connected over a network such as the Internet. Instant messaging offers real-time communication and allows easy collaboration. Instant messaging allows instantaneous communication between a multiple parties simultaneously by transmitting information quickly and efficiently, featuring immediate receipt of acknowledgement or reply.</p> <p>This FRD defines a full set of IM directory requirements for the HSIN Next Generation System.</p>
Interoperability (system-specific)	<p>Interoperability refers to the ability of systems or functional units thereof to provide data, information, materiel, and services to (and accept the same from) other systems or units. The term also denotes use of the data, information, interfaces, materiel and services so exchanged to enable these systems/units to operate effectively together.</p> <p>The HSIN Next Generation System will be the hub connecting the DHS community and their information sharing networks and applications. There are several allied networks and programs that serve, support, or leverage HSIN for the COIs. These include the HSIN/United States Computer Emergency Readiness Team (US-CERT) and the legacy COP application.</p>
Issue	An issue is any incident during which the system is operational but one or more components are operating differently than expected. It does not result in a failure, but causes the system to produce incorrect, incomplete, or inconsistent results, or impairs system usability.
Login Page	The login page is where a user enters their username (or other identification) and password to verify they are authorized to access the content of the website or system. Users that try to access content from an outside search engine or website will be re-directed to the login page before being able to continue to the material. Once users leave the site they will be required to enter their information into the login page before regaining entry.
Loose Coupling	Within an SOA framework, loose coupling refers to a functionally resilient relationship between two or more systems or organizations with some kind of implicit information exchange relationship. Each end of the transaction makes its requirements explicit and makes few assumptions about the other end. Loosely-coupled services maintain a relationship that minimizes application-specific dependencies and only requires that they maintain a "general operational awareness" of one another.
Machine-to-Machine (M2M) Messaging	<p>M2M messaging involves:</p> <ul style="list-style-type: none"> • Coordination of hardware and software systems enabling seamless data access and asset management • The integration of device-layer identification, sensing, location and processing with enterprise-layer diagnostics, monitoring and control applications • An ecosystem of vendors, integrators and ASPs creating significant value via proactive asset and enterprise data management and analysis <p>The use of M2M Messaging will provide the HSIN Next Generation System with the</p>

Table 2. Glossary of Terms	
Term	Definition
	infrastructure to establish and sustain a reliable bridge between multiple organizations, thereby enabling the interoperable sharing of data.
Maintainability	<p>Maintainability is a characteristic of design and installation that defines the probability that an item will be retained in or restored to a specified condition within a given period of time when the maintenance is performed in accordance with prescribed procedures and resources. It includes the ease with which maintenance of a functional unit can be performed in accordance with prescribed requirements.</p> <p>HSIN Next Generation System maintenance requirements will address accessibility, diagnostics, repair and sparing for all maintenance levels.</p>
Mediation	<p>Within an SOA framework, mediation refers to an indirect mapping between various data sources based on a standardized data model.</p> <p>The HSIN Next Generation System Mediation capability provides the infrastructure to integrate data providers seamlessly with data consumers and other data providers.</p>
Metrics	<p>Metrics are a system of parameters for the quantitative and periodic assessment of a measurable process. A metric should include the procedures used to conduct the measurement, as well as the analytical method for interpreting the assessment. Metrics are usually specialized by the subject area, in which case they are valid only within a certain domain and cannot be directly benchmarked or interpreted outside it. This FRD defines metrics requirements for system usage, system health and content.</p>
Multi-Level Security	<p>Multi-level security is the ability to handle multiple classification levels and compartmentalize those information pieces. The system processes information with different sensitivities (i.e. SBU and PCII), permits simultaneous access by users with different access levels, and prevents users from obtaining access to information for which they lack authorization. In the case of HSIN NextGen, multi-level security pertains to the different types of SBU data. All data used by HSIN Next Gen will be unclassified.</p> <p>Multi-level security allows less sensitive information to be shared with higher classification systems, and it allows higher classified information to be sanitized and shared with lower classification systems, such as HSIN NextGen. Sanitized data has been edited to remove information that classified it at a higher level.</p>
Non-business Requirement	<p>Non-business requirements are requirements which specify criteria that can be used to assess the general operational characteristics of a system, rather than their specific behaviors. This should be contrasted with functional requirements that define specific behaviors or functions. Non-business requirements are often called qualities of a system. Other terms for non-business requirements are constraints, quality attributes, quality goals and quality of service requirements.</p> <p>The non-business requirements for the HSIN Next Generation System are defined in section 3 of this document.</p>
Notification	<p>A notification is a message sent informing the user(s) of an action or event that may impact them in some way. For example notifications are sent to inform employees that their network will be down for a certain period due to system maintenance and therefore some services will not be available.</p>
Online Chat / Chat	<p>A chat is a real time online conversation between many computer users. The chat takes place in a "chat room", a virtual online room. Users type their messages, and their messages appear on the monitor as text entries that scroll many screens deep. Anywhere from 2 to 200 people can be in a chat room. They can send, receive and reply to messages from many chat users simultaneously. It is similar to instant messaging but</p>

Table 2. Glossary of Terms	
Term	Definition
	<p>with more than two people.</p> <p>The HSIN Next Generation System will support creating both persistent and temporary chat rooms as part of its Instant Messaging facility.</p>
Open Architecture	<p>Open architecture is a type of systems architecture that facilitates adding, upgrading and swapping functional components. Open architecture allows potential users to see inside all or parts of the architecture without any proprietary constraints. Typically, an open architecture publishes all or parts of its architecture that the developer or integrator wants to share.</p> <p>The HSIN Next Generation System development includes the design, development, integration, testing, and implementation of a multi-level fully secure Open Architecture system.</p>
Operational View (OV)	<p>A view that describes the joint capabilities that the user seeks and how to employ them. The OVs also identify the operational nodes, the critical information needed to support the piece of the process associated with the nodes, and the organizational relationships.</p>
Operational View 1 (OV-1)	<p>OV-1 refers to a high-level graphical and/or textual description of an identifiable operational concept (high-level organizations, missions, geographic configuration, connectivity, etc)..</p>
Polling	<p>Polling refers to the sequential interrogation of system devices for various purposes, such as avoiding contention, determining current operational status, or determining readiness to send or receive data.</p> <p>The HSIN Next Generation System will incorporate a polling capability to support collaborative efforts.</p>
Real-Time	<p>Occurring immediately. The term is used to describe a number of different computer features. For example, real-time operating systems are systems that respond to input immediately. They are used for such tasks as navigation, in which the computer must react to a steady flow of new information without interruption. Most general-purpose operating systems are not real-time because they can take a few seconds, or even minutes, to react.</p> <p>A real-time system may be one where its application can be considered (within context) to be mission critical.</p>
Reliability	<p>Reliability is the ability of a system or component to perform its required functions under stated conditions for a specified period of time. Reliability is the ability of a system to perform and maintain its functions in routine conditions, as well as unexpected and even hostile circumstances.</p> <p>The HSIN Next Generation System infrastructure will maintain reliability during peak demand or periods of stress, but will allow vendors the flexibility to distribute system load across sites.</p>
Routine Problem	<p>A routine problem refers to any problem that is commonly resolved within the span of a Help Desk call or quickly resolved following the call. If there is a defect, it is the result of non-conformance to a standard, related to the aesthetics of the system, or a request for an enhancement. A defect at this level may be deferred or even ignored at the discretion of DHS. It can be resolved in a future system update or not at all.</p>
Scalability	<p>In systems engineering, scalability is a desirable property of a system, network, or process that indicates its ability to handle growing amounts of work in a graceful manner, or to be readily enlarged. For example, scalability refers to the capability of a system to</p>

Table 2. Glossary of Terms	
Term	Definition
	<p>increase total throughput under an increased load when resources are added.</p> <p>The HSIN Next Generation System will be designed to facilitate consistent and graceful expansion.</p>
Section 508 (Rehabilitation Act of 1973)	<p>In 1998 the US Congress amended the Rehabilitation Act to require Federal agencies to make their electronic and information technology accessible to people with disabilities. Inaccessible technology interferes with an individual's ability to obtain and use information quickly and easily.</p> <p>Section 508 was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities, and to encourage development of technologies that will help achieve these goals. The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Under Section 508, agencies must give disabled employees and members of the public access to information that is comparable to the access available to others.</p> <p>The HSIN Next Generation System will be Section 508-compliant.</p>
Sensitive But Unclassified (SBU)	<p>"Sensitive But Unclassified" is a U.S. designation of information, often referred to as "Sensitive Homeland Security Information." SBU is a broad category of information including For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g., SSI, CII) while others (FOUO) do not.</p> <p>The HSIN Next Generation System will support Sensitive But Unclassified (SBU) information and operations.</p>
Service Discovery	<p>Within an SOA framework, service discovery refers to "services" that are designed to be outwardly descriptive so that they can be found and assessed via available discovery mechanisms.</p> <p>A key component of the HSIN Next Generation System SOA framework will be a searchable repository of services that provides an asset management capability for services within DHS and supports the full life-cycle of services and service artifacts. Service discovery allows service providers to publish/advertise service specifications, metadata, and service accessibility to the entire user community. Service discovery also allows service consumers to discover information that has been advertised by providers.</p>
Service-Oriented Architecture (SOA)	<p>Service-oriented architecture is a computer systems architectural style for creating and using business processes (packaged as "services") throughout their life-cycle. The SOA framework also defines the IT infrastructure that allows different applications to exchange data and participate in business processes. One of the underpinning concepts of SOA is that these services are best used when <i>loosely coupled</i> with the operating systems and programming languages that support the applications themselves.</p> <p>The SOA framework separates functions into distinct operational units (i.e., "services"), which can then be distributed over a network to be combined and reused when creating business applications. These services communicate with each other by passing data from one service to another, or by coordinating a predefined business activity between two or more services. SOA concepts are often seen as having logically evolved from the older systems development concepts of distributed computing and modular programming.</p> <p>The HSIN Next Generation System will promote interoperability with DHS enterprise and Federal, State, local, Tribal, Territorial, private sector, and international partners through</p>

