ORDER FOR SUPPLIES OR SERVICES

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

1. DATE OF ORDER: 5/14/08

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

3. ORDER NO.: HSHQDC-08-J-00116

4. REQUISITION/REFERENCE NO.: RNCP-08-00005

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

6. SHIP TO:
a. NAME OF CONSIGNEE
b. STREET ADDRESS
c. CITY
d. STATE
e. ZIP CODE

7. TO:
a. NAME OF CONTRACTOR: GENERAL DYNAMICS ONE SOURCE LLC
b. COMPANY NAME
c. STREET ADDRESS: 3211 JERMANTOWN ROAD
d. CITY: FAIRFAX
e. STATE: VA
f. ZIP CODE: 22030

f. SHIP VIA

8. TYPE OF ORDER
[ ] a. PURCHASE
REFERENCE YOUR:
Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.

[X] b. DELIVERY
Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA: See Schedule

10. REQUISITIONING OFFICE: Department of Homeland Security

11. BUSINESS CLASSIFICATION *(Check appropriate box(es))*
[ ] a. SMALL
[X] b. OTHER THAN SMALL
[ ] c. DISADVANTAGED
[ ] g. SERVICE-DISABLED VETERAN-OWNED
[ ] d. WOMEN-OWNED
[ ] e. HUBZone
[ ] f. EMERGING SMALL BUSINESS

12. F.O.B. POINT: Destination

13. PLACE OF
a. INSPECTION: Destination
b. ACCEPTANCE: Destination

14. GOVERNMENT B/L NO.

15. DELIVER TO F.O.B. POINT ON OR BEFORE *(Date)*

16. DISCOUNT TERMS: Net 30

17. SCHEDULE *(See reverse for Rejections)*

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

18. SHIPPING POINT

19. GROSS SHIPPING WEIGHT

20. INVOICE NO.

17(h) TOTAL *(Cont. pages)*: $3,598,217.00

21. MAIL INVOICE TO:
a. NAME: Department of Homeland Security
b. STREET ADDRESS (or P.O. Box): Departmental Operations Branch
Room 3621
245 Murray Lane, SW
Building 410
c. CITY: Washington
d. STATE: DC
e. ZIP CODE: 20528

SEE BILLING INSTRUCTIONS ON REVERSE

17(i) GRAND TOTAL: $3,598,217.00

22. UNITED STATES OF AMERICA
BY *(Signature)*: (b)(6) 5/14/08

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

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

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

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-08-J-00116

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	This is a time and materials task order under the Enterprise Acquisition Gateway Leading Edge (EAGLE) (Functional Category 1) to provide professional services to National Infrastructure Coordinating Center (NICC) for Insight Support. (a) The original invoice shall be submitted to the Finance Office designated herein. Copies of the invoice shall be submitted to the COTR and the Contracting Officer concurrently. Email addresses are provided herein for the copies. (b) To constitute a proper invoice, the invoice must include those items cited in FAR clause 52.232-7, Payments under Time-and-Materials and Labor-Hours Contracts, and FAR 52.232-25, Prompt Payment, paragraphs (a)(3)(i) through (a)(3)(x). Finance Office: NPPDVENDORINVOICES@DHS.GOV COTR: [redacted] ACO: [redacted] (b)(6) The following labor categories are applicable for the period of performance 05/14/08-05/13/09 [redacted] (b)(4) Continued ...					