Table 2. Glossary of Terms	
Term	Definition
	an SOA. The HSIN Next Generation SOA objective is intended to define a set of capabilities that can be satisfied with commercially available products and open standards. It will include the following enterprise core services: Enterprise Service Management (ESM), Content Discovery and Delivery (CDD), Machine-to-Machine (M2M) Messaging, and Service Discovery.
Survey	Survey refers to a representative sampling (or partial collection) of gathered information that is used to approximate what a complete collection and analysis might reveal. The HSIN Next Generation System will incorporate a survey capability to support collaborative efforts.
Survivability	In systems engineering, survivability is the quantified ability of a system, subsystem, equipment, process, or procedure to continue to function during and after a natural or man-made disturbance. For a given application survivability must be qualified by specifying the range of conditions over which the entity will survive, the minimum acceptable level of post-disturbance functionality and the maximum acceptable outage duration. The HSIN Next Generation System will remain operational during and following a system or environmental disturbance. This requires that resources be reconstituted in time or failover in place.
System Failure	System failure is any incident that causes total loss of functionality for one of the HSIN tools and severely affects system use. The problem is of a time-sensitive nature. While it does not cause a complete work stoppage, no workaround is available and operational activities can only continue in a restricted fashion. Alternatively, it may be a "critical failure" for which a customer-acceptable workaround exists.
Test	Test refers to verification through systematic exercising of the applicable item under appropriate conditions with instrumentation to measure required parameters and the collection, analysis, and evaluation of quantitative data to show that measured parameters equal or exceed specified requirements.
Universal Description, Discovery, and Integration (UDDI)	UDDI is a platform-independent, XML-based registry for businesses worldwide to list themselves on the Internet. UDDI is an open industry initiative, sponsored by OASIS, enabling businesses to publish service listings and discover each other and define how the services or software applications interact over the Internet. A UDDI business registration consists of three components: <ul style="list-style-type: none"> • White Pages: Address, contact, and known identifiers • Yellow Pages: Industrial categorizations based on standard taxonomies • Green Pages: Technical information about services exposed by the business The HSIN Next Generation System will conform to the UDDI V3.0.2 standard, including a Service Discovery specification for support of the overall SOA framework.
Upload	To 'upload' is the ability for HSIN users to be able to send/transfer data from a local source, such as the user's desktop, and save/copy it onto the HSIN Next generation system. For example, "Uploading a video to HSIN NextGen" means sending a video to the system, which can be accessed by other HSIN NextGen users, through the system.
Usability	In human/computer interaction, the term usability usually refers to the elegance and clarity with which the interaction with an automated system or web site is designed. The primary notion of usability is that a system designed with the users' psychology and

Table 2. Glossary of Terms	
Term	Definition
	<p>physiology in mind is, for example:</p> <ul style="list-style-type: none"> • More Efficient to Use: Takes less time to accomplish a particular task • Easier to Learn: Operation can be learned by observing the object • General Satisfaction: More satisfying to use <p>The HSIN Next Generation System interfaces and functions will be designed for ease-of-use at all levels of anticipated user abilities.</p>
Visualization	<p>Data visualization is the use of interactive, visual representations of abstract and non-abstract data to provide for decision support and situational awareness. Visualization provides user interactivity and dynamic visual representation. The user can modify the visualization in real-time, thus affording perception of patterns and structural relations in the abstract data in question.</p> <p>The HSIN Next Generation System will support visualization tools to view data in graphical, geospatial, and temporal views.</p>
Web Browser	<p>A web browser is a software application that enables a user to display and interact with text, images, videos, music, and other information typically located on a web page, at a website, on the World Wide Web, or on a local area network. Text and images on a web page can contain hyperlinks to other web pages at the same or different website. Web browsers allow a user to quickly and easily access information provided on many web pages at many websites by traversing these links. Web browsers may display or format the same HTML information a differently, so the appearance of any given web page may differ somewhat between browsers.</p> <p>Some of the Web browsers available for personal computers include Internet Explorer, Mozilla Firefox, Safari, and Opera in order of descending popularity (as of November 2007).</p> <p>The HSIN Next Generation System will be fully web-enabled.</p>
XML	<p>"XML" is short for eXtensible Markup Language. XML is a general purpose markup language, and is essentially a pared-down version of the Standard Generalized Markup Language (SGML). It is designed especially for web documents. XML allows designers to create their own customized tags, thereby enabling the definition, transmission, validation, and interpretation of data between applications and between organizations. Its primary purpose is to facilitate the sharing of structured data across different information systems, particularly via the Internet. It is used both to encode documents and to serialize data.</p>

14.0 PWS/SOO/FRD CROSS REFERENCE TABLE

The following table provides a cross reference from the PWS sections (to the 5th level) to the Task Order Statement Of Objectives (SOO), the Functional Requirements, and Contract Work Breakdown Structure (CWBS). Each level (1st, 2nd, 3rd, and 4th) of the CWBS map directly to the first 4 levels identified in Section 5.0, the HSIN Performance Requirements.

PWS – STATEMENT OF OBJECTIVES/FUNCTIONAL REQUIREMENTS DOCUMENT CROSS REFERENCE				
PWS Section	PWS Task	SOO	FRD & HSIN-CS	CWBS
1	BACKGROUND	2.0 Background	N/A	N/A
2	SCOPE	1.0 Overview	N/A	N/A
2.1	Program Objectives	5.0 Program Objectives	N/A	N/A
3.0	APPLICABLE DOCUMENTS	N/A	N/A	N/A
4.0	PERFORMANCE REQUIREMENTS	N/A	N/A	N/A
4.1	BASE YEAR	N/A	HSIN-CS, HSIN NexGen FRD 2.X	1.1
4.1.1	Program and Technical Management	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1
4.1.1.1	Program Planning and Execution	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1.1
4.1.1.1.1	Program Plan	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1.1
4.1.1.1.2	Tailored Development Process	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1.1
4.1.1.1.3	Risk Management Plan	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1.1
4.1.1.1.4	IT Security Plan	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1.1
4.1.1.1.5	Master Test and Evaluation Plan	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1.1
4.1.1.1.6	Software Development Plan	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1.1
4.1.1.1.7	Quality Assurance Surveillance Plan	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1.1
4.1.1.1.8	Service Level Agreements (SLA)	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1.1
4.1.1.2	Earned Value Management Systems (EVMS)	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1.2
4.1.1.3	Subcontract Management	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1.3
4.1.1.4	Configuration Management	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1.4
4.1.1.5	Program Quality Assurance	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1.5
4.1.1.6	Program Reviews	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1.6
4.1.1.7	Performance Measures	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X	1.1.1.7
4.1.2	Spiral 1 – HSIN-CS	6.3 Technical Objectives	HSIN-CS	1.1.2
4.1.2.1	Technical Management	6.2 Core Functional Areas	HSIN-CS	1.1.2.1
4.1.2.2	Architecture and Systems Engineering	6.2 Core Functional Areas	HSIN-CS	1.1.2.2
4.1.2.3	Analysis, Design, Development and Implementation	6.2 Core Functional Areas	HSIN-CS	1.1.2.3
4.1.2.4	Certification and Accreditation	6.2 Core Functional Areas	HSIN-CS	1.1.2.4

PWS – STATEMENT OF OBJECTIVES/FUNCTIONAL REQUIREMENTS DOCUMENT CROSS REFERENCE

PWS Section	PWS Task	SOO	FRD & HSIN-CS	CWBS
4.1.2.5	System Test and Evaluation	6.2 Core Functional Areas	HSIN-CS	1.1.2.5
4.1.2.6	Organizational Change and Training	6.2 Core Functional Areas	HSIN-CS	1.1.2.6
4.1.2.6.1	Organizational Change	6.2 Core Functional Areas	HSIN-CS	1.1.2.6
4.1.2.6.2	Training	6.2 Core Functional Areas	HSIN-CS	1.1.2.6
4.1.2.7	Operational/Site Activation	6.2 Core Functional Areas	HSIN-CS	1.1.2.7
4.1.2.7.1	Installation Plan	6.2 Core Functional Areas	HSIN-CS	1.1.2.7
4.1.3	Spiral 2 – HSIN NexGen IOC	6.3 Technical Objectives	HSIN NexGen FRD 2.X	1.1.3
4.1.3.1	Technical Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X	1.1.3.1
4.1.3.2	Architecture and System Engineering	6.2 Core Functional Areas	HSIN NexGen FRD 2.X	1.1.3.2
4.1.3.3	Analysis, Design, Development and Implementation	6.2 Core Functional Areas	HSIN NexGen FRD 2.X	1.1.3.3
4.1.3.4	Certification and Accreditation	6.3 Technical Objectives	HSIN NexGen FRD 2.X	1.1.3.4
4.1.3.5	System Test and Evaluation	6.2 Core Functional Areas	HSIN NexGen FRD 2.X	1.1.3.5
4.1.3.5.1	Independent Verification and Validation	6.3 Technical Objectives	HSIN NexGen FRD 2.X	1.1.3.5
4.1.3.6	Organizational Change and Training	6.2 Core Functional Areas	HSIN NexGen FRD 2.X	1.1.3.6
4.1.3.6.1	Organizational Change	6.2 Core Functional Areas	HSIN NexGen FRD 2.X	1.1.3.6
4.1.3.6.2	Training	6.2 Core Functional Areas	HSIN NexGen FRD 2.X	1.1.3.6
4.1.3.7	Operational/Site Activation	6.2 Core Functional Areas	HSIN NexGen FRD 2.X	1.1.3.7
4.1.3.7.1	Installation Plan	6.2 Core Functional Areas	HSIN NexGen FRD 2.X	1.1.3.7
4.1.4	Spiral 4 – HSIN NexGen FOC	6.3 Technical Objectives	HSIN NexGen FRD 3.X	1.1.4
4.1.4.1	Technical Management	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.1.4.1
4.1.4.2	Architecture and System Engineering	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.1.4.2
4.1.4.3	Analysis, Design, Development and Implementation	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.1.4.3
4.1.4.4	Certification and Accreditation	6.3 Technical Objectives	HSIN NexGen FRD 3.X	1.1.4.4
4.1.4.5	System Test and Evaluation	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.1.4.5
4.1.4.6	Organizational Change and Training	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.1.4.6
4.1.4.6.1	Organizational Change	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.1.4.6
4.1.4.6.2	Training	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.1.4.6
4.1.5	HSIN NexGen Operations and Maintenance (O&M) Support	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN NexGen FRD 3.X	1.1.5
4.1.5.1	Program Management	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.1.5.1

PWS – STATEMENT OF OBJECTIVES/FUNCTIONAL REQUIREMENTS DOCUMENT CROSS REFERENCE

PWS Section	PWS Task	SOO	FRD & HSIN-CS	CWBS
4.1.5.2	Help Desk Services	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN NexGen FRD 3.X	1.1.5.2
4.1.5.3	Tier 2 – System Administration	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN NexGen FRD 3.X	1.1.5.3
4.1.5.4	Tier 3 – Infrastructure & Network Services	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN NexGen FRD 3.X	1.1.5.4
4.2	Option 1	N/A	HSIN NexGen FRD 2.X & 3.X	1.2
4.2.1	Program and Technical Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.2.1
4.2.1.1	Program Planning and Execution	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.2.1.1
4.2.1.2	Earned Value Management System (EVMS)	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.2.1.2
4.2.1.3	Subcontract Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.2.1.3
4.2.1.4	Configuration Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.2.1.4
4.2.1.5	Program Quality Assurance	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.2.1.5
4.2.1.6	Program Reviews	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.2.1.6
4.2.1.7	Performance Measures	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.2.1.7
4.2.2	Spiral 3 – HSIN NexGen MOC	6.3 Technical Objectives	HSIN NexGen FRD 2.X	1.2.2
4.2.2.1	Technical Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X	1.2.2.1
4.2.2.2	Organizational Change and Training	6.2 Core Functional Areas	HSIN NexGen FRD 2.X	1.2.2.2
4.2.2.2.1	Organizational Change	6.2 Core Functional Areas	HSIN NexGen FRD 2.X	1.2.2.2
4.2.2.2.2	Training	6.2 Core Functional Areas	HSIN NexGen FRD 2.X	1.2.2.2
4.2.2.3	Operational/Site Activation	6.2 Core Functional Areas	HSIN NexGen FRD 2.X	1.2.2.3
4.2.2.4	Decommissioning	6.2 Core Functional Areas	HSIN NexGen FRD 2.X	1.2.2.4
4.2.3	Spiral 4 – HSIN NexGen FOC	6.3 Technical Objectives	HSIN NexGen FRD 3.X	1.2.3
4.2.3.1	Technical Management	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.2.3.1
4.2.3.2	Architecture and System Engineering	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.2.3.2
4.2.3.3	Analysis, Design, Development and Implementation	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.2.3.3
4.2.3.4	Certification and Accreditation	6.3 Technical Objectives	HSIN NexGen FRD 3.X	1.2.3.4
4.2.3.5	System Test and Evaluation	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.2.3.5
4.2.3.5.1	Independent Verification and Validation	6.3 Technical Objectives	HSIN NexGen FRD 3.X	1.2.3.5
4.2.3.6	Organizational Change and Training	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.2.3.6
4.2.3.6.1	Organizational Change	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.2.3.6
4.2.3.6.2	Training	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.2.3.6
4.2.3.7	Operational/Site Activation	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.2.3.7

PWS – STATEMENT OF OBJECTIVES/FUNCTIONAL REQUIREMENTS DOCUMENT CROSS REFERENCE

PWS Section	PWS Task	SOO	FRD & HSIN-CS	CWBS
4.2.3.7.1	Installation Plan	6.2 Core Functional Areas	HSIN NexGen FRD 3.X	1.2.3.7
4.2.4	HSIN NexGen O&M Support	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X & 3.X	1.2.4
4.2.4.1	Program Management	6.2 Core Functional Areas	HSIN-CS, HSIN NexGen FRD 2.X & 3.X	1.2.4.1
4.2.4.2	Help Desk Services	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN-CS, HSIN NexGen FRD 2.X & 3.X	1.2.4.2
4.2.4.3	Tier 2 – System Administration	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN-CS, HSIN NexGen FRD 2.X & 3.X	1.2.4.3
4.2.4.4	Tier 3 – Infrastructure & Network Services	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN-CS, HSIN NexGen FRD 2.X & 3.X	1.2.4.4
4.3	Option 2	N/A	HSIN NexGen FRD 2.X & 3.X	1.3
4.3.1	Program and Technical Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.3.1
4.3.1.1	Program Planning and Execution	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.3.1.1
4.3.1.2	Earned Value Management System (EVMS)	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.3.1.2
4.3.1.3	Subcontract Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.3.1.3
4.3.1.4	Configuration Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.3.1.4
4.3.1.5	Program Quality Assurance	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.3.1.5
4.3.1.6	Program Reviews	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.3.1.6
4.3.1.7	Performance Measures	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.3.1.7
4.3.2	HSIN NexGen O&M Support	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.3.2
4.3.2.1	Program Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.3.2.1
4.3.2.2	Help Desk Services	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN NexGen FRD 2.X & 3.X	1.3.2.2
4.3.2.3	Tier 2 – System Administration	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN NexGen FRD 2.X & 3.X	1.3.2.3
4.3.2.4	Tier 3 – Infrastructure & Network Services	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN NexGen FRD 2.X & 3.X	1.3.2.4
4.4	Option 3	N/A	HSIN NexGen FRD 2.X & 3.X	1.4
4.4.1	Program and Technical Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.4.1
4.4.1.1	Program Planning and Execution	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.4.1.1
4.4.1.2	Earned Value Management System (EVMS)	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.4.1.2
4.4.1.3	Subcontract Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.4.1.3
4.4.1.4	Configuration Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.4.1.4

PWS – STATEMENT OF OBJECTIVES/FUNCTIONAL REQUIREMENTS DOCUMENT CROSS REFERENCE

PWS Section	PWS Task	SOO	FRD & HSIN-CS	CWBS
4.4.1.5	Program Quality Assurance	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.4.1.5
4.4.1.6	Program Reviews	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.4.1.6
4.4.1.7	Performance Measures	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.4.1.7
4.4.2	HSIN NexGen O&M Support	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.4.2
4.4.2.1	Program Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.4.2.1
4.4.2.2	Help Desk Services	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN NexGen FRD 2.X & 3.X	1.4.2.2
4.4.2.3	Tier 2 – System Administration	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN NexGen FRD 2.X & 3.X	1.4.2.3
4.4.2.4	Tier 3 – Infrastructure & Network Services	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN NexGen FRD 2.X & 3.X	1.4.2.4
4.5	Option 4	N/A	HSIN NexGen FRD 2.X & 3.X	1.5
4.5.1	Program and Technical Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.5.1
4.5.1.1	Program Planning and Execution	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.5.1.1
4.5.1.2	Earned Value Management System (EVMS)	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.5.1.2
4.5.1.3	Subcontract Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.5.1.3
4.5.1.4	Configuration Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.5.1.4
4.5.1.5	Program Quality Assurance	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.5.1.5
4.5.1.6	Program Reviews	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.5.1.6
4.5.1.7	Performance Measures	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.5.1.7
4.5.2	HSIN NexGen O&M Support	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.5.2
4.5.2.1	Program Management	6.2 Core Functional Areas	HSIN NexGen FRD 2.X & 3.X	1.5.2.1
4.5.2.2	Help Desk Services	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN NexGen FRD 2.X & 3.X	1.5.2.2
4.5.2.3	Tier 2 – System Administration	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN NexGen FRD 2.X & 3.X	1.5.2.3
4.5.2.4	Tier 3 – Infrastructure & Network Services	6.2 Core Functional Areas 6.3 Technical Objectives	HSIN NexGen FRD 2.X & 3.X	1.5.2.4
5.0	PERFORMANCE STANDARDS	6.2 Core Functional Areas 6.3 Technical Objectives	N/A	N/A
6.0	INCENTIVES	N/A	N/A	N/A
7.0	DELIVERABLES AND DELIVERY SCHEDULE	6.2 Core Functional Areas 6.3 Technical Objectives	N/A	N/A
8.0	GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION	N/A	N/A	N/A

PWS – STATEMENT OF OBJECTIVES/FUNCTIONAL REQUIREMENTS DOCUMENT CROSS REFERENCE

PWS Section	PWS Task	SOO	FRD & HSIN-CS	CWBS
9.0	PLACE OF PERFORMANCE	N/A	N/A	N/A
9.1	Travel Requirements	N/A	N/A	N/A
10.0	PERIOD OF PERFORMANCE	N/A	N/A	N/A
11.0	SECURITY	6.2 Core Functional Areas	N/A	N/A
12.0	QUALITY ASSURANCE SURVEILLANCE PLAN	6.2 Core Functional Areas	N/A	N/A
13.0	PERFORMANCE STANDARDS	6.2 Core Functional Areas 6.3 Technical Objectives	N/A	N/A
14.0	PWS CROSS REFERENCE TABLE	N/A	N/A	N/A
15.0	CONTRACT WORK BREAKDOWN STRUCTURE	N/A	N/A	N/A
16.0	PWS/SOO/CWBS CROSS REFERENCE MATRIX	N/A	N/A	N/A

b(4)

16.0 PWS/SOO/CWBS CROSS REFERENCE MATRIX

PWS/SOO/CWBS Cross Reference Matrix			
PWS Section	PWS Task	SOO	CWBS
1	BACKGROUND	2	
2	SCOPE	3	
3	APPLICABLE DOCUMENTS	N/A	
4.1	BASE YEAR	3.0; 4.0; 5.0; 6.0	1.1
4.1.1	Program and Technical Management	3.0; 4.0; 5.0; 6.0	1.1.1
4.1.1.1	Program Planning and Execution	6.1; 6.2; 6.3; 6.4	1.1.1.1
4.1.1.1	Program Plan	6.2a; 6.2c	1.1.1.1
4.1.1.1.2	Tailored Development Process	6.2c; 6.3.3	1.1.1.1
4.1.1.1.3	Risk Management Plan	6.2c	1.1.1.1
4.1.1.1.4	IT Security Plan	6.2f; 6.4p; 6.4q	1.1.1.1
4.1.1.1.5	Master Test and Evaluation Plan	6.2d; 6.4p; 6.4q; 6.4r	1.1.1.1
4.1.1.1.6	Software Development Plan	6.2a; 6.2b; 6.4b	1.1.1.1
4.1.1.1.7	Quality Assurance Surveillance Plan	6.2e; 6.4p; 6.4q; 6.4r	1.1.1.1
4.1.1.1.8	Service Level Agreements (SLA)	6.2e; 6.4p; 6.4q; 6.4r	1.1.1.1
4.1.1.2	Earned Value Management Systems (EVMS)	6.2a; 6.2c; 6.4m	1.1.1.2
4.1.1.3	Subcontract Management	6.2a; 6.2c	1.1.1.3
4.1.1.4	Configuration Management	6.2a; 6.2c; 6.4n; 6.4o	1.1.1.4
4.1.1.5	Program Quality Assurance	6.2e; 6.4p; 6.4q; 6.4r	1.1.1.5
4.1.1.6	Program Reviews	6.2a; 6.2c; 6.2e	1.1.1.6
4.1.1.7	Performance Measures	6.2a; 6.2c; 6.2e	1.1.1.7
4.1.2	Spiral 1 – HSIN-CS	3.0; 4.0; 5.0; 6.0	1.1.2
4.1.2.1	Technical Management	6.2b; 6.2c; 6.3.1-S1; 6.3.2; 6.3.3; 6.4	1.1.2.1
4.1.2.2	Architecture and System Engineering	6.2b; 6.2c; 6.3.1-S1; 6.3.2; 6.4	1.1.2.2
4.1.2.2.1	System Analysis, Design, Development and Implementation	6.2a; 6.2b; 6.2c; 6.3.1-S1; 6.3.2; 6.4i; 6.4j; 6.4k; 6.4q	1.1.2.2
4.1.2.2.2	System Requirements and Design	6.2b; 6.2c; 6.3.1-S1; 6.3.2; 6.4i; 6.4j; 6.4k; 6.4q	1.1.2.2
4.1.2.2.3	Architecture and Systems Engineering of HSIN NextGen	6.2b; 6.2c; 6.3.1-S1; 6.3.2; 6.4i; 6.4j; 6.4k; 6.4q	1.1.2.2
4.1.2.3	Prime Mission Product	6.2b; 6.2c; 6.3.1-S1; 6.3.2; 6.4	1.1.2.3
4.1.2.3.1	Product Implementation	6.2b; 6.2c; 6.3.1-S1; 6.3.2; 6.4i; 6.4j	1.1.2.3
4.1.2.3.2	Product Test	6.2d; 6.3.2; 6.4g; 6.4p; 6.4q	1.1.2.3
4.1.2.3.3	Version Description Document	6.2e; 6.3.2; 6.4p	1.1.2.3
4.1.2.4	Certification and Accreditation	6.2d; 6.2e; 6.3.1-S1; 6.3.2; 6.4g; 6.4p; 6.4q	1.1.2.4
4.1.2.5	System Test and Evaluation	6.2d; 6.3.1-S1; 6.3.2; 6.4g; 6.4i; 6.4j; 6.4p; 6.4q	1.1.2.5
4.1.2.5.1	System Integration Test	6.2d; 6.3.2; 6.4g; 6.4i; 6.4j; 6.4p; 6.4q	1.1.2.5
4.1.2.5.2	Customer Test Readiness Review	6.2d; 6.3.2; 6.4g; 6.4i; 6.4j; 6.4p; 6.4q	1.1.2.5