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

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-08-J-00116

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	Admin Office: Department of Homeland Security Office of Procurement Ops. (ITAC) 245 Murray Drive Bldg. 410 Washington DC 20528 Period of Performance: 05/14/2008 to 05/13/2009					
0001	The contractor shall provide professional services and data in accordance with the Statement of Work entitled "National Infrastructure Coordinating Center (NICC) INSight Support" dated March 3, 2008. (Not Separately Priced)	1	LO			
0001AA	Task 1.0 INSIGHT System Design and Development Accounting Info: 400MPAD 000 M8 4060-11-400 01-06-0000-00-00-00-00 GE-OE-25-11 CP805 Funded: (b)(4)					
0001AB	Task 2.0 Master Watch Control Log (MWCL) Techncial Support Accounting Info: 400MPAD 000 M8 4060-11-400 01-06-0000-00-00-00-00 GE-OE-25-11 CP805 Funded: (b)(4)					
0001AC	Task 3.0 Data Repository Layer Support Accounting Info: 400MPAD 000 M8 4060-11-400 01-06-0000-00-00-00-00 GE-OE-25-11 CP805 Funded: (b)(4)					
0001AD	Task 4.0 Development and Management of Information and User Interface Layers Accounting Info: Continued ...					

(b)(4)

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

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-08-J-00116

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	400MPAD 000 M8 4060-11-400 01-06-0000-00-00-00-00 GE-OE-25-11 CP805 Funded: (b)(4) Accounting Info: 300MPAD 000 K8 6030-11-300 01-06-0000-00-00-00-00 GE-OE-25-11 CP8005 Funded (b)(4)					
0001AE	Task 5.0 NICC Web-Page Development and Support Accounting Info: 300MPAD 000 K8 6030-11-300 01-06-0000-00-00-00-00 GE-OE-25-11 CP8005 Funded: (b)(4)				(b)(4)	
0001AF	Task 6.0 Development of Mock-ups Accounting Info: 300MPAD 000 K8 6030-11-300 01-06-0000-00-00-00-00 GE-OE-25-11 CP8005 Funded: (b)(4)					
0001AG	Task 7.0 Work Flow Evaluation and Improvement Accounting Info: 300MPAD 000 K8 6030-11-300 01-06-0000-00-00-00-00 GE-OE-25-11 CP8005 Funded: (b)(4)					
0001AH	Task 8.0 System Architecture Requirements Accounting Info: 300MPAD 000 K8 6030-11-300 01-06-0000-00-00-00-00 GE-OE-25-11 CP8005 Funded: (b)(4)					
0001AJ	Task 9.0 Reporting, Schedule, and Meetings Continued ...					

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

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-08-J-00116

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	Accounting Info: 300MPAD 000 K8 6030-11-300 01-06-0000-00-00-00-00 GE-OE-25-11 CP8005 Funded: (b)(4)				(b)(4)	
0001AK	Task 10.0 Certification and Accreditation Support Accounting Info: 300MPAD 000 K8 6030-11-300 01-06-0000-00-00-00-00 GE-OE-25-11 CP8005 Funded: (b)(4)					
0001AL	Task 11.0 INSight System Support Accounting Info: 300MPAD 000 K8 6030-11-300 01-06-0000-00-00-00-00 GE-OE-25-11 CP8005 Funded: (b)(4) Accounting Info: 300MPAD 000 K8 6030-30-300 01-06-0000-00-00-00-00 GE-OE-25-11 CP8005 Funded: (b)(4)					
0001AM	Task 12.0 Transition Plan Accounting Info: 300MPAD 000 K8 6030-30-300 01-06-0000-00-00-00-00 GE-OE-25-11 CP8005 Funded: (b)(4)					
0001AN	Task 13.0 Project Management Accounting Info: 300MPAD 000 K8 6030-30-300 01-06-0000-00-00-00-00 GE-OE-25-11 CP8005 Funded: (b)(4)					
0002	Other Direct Costs (Not Separately Priced) Continued ...	1	LO			

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

SCHEDULE - CONTINUATION

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-06-D-00024	HSHQDC-08-J-00116

TEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
0002AA	Travel shall be in accordance with the Federal Travel Regulations (FTR), Not-to-Exceed (b)(4) a reimbursable basis. Accounting Info: 300MPAD 000 K8 6030-30-300 01-06-0000-00-00-00-00 GE-OE-25-11 CP8005 Funded: (b)(4)				(b)(4)	
0002AB	Equipment, Not-to-Exceed $285,500.00 on a reimbursable basis. Accounting Info: 300MPAD 000 K8 6030-30-300 01-06-0000-00-00-00-00 GE-OE-25-11 CP8005 Funded: (b)(4) Contractor Acceptance: (b)(6) Lead Contracts Specialist for General Dynamics/Printed Name/Title (b)(6) 5/13/08 Signature Date The total amount of award: $3,598,217.00. The obligation for this award is shown in box 17(i).					