PWS/SOO/CWBS Cross Reference Matrix

PWS Section	PWS Task	SOO	CWBS
4.1.2.6	Organizational Change and Training	6.2g; 6.3.1-S1; 6.3.4; 6.4c; 6.4e; 6.4f; 6.4h; 6.4i; 6.4o	1.1.2.6
4.1.2.6.1	Organizational Change	6.2g; 6.3.4; 6.4c; 6.4e; 6.4f; 6.4h; 6.4i; 6.4o	1.1.2.6
4.1.2.6.2	Training Plan	6.2g; 6.3.4; 6.4e; 6.4f; 6.4h; 6.4i	1.1.2.6
4.1.2.6.3	Training Materials	6.2g; 6.3.4; 6.4e; 6.4f; 6.4h; 6.4i	1.1.2.6
4.1.2.6.4	Training Delivery	6.2g; 6.3.4; 6.4e; 6.4f; 6.4h; 6.4i	1.1.2.6
4.1.2.7	Operational/Site Activation	6.2h; 6.3.1-S1; 6.3.4; 6.4d; 6.4f; 6.4h; 6.4i; 6.4o; 6.4p	1.1.2.7
4.1.2.7.1	Installation Plan	6.2h; 6.3.4; 6.4d; 6.4f; 6.4h; 6.4i; 6.4o	1.1.2.7
4.1.2.7.1.1	Facilities Management.	6.2h; 6.3.4; 6.4d; 6.4f; 6.4h; 6.4i; 6.4o	1.1.2.7
4.1.2.7.1.2	Installation Drawings.	6.2h; 6.3.4; 6.4d; 6.4f; 6.4h; 6.4i; 6.4o	1.1.2.7
4.1.3	Spiral 2 – HSIN NextGen IOC	3.0; 4.0; 5.0; 6.0	1.1.3
4.1.3.1	Technical Management	6.2b; 6.2c; 6.3.1-S2; 6.3.2; 6.3.3; 6.4	1.1.3.1
4.1.3.2	Architecture and System Engineering	6.2b; 6.2c; 6.3.1-S2; 6.3.2; 6.4	1.1.3.2
4.1.3.2.1	System Analysis, Design, Development and Implementation	6.2a; 6.2b; 6.2c; 6.3.1-S2; 6.3.2; 6.4i; 6.4j; 6.4k; 6.4q	1.1.3.2
4.1.3.2.2	System Requirements and Design	6.2b; 6.2c; 6.3.1-S2; 6.3.2; 6.4i; 6.4j; 6.4k; 6.4q	1.1.3.2
4.1.3.2.3	Customer System Requirements Review	6.2b; 6.2c; 6.3.1-S2; 6.3.2; 6.4i; 6.4j; 6.4k; 6.4q	1.1.3.2
4.1.3.2.4	Architecture and Systems Engineering of HSIN NextGen	6.2b; 6.2c; 6.3.1-S2; 6.3.2; 6.4i; 6.4j; 6.4k; 6.4q	1.1.3.2
4.1.3.3	Prime Mission Product	6.2b; 6.2c; 6.3.1-S2; 6.3.2; 6.4	1.1.3.3
4.1.3.3.1	Product Implementation	6.2b; 6.2c; 6.3.1-S2; 6.3.2; 6.4i; 6.4j	1.1.3.3
4.1.3.3.2	Customer System/Software Design Review	6.2b; 6.2c; 6.3.1-S2; 6.3.2; 6.4i; 6.4j	1.1.3.3
4.1.3.3.3	Product Test	6.2d; 6.3.2; 6.4g; 6.4p; 6.4q	1.1.3.3
4.1.3.3.4	Version Description Document	6.2e; 6.3.2; 6.4p	1.1.3.3
4.1.3.4	Certification and Accreditation	6.2d; 6.2e; 6.3.1-S2; 6.3.2; 6.4g; 6.4p; 6.4q	1.1.3.4
4.1.3.5	System Test and Evaluation	6.2d; 6.3.1-S2; 6.3.2; 6.4g; 6.4i; 6.4j; 6.4p; 6.4q	1.1.3.5
4.1.3.5.1	Customer Test Readiness Review	6.2d; 6.3.2; 6.4g; 6.4i; 6.4j; 6.4p; 6.4q	1.1.3.5
4.1.3.5.2	Independent Verification and Validation	6.2d; 6.3.2; 6.4g; 6.4i; 6.4j; 6.4p; 6.4q	1.1.3.5
4.1.3.6	Organizational Change and Training	6.2g; 6.3.1-S2; 6.3.4; 6.4c; 6.4e; 6.4f; 6.4h; 6.4i; 6.4o	1.1.3.6
4.1.3.6.1	Organizational Change	6.2g; 6.3.4; 6.4c; 6.4e; 6.4f; 6.4h; 6.4i; 6.4o	1.1.3.6
4.1.3.6.2	Training Plan	6.2g; 6.3.4; 6.4e; 6.4f; 6.4h; 6.4i	1.1.3.6
4.1.3.6.3	Training Materials	6.2g; 6.3.4; 6.4e; 6.4f; 6.4h; 6.4i	1.1.3.6
4.1.3.6.4	Training Delivery	6.2g; 6.3.4; 6.4e; 6.4f; 6.4h; 6.4i	1.1.3.6
4.1.3.7	Operational/Site Activation	6.2h; 6.3.1-S2; 6.3.4; 6.4d; 6.4f; 6.4h; 6.4i; 6.4o; 6.4p	1.1.3.7
4.1.3.7.1	Installation Plan	6.2h; 6.3.4; 6.4d; 6.4f; 6.4h; 6.4i; 6.4o	1.1.3.7
4.1.3.7.1.1	Facilities Management.	6.2h; 6.3.4; 6.4d; 6.4f; 6.4h; 6.4i; 6.4o	1.1.3.7
4.1.3.7.1.2	Installation Drawings.	6.2h; 6.3.4; 6.4d; 6.4f; 6.4h; 6.4i; 6.4o	1.1.3.7
4.1.4	Spiral 4 – HSIN NextGen FOC	3.0; 4.0; 5.0; 6.0	1.1.4
4.1.4.1	Technical Management	6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.3.3; 6.4	1.1.4.1

PWS/SOO/CWBS Cross Reference Matrix

PWS Section	PWS Task	SOO	CWBS
4.1.4.2	Architecture and System Engineering	6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.4	1.1.4.2
4.1.4.2.1	System Analysis, Design, Development and Implementation	6.2a; 6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.4i; 6.4j; 6.4k; 6.4q	1.1.4.2
4.1.4.2.2	System Requirements and Design	6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.4i; 6.4j; 6.4k; 6.4q	1.1.4.2
4.1.4.2.3	Customer System Requirements Review	6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.4i; 6.4j; 6.4k; 6.4q	1.1.4.2
4.1.4.2.4	Architecture and Systems Engineering of HSIN NextGen	6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.4i; 6.4j; 6.4k; 6.4q	1.1.4.2
4.1.4.3	Prime Mission Product	6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.4	1.1.4.3
4.1.4.3.1	Product Implementation	6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.4i; 6.4j	1.1.4.3
4.1.4.3.2	Product Test	6.2d; 6.3.2; 6.4g; 6.4p; 6.4q	1.1.4.3
4.1.4.4	Certification and Accreditation	6.2d; 6.2e; 6.3.1-S4; 6.3.2; 6.4g; 6.4p; 6.4q	1.1.4.4
4.1.4.5	System Test and Evaluation.	6.2d; 6.3.1-S4; 6.3.2; 6.4g; 6.4i; 6.4j; 6.4p; 6.4q	1.1.4.5
4.1.4.4.1	System Integration Test	6.2d; 6.3.2; 6.4g; 6.4i; 6.4j; 6.4p; 6.4q	1.1.4.5
4.1.4.6	Organizational Change and Training	6.2g; 6.3.1-S4; 6.3.4; 6.4c; 6.4e; 6.4f; 6.4h; 6.4i; 6.4o	1.1.4.6
4.1.4.6.1	Organizational Change	6.2g; 6.3.4; 6.4c; 6.4e; 6.4f; 6.4h; 6.4i; 6.4o	1.1.4.6
4.1.4.6.2	Training Plan	6.2g; 6.3.4; 6.4e; 6.4f; 6.4h; 6.4i	1.1.4.6
4.1.4.6.3	Training Materials	6.2g; 6.3.4; 6.4e; 6.4f; 6.4h; 6.4i	1.1.4.6
4.1.5	HSIN NextGen Operations and Maintenance (O&M) Support	3.0; 4.0; 5.0; 6.0	1.1.5
4.1.5.1	Program Management	6.2a; 6.2b; 6.2c; 6.2h; 6.3.1-O&M; 6.3.2; 6.3.3; 6.3.4; 6.4	1.1.4.1
4.1.5.2	Help Desk Services	6.2e; 6.2g; 6.2h; 6.3.1-O&M; 6.3.4; 6.4d; 6.4f	1.1.4.2
4.1.5.3	Tier II – System Administration	6.2e; 6.2g; 6.2h; 6.3.1-O&M; 6.3.4; 6.4d; 6.4f	1.1.4.3
4.1.4.4	Tier III – Infrastructure & Network Services	6.2e; 6.2g; 6.2h; 6.3.1-O&M; 6.3.4; 6.4d; 6.4f	1.1.4.4
4.2	OPTION 1	3.0; 4.0; 5.0; 6.0	1.2
4.2.1	Program and Technical Management	3.0; 4.0; 5.0; 6.0	1.2.1
4.2.1.1	Program Planning and Execution	6.1; 6.2; 6.3; 6.4	1.2.1.1
4.2.1.2	Earned Value Management Systems (EVMS)	6.2a; 6.2c; 6.4m	1.2.1.2
4.2.1.3	Subcontract Management	6.2a; 6.2c	1.2.1.3
4.2.1.4	Configuration Management	6.2a; 6.2c; 6.4n; 6.4o	1.2.1.4
4.2.1.5	Program Quality Assurance	6.2e; 6.4p; 6.4q; 6.4r	1.2.1.5
4.2.1.6	Program Reviews	6.2a; 6.2c; 6.2e	1.2.1.6
4.2.1.7	Performance Measures	6.2a; 6.2c; 6.2e	1.2.1.7
4.2.2	Spiral 3 – HSIN NextGen MOC	3.0; 4.0; 5.0; 6.0	1.2.2
4.2.2.1	Technical Management	6.2b; 6.2c; 6.3.1-S3; 6.3.2; 6.3.3; 6.4	1.2.2.1
4.2.2.2	Organizational Change and Training	6.2g; 6.3.1-S3; 6.3.4; 6.4c; 6.4e; 6.4f; 6.4h; 6.4i; 6.4o	1.2.2.2
4.2.2.3	Operational/Site Activation	6.2h; 6.3.1-S3; 6.3.4; 6.4d; 6.4f; 6.4h; 6.4i; 6.4o; 6.4p	1.2.2.3
4.2.2.4	Decommissioning	6.2h; 6.3.1-S3; 6.3.4; 6.4d; 6.4f; 6.4h; 6.4i; 6.4o; 6.4p	1.2.2.4
4.2.3	Spiral 4 – HSIN NextGen FOC	3.0; 4.0; 5.0; 6.0	1.2.3
4.2.3.1	Technical Management	6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.3.3; 6.4	1.2.3.1

PWS/SOO/CWBS Cross Reference Matrix

PWS Section	PWS Task	SOO	CWBS
4.2.3.2	Architecture and System Engineering	6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.4	1.2.3.2
4.2.3.2.1	System Analysis, Design, Development and Implementation	6.2a; 6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.4i; 6.4j; 6.4k; 6.4q	1.2.3.2
4.2.3.2.2	System Requirements and Design	6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.4i; 6.4j; 6.4k; 6.4q	1.2.3.2
4.2.3.2.3	Architecture and Systems Engineering of HSIN NextGen	6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.4i; 6.4j; 6.4k; 6.4q	1.2.3.2
4.2.3.3	Prime Mission Product	6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.4	1.2.3.3
4.2.3.3.1	Product Implementation	6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.4i; 6.4j	1.2.3.3
4.2.3.3.2	Customer System/Software Design Review	6.2b; 6.2c; 6.3.1-S4; 6.3.2; 6.4i; 6.4j; 6.4k; 6.4q	1.2.3.3
4.2.3.3.3	Product Test	6.2d; 6.3.2; 6.4g; 6.4p; 6.4q	1.2.3.3
4.2.3.3.4	Version Description Document	6.2e; 6.3.2; 6.4p	1.2.3.3
4.2.3.4	Certification and Accreditation	6.2d; 6.2e; 6.3.1-S4; 6.3.2; 6.4g; 6.4p; 6.4q	1.2.3.4
4.2.3.5	System Test and Evaluation	6.2d; 6.3.1-S4; 6.3.2; 6.4g; 6.4i; 6.4j; 6.4p; 6.4q	1.2.3.5
4.2.3.5.1	System Integration Test	6.2d; 6.3.2; 6.4g; 6.4i; 6.4j; 6.4p; 6.4q	1.2.3.5
4.2.3.5.2	Customer Test Readiness Review	6.2d; 6.3.2; 6.4g; 6.4i; 6.4j; 6.4p; 6.4q	1.2.3.5
4.2.3.5.3	Independent Verification and Validation	6.2d; 6.3.2; 6.4g; 6.4i; 6.4j; 6.4p; 6.4q	1.2.3.5
4.2.3.6	Organizational Change and Training	6.2g; 6.3.1-S4; 6.3.4; 6.4c; 6.4e; 6.4f; 6.4h; 6.4i; 6.4o	1.2.3.6
4.2.3.6.1	Organizational Change	6.2g; 6.3.4; 6.4c; 6.4e; 6.4f; 6.4h; 6.4i; 6.4o	1.2.3.6
4.2.3.6.2	Training Plan	6.2g; 6.3.4; 6.4e; 6.4f; 6.4h; 6.4i	1.2.3.6
4.2.3.6.3	Training Materials	6.2g; 6.3.4; 6.4e; 6.4f; 6.4h; 6.4i	1.2.3.6
4.2.3.6.4	Training Delivery	6.2g; 6.3.4; 6.4e; 6.4f; 6.4h; 6.4i	1.2.3.6
4.2.3.7	Operational/Site Activation	6.2h; 6.3.1-S4; 6.3.4; 6.4d; 6.4f; 6.4h; 6.4i; 6.4o; 6.4p	1.2.3.7
4.2.3.7.1	Installation Plan	6.2h; 6.3.4; 6.4d; 6.4f; 6.4h; 6.4i; 6.4o	1.2.3.7
4.2.3.7.1.1	Facilities Management.	6.2h; 6.3.4; 6.4d; 6.4f; 6.4h; 6.4i; 6.4o	1.2.3.7
4.2.3.7.1.2	Installation Drawings.	6.2h; 6.3.4; 6.4d; 6.4f; 6.4h; 6.4i; 6.4o	1.2.3.7
4.2.4	HSIN NextGen Operations and Maintenance (O&M) Support	3.0; 4.0; 5.0; 6.0	1.2.4
4.2.4.1	Program Management	6.2a; 6.2b; 6.2c; 6.2h; 6.3.1-O&M; 6.3.2; 6.3.3; 6.3.4; 6.4	1.2.4.1
4.2.4.2	Help Desk Services	6.2e; 6.2g; 6.2h; 6.3.1-O&M; 6.3.4; 6.4d; 6.4f	1.2.4.2
4.2.4.3	Tier II – System Administration	6.2e; 6.2g; 6.2h; 6.3.1-O&M; 6.3.4; 6.4d; 6.4f	1.2.4.3
4.2.4.4	Tier III – Infrastructure & Network Services	6.2e; 6.2g; 6.2h; 6.3.1-O&M; 6.3.4; 6.4d; 6.4f	1.2.4.4
4.3	OPTION 2	3.0; 4.0; 5.0; 6.0	1.3
4.3.1	Program and Technical Management	3.0; 4.0; 5.0; 6.0	1.3.1
4.3.1.1	Program Planning and Execution	6.1; 6.2; 6.3; 6.4	1.3.1.1
4.3.1.2	Earned Value Management Systems (EVMS).	6.2a; 6.2c; 6.4m	1.3.1.2
4.3.1.3	Subcontract Management	6.2a; 6.2c	1.3.1.3
4.3.1.4	Configuration Management	6.2a; 6.2c; 6.4n; 6.4o	1.3.1.4
4.3.1.5	Program Quality Assurance	6.2e; 6.4p; 6.4q; 6.4r	1.3.1.5
4.3.1.6	Program Reviews	6.2a; 6.2c; 6.2e	1.3.1.6

PWS/SOO/CWBS Cross Reference Matrix

PWS Section	PWS Task	SOO	CWBS
4.3.1.7	Performance Measures	6.2a; 6.2c; 6.2e	1.3.1.7
4.3.2	HSIN NextGen Operations and Maintenance (O&M) Support	3.0; 4.0; 5.0; 6.0	1.3.2
4.3.2.1	Program Management	6.2a; 6.2b; 6.2c; 6.2h; 6.3.1-O&M; 6.3.2; 6.3.3; 6.3.4; 6.4	1.3.2.1
4.3.2.2	Help Desk Services	6.2e; 6.2g; 6.2h; 6.3.1-O&M; 6.3.4; 6.4d; 6.4f	1.3.2.2
4.3.2.3	Tier II – System Administration	6.2e; 6.2g; 6.2h; 6.3.1-O&M; 6.3.4; 6.4d; 6.4f	1.3.2.3
4.3.2.4	Tier III – Infrastructure & Network Services	6.2e; 6.2g; 6.2h; 6.3.1-O&M; 6.3.4; 6.4d; 6.4f	1.3.2.4
4.4	OPTION 3	3.0; 4.0; 5.0; 6.0	1.4
4.4.1	Program and Technical Management	3.0; 4.0; 5.0; 6.0	1.4.1
4.4.1.1	Program Planning and Execution	6.1; 6.2; 6.3; 6.4	1.4.1.1
4.4.1.2	Earned Value Management Systems (EVMS)	6.2a; 6.2c; 6.4m	1.4.1.2
4.4.1.3	Subcontract Management	6.2a; 6.2c	1.4.1.3
4.4.1.4	Configuration Management	6.2a; 6.2c; 6.4n; 6.4o	1.4.1.4
4.4.1.5	Program Quality Assurance	6.2e; 6.4p; 6.4q; 6.4r	1.4.1.5
4.4.1.6	Program Reviews	6.2a; 6.2c; 6.2e	1.4.1.6
4.4.1.7	Performance Measures	6.2a; 6.2c; 6.2e	1.4.1.7
4.4.2	HSIN NextGen Operations and Maintenance (O&M) Support	3.0; 4.0; 5.0; 6.0	1.4.2
4.4.2.1	Program Management	6.2a; 6.2b; 6.2c; 6.2h; 6.3.1-O&M; 6.3.2; 6.3.3; 6.3.4; 6.4	1.4.2.1
4.4.2.2	Help Desk Services	6.2e; 6.2g; 6.2h; 6.3.1-O&M; 6.3.4; 6.4d; 6.4f	1.4.2.2
4.4.2.3	Tier II – System Administration	6.2e; 6.2g; 6.2h; 6.3.1-O&M; 6.3.4; 6.4d; 6.4f	1.4.2.3
4.4.2.4	Tier III – Infrastructure & Network Services	6.2e; 6.2g; 6.2h; 6.3.1-O&M; 6.3.4; 6.4d; 6.4f	1.4.2.4
4.5	OPTION 4	3.0; 4.0; 5.0; 6.0	1.5
4.5.1	Program and Technical Management	3.0; 4.0; 5.0; 6.0	1.4.1
4.5.1.1	Program Planning and Execution	6.1; 6.2; 6.3; 6.4	1.4.1.1
4.5.1.2	Earned Value Management Systems (EVMS)	6.2a; 6.2c; 6.4m	1.4.1.2
4.5.1.3	Subcontract Management	6.2a; 6.2c	1.4.1.3
4.5.1.4	Configuration Management	6.2a; 6.2c; 6.4n; 6.4o	1.4.1.4
4.5.1.5	Program Quality Assurance	6.2e; 6.4p; 6.4q; 6.4r	1.4.1.5
4.5.1.6	Program Reviews	6.2a; 6.2c; 6.2e	1.4.1.6
4.5.1.7	Performance Measures	6.2a; 6.2c; 6.2e	1.4.1.7
4.5.2	HSIN NextGen Operations and Maintenance (O&M) Support	3.0; 4.0; 5.0; 6.0	1.4.2
4.5.2.1	Program Management	6.2a; 6.2b; 6.2c; 6.2h; 6.3.1-O&M; 6.3.2; 6.3.3; 6.3.4; 6.4	1.4.2.1
4.5.2.2	Help Desk Services	6.2e; 6.2g; 6.2h; 6.3.1-O&M; 6.3.4; 6.4d; 6.4f	1.4.2.2
4.5.2.3	Tier II – System Administration	6.2e; 6.2g; 6.2h; 6.3.1-O&M; 6.3.4; 6.4d; 6.4f	1.4.2.3
4.5.2.4	Tier III – Infrastructure & Network Services	6.2e; 6.2g; 6.2h; 6.3.1-O&M; 6.3.4; 6.4d; 6.4f	1.4.2.4
5	PERFORMANCE STANDARDS	3.0; 4.0; 5.0; 6.0	N/A
6	INCENTIVES	N/A	N/A

PWS/SOO/CWBS Cross Reference Matrix

PWS Section	PWS Task	SOO	CWBS
7	DELIVERABLES AND DELIVERY SCHEDULE	3.0; 4.0; 5.0; 6.0	N/A
8	GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION	2.0; 3.0; 4.0	N/A
9	PLACE OF PERFORMANCE	2.0; 3.0; 4.0	N/A
9.1	TRAVEL REQUIREMENTS	3.0; 4.0; 5.0; 6.0	N/A
10	PERIOD OF PERFORMANCE	3.0; 4.0; 5.0; 6.0	N/A
11	SECURITY	3.0; 4.0; 5.0; 6.0	N/A
12	QUALITY ASSURANCE SURVEILLANCE PLAN	N/A	N/A
13	PERFORMANCE MEASUREMENT SUMMARY	N/A	N/A
14	PWS/SOO/FRD CROSS REFERENCE MATRIX	N/A	N/A
15	CONTRACTOR WORK BREAKDOWN STRUCTURE		
16	PWS/SOO/CWBS CROSS REFERENCE MATRIX	N/A	N/A

b(4)