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

STATEMENT OF WORK

March 3, 2008

Contracting Officer Technical Representative (COTR): Gregory McShane

Alternate Contracting Officer Technical Representative (ACOTR): TBD

1. **PROJECT TITLE:** National Infrastructure Coordinating Center (NICC) INSight Support.

2. **BACKGROUND:** As the operational arm for the DHS Office of Infrastructure Protection (OIP) and a core component of the National Operations Center (NOC), the NICC is responsible for communicating infrastructure-related information to numerous government and industry partners. NICC Watch Analysts search for operational anomalies; coordinate with the NOC, OIP, and other government agencies; perform initial analysis with industry, when warranted; and participate in tests and exercises to maintain preparedness and improve coordination. During incidents and events, the NICC assesses and triages information from a variety of resources and conducts initial analysis of the incidents and events.

   The NICC is also responsible for generating the following products:

   - **Patriot Reports** – The NICC receives reports of suspicious activities and potential terrorist threats from the private sector. This information is assembled and is disseminated to the Information Coordination Analysis Office (ICAO) Sector Specialists and agencies within the NOC. This information has the potential to be included in the Secretary's Morning Brief, the Homeland Security Operations Morning Brief, Homeland Security Information Messages, Information Bulletins, DHS Advisories, or other DHS generated reports.
   - **Spot Reports** – The NICC generates and disseminates Spot Reports of serious emerging incidents or events. These reports provide current situation status and a snapshot assessment of operational impacts that resulted.
   - **Current Situation Reports** – These reports are usually created for various incidents or events that have continued past 24-48 hours. The reports are produced at regularly scheduled intervals as determined by leadership and provide detailed assessments of operational impacts.
   - **Daily Sector Pulse Report** – This report highlights operational anomalies across the critical infrastructures and key resources for the previous 24 hour period.

- **Critical Infrastructure/Critical Resources (CI/KR) Quicklook** – This report provides a geo-spatial depiction of critical infrastructures and key resources within an area surrounding a developing incident or potential incident.

During major incidents/events, the NICC serves as a 24x7 customer service interface for CI/KR partners by collecting (via email and phone), tracking, and facilitating responses to requests for information and assistance. Additionally, the NICC conducts daily teleconferences with CI/KR stakeholders, in close coordination with Sector Specific Agencies and Sector Specialists, to provide situational awareness to industry partners. Lastly, the NICC provides access to approved DHS Situation Reports, bulletins, press releases, and other important documents to serve industry partners' continuity-of-business information needs.

The NICC operates the INSight Information Management System (formerly known as Prizm), designed to support the identification of potentially significant changes in the operational status of the nation's Critical Infrastructures and Key Resources (CI/ KR) so that trained analysts can provide timely coordination with the NOC, respective Information Sharing and Analysis Centers (ISAC), and other involved agencies in the public sector and federal sectors. INSight also supports the NICC's business processes by creating an infrastructure that helps to enable the operational management of the NICC Watch and associated support functions.

The high-level functional architecture of INSight is comprised of four layers: the data source layer, the data repository layer, the information management layer (formerly referred to as the "applied knowledge management layer"), and the user interface layer. The INSight system currently consists of a development environment, testing and training environment, and operational environment all hosted at the current contractor site in Fairfax, Virginia.

3. **SCOPE:** Functional Category 1. Requirements definition process, development of operational tools, and the further build out of an INSight operational and back up system environment to support the NICC Watch Operations full software-development lifecycle management, and 24x7 system operations and user-level support.