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT ID CODE	PAGE OF PAGES 1 2
2. AMENDMENT/MODIFICATION NO. P00001	3. EFFECTIVE DATE 06/09/2008	4. REQUISITION/PURCHASE REQ. NO. See Schedule	5. PROJECT NO. (if applicable)
6 ISSUED BY Department of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	CODE DHS/OPO/ITAC	7. ADMINISTERED BY (if other than Item 6)	CODE DHS/OPO/ITAC
8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) GENERAL DYNAMICS ONE SOURCE LLC 3211 JERMANTOWN ROAD FAIRFAX VA 22030		(x) 9A. AMENDMENT OF SOLICITATION NO.	
		9B. DATED (SEE ITEM 11)	
		X 10A. MODIFICATION OF CONTRACT/ORDER NO. HSHQDC-06-D-00024 HSHQDC-08-J-00134	
		10B. DATED (SEE ITEM 11) 05/23/2008	
CODE 6103202150000	FACILITY CODE		

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) Net Increase: \$2,597,814.40
See Schedule

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

CHECK ONE	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.
	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).
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: FAR 52.243-2 Changes - Cost Reimbursement (AUG 1987)
	D. OTHER (Specify type of modification and authority)

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

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

DUNS Number: 610320215+0000

A. The purpose of this modification is to
 (1) incorporate changes to the attached OF 347 continuation pages at no cost to the task order
 (2) Release funding increment in the amount of \$2,597,814.40
 (3) Incorporate attached COTR designation letter
 (4) Correct administration error to CLIN 0001 estimated cost/fixed fee allocation.

B. The total obligated amount has been increased by \$2,597,814.40 from \$10,000,000 to \$12,597,814.40.

Delivery Location Code: DHS

Continued ...

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) Laura Walsh-Steinman, Lead Contracts Specialist	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Purnell Drew
15B. CONTRACTOR/OFFEROR (b(4))	16B. UNITED STATES OF AMERICA (b(6))
15C. DATE SIGNED 6/9/08	16C. DATE SIGNED 06/09/2008

NSN 7540-01-152-8070
Previous edition unusable

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

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00024/HSHQDC-08-J-00134/P00001

PAGE OF
 2 2

NAME OF OFFEROR OR CONTRACTOR
 GENERAL DYNAMICS ONE SOURCE LLC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0001	Department of Homeland Security 245 Murray Lane Bldg. 410 Washington DC 20528 FOB: Destination Change Item 0001 to read as follows (amount shown is the obligated amount): CPFF Engineering support to the HSIN Next Generation in accordance with the Attached Performance Work Statement (PWS) dated April 14, 2008 and the Functional Requirements Document (FRD) dated March 11, 2008. Estimated cost (b(4))) Fixed Fee (b(4))) Total CPFF \$18,948,405 Total Line Item Value \$18,948,405.00 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Requisition No: ROOP-08-00054, RPPD-07-00065, RPPD-07-00065 Accounting Info: ((b(2))) Funded: \$0.00 Accounting Info: ((b(2))) Funded: \$0.00 Accounting Info: ((b(2))) Funded: \$242,814.40 Accounting Info: ((b(2))) Funded: \$1,670,000.00 Accounting Info: ((b(2))) Funded: \$685,000.00				2,597,814.40

Section D – Packaging and Marking

D.1 – Packaging and Marking

Packaging and marking shall be performed in accordance with the instructions of the basic EAGLE contract.

Section E – Inspection and Acceptance

E.1 – Inspection and Acceptance

EAGLE sections E.1 and E.2 FAR clauses incorporated by reference.

E.2 – Inspection and Acceptance – Quality Assurance

As a performance based task order, the contractor identified performance measures and metric/service level agreements will form the basis of the inspection and acceptance Quality Assurance program.

Using the contractor provided metrics, the Government and the contractor will agree on a Quality Assurance framework, and methodology to establish initial performance levels and the ongoing performance level management. The Governance framework will continuously seek to refine, allocate and adjust service levels to reflect changes in priority and to ensure that throughout the life of this agreement that the program delivers improved performance and reduced cost.

E.3 – Place of Inspection and Acceptance

Inspection and acceptance of all work performed, reports, and other deliverables under this task order shall be performed by the Contracting Officer's Technical Representative (COTR) in accordance paragraphs E.4 through E.8.

E.4 – Scope of Inspection

All deliverables will be inspected for content, completeness, accuracy and conformance to the task order requirements by the COTR.

E.5 – Basis of Acceptance

- a. The basis for acceptance of services will be in compliance with the best commercial practices and those requirements provided in the task order.
- b. Items such as Other Direct Costs (ODC) (e.g. travel, equipment purchases) must be approved in advance. Request for ODC purchases must include a ROM estimate. ODCs will be accepted upon receipt of proper documentation as specified in the performance work statement (PWS).
- c. Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

- d. The contractor shall provide electronic copies of each deliverable. Electronic copies shall be delivered via email attachment or other media by mutual agreement of the parties. The electronic copies shall be compatible with MS Office 2000 or other applications as appropriate and mutually agreed to by the parties.
- e. The contractor shall use best commercial practice for formatting deliverables under this contract.
- f. All of the Government's comments on deliverables must either be incorporated in the succeeding version or the contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.
- g. If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, improper format, or otherwise does not conform to the requirements stated within this solicitation, the document may be immediately rejected without further review and returned to the contractor for correction and re-submission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the COTR.
- h. For software development, the final acceptance of the software program will occur when all discrepancies, errors or other deficiencies identified in writing by the Government have been resolved, either through documentation updates, program correction, or other mutually agreeable methods.

E.6 – Draft Deliverables

The Government will provide written acceptance, comments and/or change requests, if any, within 15 working days from receipt by the Government of each initial deliverable. Upon receipt of the Government comments, the contractor shall have 15 working days to incorporate the government's comments and/or change requests and to resubmit the deliverable in its final form.

E.7 – Written Acceptance

The Government shall provide written notification of acceptance or rejection of all final deliverables within thirty (30) calendar days of receipt. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection. The contractor shall assume acceptance if not notified by the Government within thirty (30) calendar days.

E.8 – Non-Conforming Products or Services

Non-conforming products or services will be rejected. Deficiencies will be corrected within 30 calendar days of the rejection notice. If the deficiencies cannot be corrected within 30 calendar days, the contractor will immediately notify the COTR of the reason for the delay and provide a proposed corrective action plan within ten (10) working days of notification.

- d. The contractor shall provide electronic copies of each deliverable. Electronic copies shall be delivered via email attachment or other media by mutual agreement of the parties. The electronic copies shall be compatible with MS Office 2000 or other applications as appropriate and mutually agreed to by the parties.
- e. The contractor shall use best commercial practice for formatting deliverables under this contract.
- f. All of the Government's comments on deliverables must either be incorporated in the succeeding version or the contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.
- g. If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, improper format, or otherwise does not conform to the requirements stated within this solicitation, the document may be immediately rejected without further review and returned to the contractor for correction and re-submission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the COTR.
- h. For software development, the final acceptance of the software program will occur when all discrepancies, errors or other deficiencies identified in writing by the Government have been resolved, either through documentation updates, program correction, or other mutually agreeable methods.

E.6 – Draft Deliverables

The Government will provide written acceptance, comments and/or change requests, if any, within 15 working days from receipt by the Government of each initial deliverable. Upon receipt of the Government comments, the contractor shall have 15 working days to incorporate the government's comments and/or change requests and to resubmit the deliverable in its final form.

E.7 – Written Acceptance

The Government shall provide written notification of acceptance or rejection of all final deliverables within thirty (30) calendar days of receipt. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection. The contractor shall assume acceptance if not notified by the Government within thirty (30) calendar days.

E.8 – Non-Conforming Products or Services

Non-conforming products or services will be rejected. Deficiencies will be corrected within 30 calendar days of the rejection notice. If the deficiencies cannot be corrected within 30 calendar days, the contractor will immediately notify the COTR of the reason for the delay and provide a proposed corrective action plan within ten (10) working days of notification.

Section F – Deliveries and Performance

F.1 – Period of Performance

The task order's basic period of performance shall be from May 27, 2008 – May 26, 2009. Beyond the base period, there are four one-year option periods. Taken together with the base period and option periods, the task order term may last for a total period not to exceed five years.

Periods of Task Order Performance to begin as follows:

Base Period: May 27, 2008 – May 26, 2009
Option Year 1: May 27, 2009 – May 26, 2010
Option Year 2: May 27, 2010 – May 26, 2011
Option Year 3: May 27, 2011 – May 26, 2012
Option Year 4: May 27, 2012 – May 26, 2013

F.2 – Option to Extend the Term of the Contract

**OPTION TO EXTEND THE TERM OF THE CONTRACT
(FAR 52.217-9) (MAR 2000)**

- (a) The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.
- (b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
- (c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months, excluding an extension under 52.217-8.

F.3 – Place of Performance

The primary place of performance for the HSIN NextGen task order contractor shall be at the contractor's facility which is required to be located within the National Capital Region, or a fifty mile radius of the DHS Office of Operations Coordination (OPS), currently at the Nebraska Avenue Complex (NAC) in NW Washington DC. HSIN NextGen system build activities shall be conducted at the DHS Data Centers (to be determined) and HSIN NextGen testing tasks may require periods of travel to one or more of the DHS HSIN NextGen stakeholder offices located in the continental United States, United States territories, and internationally.

Section G – Contract Administration Data

G.1 – Contracting Officer

The TO Contracting Officer (TO CO) is the only person authorized to make any changes, approve any changes in the requirements of this Task Order, obligate funds and authorize the expenditure of funds, and notwithstanding any provisions contained elsewhere in this task order, the said authority remains solely in the TO CO. In the event the contractor makes any changes at the direction of any person other than the TO CO, the change will be considered to have been without authority and no adjustment will be made in the task order price to cover any increase in costs occurred as a result thereof. It is incumbent on the Contractor to make sure that this requirement is enforced, or work performed will be performed at the Contractor's own risk.

The following TO Contracting Officer is assigned to this Task Order:

TO Contracting Officer:

NAME: Purnell Drew
PHONE NO.: (202) 447-(b)(2))
EMAIL: (b(2) b(6))

G.2 – Contracting Officer's Technical Representative (COTR) COTR (HSAR 3052.242-72)(DEC 2003)

(a) The Contracting Officer may designate Government personnel to act as the Contracting Officer's Technical Representative (COTR) to perform functions under the task order such as review or inspection and acceptance of supplies, services, including construction, and other functions of a technical nature. The Contracting Officer will provide a written notice of such designation to the Contractor within five working days after task order award. The designation letter will set forth the authorities and limitations of the COTR under the task order.

(b) The principal role of the COTR is to support the Contracting Officer in managing the work conducted under Section C of this Task Order. This is done through furnishing technical direction within the confines of the task order, monitoring performance, ensuring requirements are met within the terms of the task order, and maintaining a strong relationship with the Contracting Officer. As a team, the Contracting Officer and COTR must ensure that program requirements are clearly communicated and that the services are performed to meet them.

G.3 – Contracting Officer's Technical Representative Designation The following TO COTR is assigned to this Task Order:

NAME: (b(2) b(6))
PHONE NO.: (202) 447-(b)(2))
EMAIL: (b(2) b(6))

G.4 – Changes in COTR Designation(s)

The COTR may be changed at any time by the Government without prior notice to the Contractor. Notification of the change, including the name and phone number of the successor COTR, will be promptly provided to the Contractor by the TO Contracting Officer in writing.

G.5 – Invoice Submission - Data Elements

The data elements indicated below shall be included on each invoice. Details and format of invoices shall be consistent with structure specified by the COTR.

Vendor Name
Invoice Number
Invoice Date
Date of Service/Product provided
Payment/Vendor Address, Telephone Number, Other Contact information
Task Order Month
Fiscal Year
Payment Due Date
Contract Number
Task Order Number
Work Order number (if applicable)
DHS Functional/Budget Code/Accounting Data
Cumulative Value to Date
Total Amount Invoiced
Vendor Point-of-Contact
DHS Point-of-Contact
Grand Total per Invoice
Page Numbers
Shipping and Payment term

G.6 – Invoice Submission – Material Order Status Report

A report of all material/labor billed to DHS is required each month to track outstanding equipment in the “field” or residing at DHS HQ. The report shall include a status of the DHS 700-21 Material Inspection and Receiving Report, a government Point-of-Contact (POC), the equipment delivery location, equipment operational location, cost of each unit, lease duration/useful life, date of acquisition, type of equipment, system capabilities/specifications, and the bureau the equipment is supporting. The data must be provided in an application that is consistent with DHS approved software, preferably Microsoft Excel or Microsoft Access format.

G.7 – Electronic Invoice Submission

Electronic invoices must be submitted to the following email addresses within thirty days of services rendered:

All invoices must be submitted to:

OCPDAcquisition@hq.dhs.gov

(b1) b(6))

In addition:

Invoices for Requisition Number RPPD-07-00065 shall be submitted to: www.DOB-Invoice@DHS.GOV.

Invoices for Requisition Number ROOP-08-00054 shall be submitted to:

(b(4)) and (b(4)):

G.8 – Travel

Travel Regulations

As required by EAGLE Contract section H.6.1, the contractor shall comply with the guidance in FAR 31.205-46 using the regulations specified below.

- a. Federal Travel Regulations (FTR) - prescribed by the General Services Administration, for travel in the contiguous United States.
- b. Joint Travel Regulations (JTR), Volume 2, DoD Civilian Personnel, Appendix A, prescribed by the Department of Defense, for travel in Alaska, Hawaii, and outlying areas of the United States.
- c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas", prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

Travel Authorization Requests

Prior to any long distance travel, the contractor shall prepare a Travel Authorization Request for Government review and COTR approval. The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

Content of Travel Requests

Requests for travel approval shall contain:

- Date, time and points of departure
- Destination, time and dates of arrival
- Name of each contractor employee and position title
- Include a description of the travel proposed including a statement as to purpose
- Identify the Task Order number
- Identify the CLIN(s) associated with the travel
- Be submitted in advance of the travel with sufficient time to permit review and approval.

G.9 – Incremental Funding

(1) The contractor is required to comply with the terms and conditions of the contract in accordance with FAR Clause 52.232-22, Limitation of Funds. A total of **\$12,597,814.40** has been provided as incremental funding. ~~The amount of (b(4)) been allotted to cover the costs incurred in the performance of the services specified in the PWS. An additional (b(4)) has been allotted to cover the fixed fee.~~

(2) In accordance with the Limitation of Funds clause, the Government shall not be obligated to reimburse the contractor for any costs (including termination costs) in excess of the above-stated amount and the contractor will not be obligated to continue performance or incur cost in excess of the above-stated amount until additional funds are made available by the issuance of a unilateral modification from the Contracting Officer. ~~In accordance with paragraph B of the Limitation of Funds clause, (b(4)) has been allotted to cover the costs and fee incurred in the performance of the services specified in the SOW.~~

(3) The above funds are estimated to cover the period from date of task order award through **January 23, 2009**.

Section H – Special Task Order Provisions

H.1 – General

The contractor shall comply with the terms and conditions of the EAGLE contract in addition to the special provisions set forth in the Task Order RFP.

H.2 – Key Personnel

Under H.2, KEY PERSONNEL, paragraph (b) of the basic contract, the following personnel are determined to be key personnel within the meaning of the provision:

<u>NAME</u>	<u>POSITION</u>
[b(4)]	Program Manager Chief Architect Development/Integration Manager Operations Manager

H.3 - Security Requirements

All of the effort to be performed by this task order will require access/protection of **Secret** information/data. The contractor shall ensure that all appropriate security and protection actions are taken (including providing personnel and procedures) consistent with the task security requirements.

The contractor will have access to and be working with information that is sensitive but unclassified, as defined by the Computer Security Act of 1987. Furthermore, the information is subject to the provisions of the Privacy Act (or any other appropriate law that applies to the information to be handled). This information will be treated as confidential information.

If the contractor is to perform work at their site:

The contractor's facility and ADP systems are required to be accredited and certified in accordance with OMB Circular A-130 Appendix III. Contact DHS' Information System Security Office for additional information.

H.4 – Mandatory Security Requirement – Security Requirements for **Secret** Information Technology Resources

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

agency's mission.

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

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

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

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

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

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

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

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

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.5, September 30, 2007) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

H.5 – Mandatory Security Requirement – Security Review

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS including the Office of Inspector General, Contracting Officers Technical Representative (COTR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against

threats and hazards to the integrity, availability, and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

H.6 – Mandatory Security Requirement – Access to **Secret** Facilities, Information Technology Resources, and Sensitive Information

The assurance of the security of **Secret** facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) **11041 Protection of Classified National Security Information Program Management**, describes how contractors must handle classified information. DHS MD 4300.1 Information Technology Systems Security and the DHS Sensitive Systems Handbooks prescribe policies and procedures on security for IT resources. Compliance with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors is required for all work performed under this contract. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

H.7 – Mandatory Security Requirement – Interconnection Security Agreements

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnect service agreements.

Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both DAAs or by the officials designated by the DAA.

H.8 – Associate Contractors

Performance of this effort may require the task order contractor to work closely with other contractors. The close interchange with associate contractor(s) may require access to, or release of, proprietary or limited/restricted rights data. To facilitate close cooperation and maximum effectiveness, the Contractor shall enter into agreement(s) with associate contractors to adequately protect such data from unauthorized use or disclosure.

H.9 – Drug-Free Workplace

Performance under any task order resulting from this Request for Proposal shall be in accordance with FAR 52.223-6 Drug-Free Workplace.

H.10 – Contractor Personnel – Employment Eligibility

The Contractor will ensure that each employee and potential employee provide his/her name and verify their identity. The Contractor shall be responsible to the Government for acts and omissions of his employees as well as Subcontractor(s) and their employees.

Subject to existing law, regulations and/or other provisions of this contract, illegal or undocumented aliens shall not be employed by the Contractor or perform on this contract. The Contractor shall ensure this provision is expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this contract.

DHS OPS has determined that performance of this contract requires the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), access to **Secret** information. Contractor employees that do not have a security clearance and require access to **Secret** information will be given a suitability determination. Requirements for suitability determination are defined in Section H.15.

H.11 – Contractor Personnel – Continued Eligibility

If a prospective employee is found to be ineligible for access to DHS facilities or information, the Contracting Office Technical Representative (COTR) will advise the Contractor that the employee shall not continue to work or be assigned to work under the contract.

DHS reserves the right to deny and/or restrict entrance to government facilities, prohibit employees from assigned work under the contract, deny and/or restrict handling of classified documents/material to any Contractor employee who DHS determines to present a risk of compromising sensitive Government information.

The Contractor shall report to the DHS Office of Security any and all adverse information brought to their attention concerning employees performing under this contract. Reports based on rumor or innuendo shall not be included. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the employee's name and social security number, along with the adverse information being reported.

H.12 – Contractor Personnel - Termination

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

H.13 – Contractor Personnel – Suitability Determination

DHS shall exercise full control over granting, denying, withholding or terminating unescorted government facility and/or access to or handling of both classified and sensitive Government information to Contractor employees based upon the results of a background investigation. DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full

employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the task order. No employee of the Contractor shall be allowed unescorted access to a DHS facility without a favorable EOD decision or suitability determination by the DHS Office of Security.

H.14 – Contractor Personnel – Background Investigation

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position sensitivity analysis based on the duties, outlined in the Position Designation Determination (PDD) for Contractor Personnel, each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI. Prospective Contractor employees shall submit the following completed forms to OSI through the COTR no less than thirty (30) days before the start date of the contract or thirty (30) days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

- a. Standard Form 85P, "Questionnaire for Public Trust Positions"
- b. FD Form 258, "Fingerprint Card" (2 copies)
- c. DHS Form 11000-6, "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
- d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
- e. Position Designation Determination for Contract Personnel Form
- f. Foreign National Relatives or Associates Statement

Required forms will be provided by DHS at the time of award of the contract. Only complete packages will be accepted by DHS Office of Security. Specific instructions on submission of packages will be provided upon award of the task order.

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

The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this contract for any position that involves access to or development of any DHS Information Technology (IT) systems. DHS OPS will consider only U.S. Citizens and LPRs for employment on this task order. DHS OPS will not approve LPRs for employment on this task order in any position that requires the LPR to access or assist in the development operation, management or maintenance of DHS IT systems. By signing this task order, the Contractor agrees to this restriction. In those instances where other non-IT requirements contained in the contract can be met by using LPRs, those requirements shall be clearly described.

H.15 – Contractor Personnel – Information Technology Security Clearance

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

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

H.16 Contractor Personnel – Information Technology Security Training and Oversight

All Contractor employees using DHS automated systems or processing DHS sensitive data shall be required to receive Security Awareness Training.

Contractors involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of DHS, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. DHS Contractors, with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access DHS information systems will be continually evaluated while performing these duties. Supervisors should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the DHS Security Office.

H.17 – Security Assurances

DHS Management Directive 4300 requires compliance with standards set forth by NIST, for evaluating computer systems used for processing **Secret** information. The Contractor shall ensure that requirements are allocated in the functional requirements and system design documents to security requirements are based on the DHS policy, NIST standards and applicable legislation and regulatory requirements. Systems shall offer the following visible security features:

- User Identification and Authentication (I&A) – I&A is the process of telling a system the identity of a subject (for example, a user) (I) and providing that the subject is who it claims to be (A). Systems shall be designed so that the identity of each user shall be established prior to authorizing system access, each system user shall have his/her own user ID and password, and each user is authenticated before access is permitted. All system and database administrative users shall have strong authentication, with passwords that shall conform to established DHS standards. All DHS Identification and Authentication shall be done using the Password Issuance Control System (PICS) or its successor. Under no circumstances will Identification and Authentication be performed by other than the DHS standard system in use at the time of a systems development.