4. **APPLICABLE DOCUMENTS:**

4.1 Information Assurance Policy. The information management program will use the following documents that describe information assurance processes and standards. All documents are available in the Chief Information Security Officer section of DHS Online or from the DNI Special Security Center website on the Joint Worldwide Intelligence Communications System (JWICS). (Vendors lacking access to these information sites can request a CD ROM):

4.1.1 DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems, 5 Jun 1999.

4.1.2 DHS National Security Systems Policy Directive 4300B Version 4.2, 29 Sept 2006.

4.1.3 DHS National Security Systems Handbook 4300B Version 4.2, 29 Sept 2006.

4.1.4 DHS National Security Systems Policy Directive 4300A Version 4.2, 29 Sept 2006.

4.1.5 DHS National Security Systems Handbook 4300A Version 4.2, 29 Sept 2006.

4.1.6 DHS Windows Secure Baseline Configuration Guide, Version 2.0, 31 May 2006.

4.1.7 DHS MD 4300.1 Information Technology Systems Security, undated.

4.2 The following DHS Management Directives are also applicable and may also be found on DHS Online:

4.2.1 DHS Interim MD 1400, 3 Mar 2006.

4.2.2 DHS MD 8200.1 Information Quality, undated.

4.2.3 DHS MD 4510 Domain Names, 14 Sept 2004.

4.2.4 DHS MD 0470.2 Privacy Act Compliance, 6 Oct 2005.

4.2.5 DHS MD 0007.1 Information Technology Integration and Management, 15 Mar 2007 with Addendum A.

4.2.6 DHS MD 1400.1 IT Capital Planning and Investment Control (CPIC) and Portfolio Management.

4.2.7 OI&A-DOC-IT_Policy-v1.0-20051028 Office of Intelligence & Analysis (I&A) Policy Information Technology Governance.

4.2.8 DHS MD 4010.2 Section 508 Program Management Office & Electronic and Information Technology Accessibility

Web Link to referenced documents:
https://dhsonline.dhs.gov/portal/jhtml/community.jhtml?index=10&community=MGMT&id=2002980003

5. SPECIFIC TASKS

TASK 1.0 – INSight System Design and Development

The contractor shall provide for the overall required level of professional, technical, and administrative services and staff to support the further development of the INSight System. This includes concept development, planning, requirements definition and analysis, system design and development, integration, implementation, and deployment of new releases and upgrades to the INSight system.

1.1 The contractor shall design and develop enhancements to the INSight system including new releases and upgrades in accordance with the DHS HLSEA, Global Justice XML Data Model (Global JXDM) and National Information Exchange Model. The final locations of these three system subcomponents (development, test and training and

operational environments) will be determined by the COTR and be in accordance with the DHS CIO and NPPD CIO policies. The INSight system shall also be designed in a manner that will allow it to complete the defined DHS Certification and Accreditation system requirements.

TASK 2.0 – Master Watch Control Log (MWCL) Technical Support

2.1 The data source layer consists of inputs from multiple sources which are logged into the NICC Master Watch Control Log (MWCL) and ingested into the INSight system. The contractor shall maintain the MWCL.

2.2 The contractor shall perform minor modifications (e.g., interface changes) to the MWCL. Any such modifications will be addressed with the contractor during Configuration Control Board (CCB) sessions and with prior approval of the NPPD CIO ERB (Engineering Review Board). Following the CCB and ERB sessions, the contractor shall be given adequate time to develop and submit the scope of work and level of effort estimates required to complete the required modification, design and specification documentation, and, if applicable, associated risk assessments.

2.3 The contractor shall also maintain a detailed software and system architecture work schedule in order to effectively manage the overall system (e.g. Updates to the inventory, managing software and hardware enterprise architecture requests/approvals, upcoming purchases, licenses/agreements, and updates to Service Level Agreements)

TASK 3.0 - Data Repository Layer Support

3.1 The data repository layer houses and maintains both the near real-time and historical data that feeds the INSight system. The contractor shall develop the requirements-definition packages for additional database requirements to support the evolving system. These requirements will be gathered primarily through meetings with the NICC government management and representatives from other program offices.

3.2 The contractor shall design, develop, and perform software lifecycle management processes required to ensure effective use of DHS' Oracle 10g (and follow-on release) software environment. At a minimum, this shall be completed as part of each INSight system upgrade or release.

TASK 4.0 – Development and Management of Information and User Interface Layers

4.1 The information management and user interface layers will leverage the data repository to support and enhance the ability for NICC Watch Analysts to perform their mission-related responsibilities. The contractor shall design and test the necessary coding to implement the requirements-definition packages for the following:

- Integration with the Homeland Security Information Network-Critical Sectors (HSIN-CS),
- integration with Integrated Common Analytical Viewer (iCAV) as the geospatial platform/user interface,
- Protected Critical Infrastructure Information (PCII) processing,
- incorporation of an Executive Notification System (ENS) such as Wide Area Rapid Notification (WARN) tool and
- an information-exchange solution with the DHS Common Operational Picture (COP).

This shall include, but is not limited to, the transfer of the applicable data using standard Web Services between the MWCL, HSIN-CS, and the iCAV system.

4.2 The contractor shall provide a web-based system Executive Notification System (ENS) Commercial Off The Self (COTS) product and service such as WARN, that is used to provide the OIP and DHS leadership with the capability to notify critical infrastructure representatives of key conference calls/meetings, critical events, changes to threat levels, or emergency notifications (as defined by IP). The system at a minimum should have the following capabilities:

- ENS messages are recorded
- Response options are customizable
- Broadcast duration can be altered
- Notifications can be sent to groups or individuals on numerous devices simultaneously
- Groups are customizable by the end user.

ENS shall be operational within 10 days of contract award. The proposed ENS shall be reviewed and approved by the COTR.

4.3 The contractor shall develop technical plans to integrate and display NICC email into the INSight system as well as expand the INSight user-base to other Office of Infrastructure Protection elements.

TASK 5.0 - NICC Web-Page Development and Support

5.1 The contractor shall design and maintain the NICC web-page for use on the internet and DHS intranet. The content of the Web page will be provided through meetings and consultations with NICC staff. The Web page shall be in accordance with DHS standards and policies.

TASK 6.0 - Development of Mock-ups

6.1 The contractor shall develop graphical mock-ups (e.g., functional diagrams) as necessary to support the design, test and implementation of various efforts. At a minimum, this shall be completed as part of each INSight system upgrade or release.

TASK 7.0 - Work Flow Evaluation and Improvement

7.1 The contractor shall maintain and update the necessary work flows for NICC reporting. Examples of this include: Situation Reports (SITREPS), EXSUM inputs, Request for Information (RFI), Request for Action (RFA), Assistant Secretary, Infrastructure Protection (ASIP), Daily Update, or other reporting/business processes. At a minimum, this shall be completed as part of each INSight system upgrade or release.

TASK 8.0 - System Architecture Requirements

8.1 The contractor shall provide a system solutions for INSight upgrades and new releases utilizing commercial off the shelf (COTS) products and reside on the existing hardware architecture. When the entire user base of the system is established (e.g., local and deployed OIP analysts and watch personnel, management personnel, additional DHS elements and security partners, etc.), the system shall provide maximum flexibility with regard to allowing and controlling access in accordance with DHS Policy 4300B.

8.2 The contractor shall ensure that the system encompasses an open architecture design (both hardware and software). The contractor shall develop the necessary software and hardware accountability processes to ensure 100% accountability of all software and hardware purchased under this effort. The contractor shall further ensure that all hardware and software maintenance for the INSight system is kept up to date. The contractor shall maintain a comprehensive inventory list as applicable including equipment/software name, date of purchase, date of expiration, model/license number, serial number, and quantity. The equipment/software shall be inventoried on a biannual schedule and the inventory submitted to the COTR.