- Discretionary Access Control (DAC) – DAC is a DHS access policy that restricts access to system objects (for example, files, directories, devices) based on the identity of the users and/or groups to which they belong. All system files shall be protected by a secondary access control measure.
- Object Reuse – Object Reuse is the reassignment to a subject (for example, user) of a medium that previously contained an object (for example, file). Systems that use memory to temporarily store user I&A information and any other Secret information shall be cleared before reallocation.
- Audit – DHS systems shall provide facilities for transaction auditing, which is the examination of a set of chronological records that provide evidence of system and user activity. Evidence of active review of audit logs shall be provided to the OPS IT Security Office on a monthly basis, identifying all security findings including failed log in attempts, attempts to access restricted information, and password change activity.
- Banner Pages – DHS systems shall provide appropriate security banners at start up identifying the system or application as being a Government asset and subject to government laws and regulations. This requirement does not apply to public facing internet pages, but shall apply to intranet applications.

H.18 – Data Security

SBU systems shall be protected from unauthorized access, modification, and denial of service. The Contractor shall ensure that all aspects of data security requirements (i.e. confidentiality, integrity, and availability) are included in the functional requirements and system design, and ensure that they meet the minimum requirements as set forth in the DHS Sensitive Systems Handbook and policies and procedures. These requirements include:

- Integrity – The computer systems used for processing SBU shall have data integrity controls to ensure that data is not modified (intentionally or unintentionally) or repudiated by either the sender or the receiver of the information. A risk analysis and vulnerability assessment shall be performed to determine what type of data integrity controls (e.g., cyclical redundancy checks, message authentication codes, security hash functions, and digital signatures, etc.) shall be used.
- Confidentiality – Controls shall be included to ensure that SBU information collected, stored, and transmitted by the system is protected against compromise. A risk analysis and vulnerability assessment shall be performed to determine if threats to the SBU exist. If it exists, data encryption shall be used to mitigate such threats.
- Availability – Controls shall be included to ensure that the system is continuously working and all services are fully available within a timeframe commensurate with the availability needs of the user community and the criticality of the information processed.
- Data Labeling. – The contractor shall ensure that documents and media are labeled consistent with the DHS Sensitive Systems Handbook.

H.19 – DHS Information Technology Standards – Homeland Security Enterprise Architecture (HLS EA) Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures as it relates to this Task Order. Specifically, the contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

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

H.20 – Section 508 of the Rehabilitation Act

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

All EIT deliverables, including but not limited to IOE Implementation Plans, within this work statement shall indicate how compliance with Section 508 standards will be accomplished for both products and services and shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable standards have been identified:

36 CFR 1194.21 – Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this task order including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

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

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

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

36 CFR 1194.25 – Self Contained, Closed Products, applies to all EIT products such as printers, copiers, fax machines, kiosks, etc. that are procured or developed under this task order. Specifically but not limited to items using biometrics as described in this work order shall apply with this requirement as well as any other technical standard involving the use of software or Web based interfaces.

36 CFR 1194.26 – Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.

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

36 CFR 1194.41 – Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required “1194.31 Functional Performance Criteria”, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this task order that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Exceptions for this task order have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

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

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

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

H.21 – Advertisements, Publicizing Awards, and News Releases

All press releases or announcements about agency programs, projects, and contract (task order) awards need to be cleared by the Program Office and the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity news release or commercial advertising without first obtaining explicit written consent to do so from the Program Office and the Contracting Officer.

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

Section I – Task Order Clauses

Federal Acquisition Regulation (48 CFR Chapter 1) Solicitation Clauses (<http://www.arnet.gov/far/>)

FAR Clause No.	Title	Date
52.251-1	Government Supply Sources	Apr 1984
52.204-2	Security Requirements	Aug 2006
52.204-9	Personal Identity Verification of Contractor Personnel	Sep 2007
52.215-19	Notifications of Ownership Changes	Oct 1997
52.215-21	Requirements For Cost Or Pricing Data Or Information Other Than Cost Or Pricing Data – Modifications Alternate IV	Oct 1997
52.232-20	Limitation Of Costs	Apr 1984
52.232-22	Limitation Of Funds	Apr 1984
52.217-8	Option To Extend Services (Fill-in: 30 days)	Nov 1999
52.219-8	Utilization Of Small Business Concerns	May 2004
52.219-9	Small Business Subcontracting Plan	Sep 2006
52.227-14	Rights In Data – General Alternates IV And V	Jun 1987
52.227-21	Technical Data Declaration Revision And Withholding Of Payment – Major Systems	Jan 1997
52.232-18	Availability Of Funds	Apr 1984
52.237-3	Continuity of Services	Jan 1991
52.244-6	Subcontracts For Commercial Items	Mar 2007
52.245-1	Government Property	Jun 2007
52.245-2	Government Property Installation Operation Services	Jun 2007

DHS AND FAR CLAUSES

Homeland Security Acquisition Regulation (HSAR) Clauses Incorporated By Reference
(<http://farsite.hill.af.mil/vfhsara.htm>)

HSAR Clause No.	Title	Date
3052.204-70 (EAGLE I.2)	Security Requirements for Unclassified Information Technology Resources	Dec 2003
3052.204-71 (EAGLE I.13)	Contractor Employee Access	Jun 2006
3052.209-70 (EAGLE I.3)	Prohibitions on Contracts with Corporate Expatriates	Dec 2003
3052-209-72 (EAGLE H.33)	Organizational Conflict of Interest	Jul 2004
3052-209-73	Limitation of Future Contracting	Jul 2004
3052.222-70	Strikes or Picketing Affecting Timely Completion of the Contract Work	Dec 2003
3052.222-71	Strikes or Picketing Affecting Access to a DHS Facility	Dec 2003
3052.245-70	Government Property Reports	Jun 2006
If Applicable (EAGLE Ref):		
3052.216-72 (I.7)	Performance Evaluation Plan	Dec 2003

- END OF TASK ORDER PROVISIONS AND CLAUSES -

Section J – List of Attachments

List of Attachments

~~Attachment J-1 – Performance Work Statement~~

Attachment J-2 – Functional Requirements Document

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT ID CODE	PAGE OF PAGES 1 1
2. AMENDMENT/MODIFICATION NO. P00002	3. EFFECTIVE DATE 06/12/2008	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (if applicable)
6. ISSUED BY Department of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528	CODE DHS/OPO/ITAC	7. ADMINISTERED BY (if other than Item 6) Department of Homeland Security Office of Procurement Ops. (ITAC) 245 Murray Drive Bldg. 410 Washington DC 20528	CODE DHS/OPO/ITAC
8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) GENERAL DYNAMICS ONE SOURCE LLC 3211 JERMANTOWN ROAD FAIRFAX VA 22030		(x) 9A. AMENDMENT OF SOLICITATION NO.	9B. DATED (SEE ITEM 11)
CODE 6103202150000	FACILITY CODE	x 10A. MODIFICATION OF CONTRACT/ORDER NO. HSHQDC-06-D-00024 HSHQDC-08-J-00134	10B. DATED (SEE ITEM 11) 05/23/2008

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 6 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)
See Schedule

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

CHECK ONE	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 data, 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 _____ copies to the issuing office.

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

DUNS Number: 610320215+0000

The purpose of this modification is to incorporate the attached DD form 254.

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)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Purnell Drew
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED
	16B. UNITED STATES OF AMERICA (b(6))
	16C. DATE SIGNED 06/12/2008

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING	
				a. FACILITY CLEARANCE REQUIRED SECRET	
				b. LEVEL OF SAFEGUARDING REQUIRED NONE	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)			3. THIS SPECIFICATION IS: (X and complete as applicable)		
<input checked="" type="checkbox"/>	a. PRIME CONTRACT NUMBER HSHQDC-06-D-00024 HSHQDC-08-J-00134		<input checked="" type="checkbox"/>	a. ORIGINAL (Complete date in all cases)	Date (YYYYMMDD) 20080611
	b. SUBCONTRACT NUMBER			b. REVISED (Supersedes all previous spacs)	Revision No. Date (YYYYMMDD)
	c. SOLICITATION OR OTHER NUMBER	Due Date (YYYYMMDD)		c. FINAL (Complete item 5 in all cases)	Date (YYYYMMDD)
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input checked="" type="checkbox"/> 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? <input type="checkbox"/> YES <input checked="" type="checkbox"/> 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 GENERAL DYNAMICS ONE SOURCE, LLC 3211 Jermantown Road Fairfax, VA 22030			B. CAGE CODE 474R7	C. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) Defense Security Service (DSS) 14428 Albemarle Point Place Ste. 140 Chantilly, VA 20151	
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE			B. CAGE CODE	C. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
8. ACTUAL PERFORMANCE					
a. NAME, ADDRESS, AND ZIP CODE Department of Homeland Security (DHS) NAC location within the greater Wash, DC metropolitan area and the contractor's site.			B. CAGE CODE 474R7	C. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) Defense Security Service (DSS) 14428 Albemarle Point Place Ste. 140 Chantilly, VA 20151	
9. GENERAL IDENTIFICATION OF THE PROCUREMENT (U) Provide engineering support to the HSIN system for the Office of Procurement Operations.					
10. THIS CONTRACT WILL REQUIRE ACCESS TO:		YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
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		l. OTHER (Specify)	
k. OTHER (Specify)			X		X

DD Form 254, DEC 1999

Previous editions are obsolete

RESET

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 Through (Specify): NONE AUTHORIZED

UNLESS CONTRACTOR HAS OBTAINED AUTHORITY TO RELEASE FROM THE DEPARTMENT OF HOMELAND SECURITY: CONTRACTOR SHALL COORDINATE WITH THE COTR AND THE OFFICE OF SECURITY (ASD) ON ALL CHANGES TO THIS GUIDANCE 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 10j: "Contractors shall control and safeguard FOUO in accordance with DHS Directive (MD11042.1) "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 (202) 447-5341."

Reference 11a: *Contract performance is restricted to General Dynamics One Source, LLC 3211 Jermantown Road, Fairfax, VA 22030, and at Department of Homeland Security (DHS), Nebraska Avenue Complex (NAC), Washington, DC 20528* and various locations within the greater Washington, DC metropolitan area, National Capitol Region and other Government facilities. Cleared personnel are required to perform this service. All contractor personnel must: be U.S. citizens, have been granted a security clearance by the U.S. Government, have been approved as meeting criteria by DHS CSO, and have been indoctrinated by a Non Disclosure Agreement, Standard Form 312 for this specific program prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are not eligible for access to classified information released or generated under this contract. Classified material released or generated under this contract is not releasable to foreign nationals without the expressed written permission of the CSO. **Recipients of classified information under this contract may not be released to subcontractors without permission of the DHS CSO.**

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 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.)

Yes No

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 JOSE J. SALAZAR (b(2) b(6))	b. TITLE PROGRAM MANAGER, INDUSTRIAL SECURITY	c. TELEPHONE (Include Area Code) (202)-447-(612)
---	---	--

d. ADDRESS (Include Zip Code)
DEPARTMENT OF HOMELAND SECURITY
301, 7TH & D ST. S.W.
WASHINGTON DC 20528

e. SIGNATURE
(b(6))

17. REQUIRED DISTRIBUTION

<input checked="" type="checkbox"/>	a. CONTRACTOR
<input type="checkbox"/>	b. SUBCONTRACTOR
<input checked="" type="checkbox"/>	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
<input type="checkbox"/>	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
<input checked="" type="checkbox"/>	e. ADMINISTRATIVE CONTRACTING OFFICER
<input checked="" type="checkbox"/>	f. OTHERS AS NECESSARY