8.3 The contractor shall develop and implement a system architecture that allows for the three separate environments (development, testing/training, and operational) to be located at sites designated by the DHS OCIO, the NPPD OCIO, COTR and NICC management.

8.4 The contractor shall provide management and technical support in evaluating, developing, determining, and relocating the INSight system to the most logical and economical options available for housing and operating the INSight system environment. This shall include: working with DHS OCIO, the NPPD CIO and NICC Management in determining what these options are, developing a phased approach working toward an eventual long term solution, evaluating the Business Continuity/Disaster Recovery and Continuity of Operations (COOP) elements necessary to ensure redundancy while supporting the overall NICC mission, developing the necessary Service Level Agreements (SLA – see section 8.5) necessary in teaming with the INSight Systems hosts, and supporting the move management for relocating the INSight operating and backup systems. The contractor shall perform a site assessment and provide a site assessment report to one designated location approximated 700 miles driving distance from Washington, DC for an approximated duration of 5 business days.

8.5 The contractor shall develop a Service Level Agreement (SLA) between the NICC and "the contractor" for supporting the INSight system. This shall include: definition of services, problem management, customer duties, warranties, Business Continuity/Disaster Recovery (Recovery Time Objectives, Recovery Point Objectives), Termination of Agreement, performance measures for Transaction Response Time (both end user and internal), application availability, application performance, outages (emergency, priority, regular and unscheduled) and network capacity planning/management.

8.6 The contractor shall develop a system software lifecycle management process that allows for each base software package to be tracked with version controls, as well as providing management for all custom-developed software used in the INSight architecture.

8.7 The contractor shall develop and deliver additional technical evaluations and studies to support the design, development and future releases of INSight. These deliverables may include: systems-integration assessments, vendor/product evaluations, and technical white papers.

TASK 9.0 – Reporting, Schedule, and Meetings

9.1 The Contractor shall prepare and submit monthly status/progress reports. These reports shall be submitted to the Contracting Officer's Technical Representative (COTR). Status/progress reports shall discuss the status of all on-going work about specific tasks listed in the SOW. At a minimum, each progress report shall contain a description of:

- work performed during the reporting period just ended to include numerical amounts for each task.
- work to be performed during the next reporting period
- any planned travel including travel objectives
- any problems encountered with corrective action proposed or taken and a statement about the potential impact of the problem
- any government action requested
- an estimate of the percent complete for each task
- cost reimbursable or time and materials tasks only
- hours and funds expended to-date and for the reporting period just ended

The contractor shall document these activities accomplished, upcoming activities/deliverables, action items, any risks to the schedule, scope, or budget, as well as any outstanding issues. Documentation shall include a roll up of the previous weekly activities and include the final week of activities for the month and an updated project schedule (MS Project).

9.2 The contractor shall gather documentation to report project status for regular reporting and management of IT projects in the NPPD CIO Portfolio.

9.3 The contractor shall update system and operational development and quality control schedules. The contractor shall evaluate all management-approved enhancements and change requests for level of effort. In conjunction with the COTR, the contractor shall evaluate the impact upon overall development schedules. All changes to the overall schedule shall be briefed to the CCB and approved by the CCB chair or the COTR and reported to the CO.

9.4 The contractor's project manager shall attend a status meeting every other Tuesday, at a minimum, at the NICC facility in Herndon, Virginia, to discuss items included in the weekly activity reports or issues from CCB briefs or discussions with the COTR. The Contractor shall maintain minutes of meetings during which the progress of the work is discussed. The Contractor shall submit the meeting minutes to the COTR. The CCB meeting minutes shall highlight any decisions reached, agreements made, or actions to be taken. The Contractor shall also prepare and submit an exception report describing any problems encountered that may impact the government adversely, require clarification or action by the government, require documentation, or result in a deviation from the approved work plan.

TASK 10.0 - Certification and Accreditation Support

10.1 The contractor shall ensure that the INSight system meets all DHS requirements in accordance with DHS Sensitive Systems Policy Directive 4300A and its companion, DHS 4300B Sensitive Systems Handbook, and DHS National Security Systems Policy Directive 4300B and its companion, DHS 4300B National Security Systems Handbook. Therefore, in conjunction with the COTR and NICC management, the contractor shall participate in C&A planning/training sessions and work directly with the DHS IT Security points of contacts, processes and system tools to ensure compliance with DHS policy. Additionally, as a result of these sessions, the contractor shall be required to produce or update C&A-related documentation to include but not be limited to: Incident Response Plan (IRP), Plan of Execution, Business Continuity/Disaster Recovery (BC/DR) Plan, System Security Plan (SSP), Privacy Impact Assessments and estimated timelines. Certification and Accreditation documents shall also be uploaded through the NPPD and DHS OCIO systems. In addition, the system shall comply with all Privacy Act requirements and the DHS Sensitive System Handbook.

10.2 The contractor shall ensure that the INSight system is maintained in accordance with all required DHS and NIST security policies and requirements so that the system can process and maintain Disaster Management, Homeland Security, Law Enforcement, and Internal Risk and Management data, as well as Protected Critical Infrastructure Information, and USPERSONs information. As the INSight system changes are made with further upgrades and enhancements, the Contractor shall ensure further Certification and Accreditation requirements are met. The contractor shall notify the Government within 24 hours if the INSight system IT Security requirements are discovered or compromised. At a minimum, the contractor shall update the Certification and Accreditation on an annual basis and after major upgrades and changes to the INSight system or as directed by the NPPD OCIO.

10.3 The contractor will ensure the INSight system obtains and maintains a DHS Interim or Full CIO Authority to Operate, and complies with all DHS requirements in accordance with DHS Certification and Accreditation Guidance for Sensitive But Unclassified (SBU) Systems User's Manual. The contractor shall ensure that all FIPS-199 controls are maintained and managed to allow INSight to operate in a manner allowing High confidentiality, High Integrity, and High Availability in accordance with Federal Information Processing Standards Publication (FIPS) 199 "Standards for Security Categorization of Federal Information and Information Systems.

TASK 11.0 - INSight System Support

11.1 The contractor shall staff for the 24x7 system operations and user-level support, to the NICC. The INSight system support includes the necessary day-to day operations and maintenance to sustain an INSight application availability (up time) of 99.999 percent.

11.2 The contractor shall provide services as needed for technical support, training, and troubleshooting to the NICC Watch's MWCL application. This technical support shall ensure that any NICC Watch Management and/or Watch Standers have a technical point of contact that is reachable by either office phone (M-F 7am to 5pm) or pager (M-F 5pm to 7am; 24 hours weekends and holidays).

11.3 The contractor shall ensure that the INSight system is operated and maintained in accordance with the DHS Homeland Security Enterprise Architecture (HLS EA), Global Justice XML Data Model (Global JXDM) and National Information Exchange Model.

11.4 The contractor shall provide and document system performance compliance based on the critical applications that support INSight. Application performance (transaction response time) measurement at most is limited by current technology, network configuration, capacity of the system, or other elements that could impact performance. The contractor shall complete performance measurements through a sampling of represented commands over a period of time. If system performance is identified as a consistent problem, the contractor shall provide the necessary efforts to define the extent of the problem and determine appropriate action to correct the problem. The contractor shall document system performance monthly and include it monthly report requirement in Task 9.

TASK 12.0 - Transition Plan

The contractor shall prepare a transition plan to transition the INSight system (hosted or moved) to a DHS approved data center or location for the initial phase (contract award). The final determination for the location of the INSight system is described in Task 8.

TASK 13.0 Final Project Management

The objective of this task is to manage the contract process by maintaining cost control, schedule, and quality of all services and products. The Contractor shall determine the project organization and overall management required to accomplish the task order.

6. DELIVERABLES AND DELIVERY SCHEDULE

All Reports and deliverables shall be submitted electronically in MS 2003 Word, Excel, or Project directly to the COTR. The Monthly Status/Progress Reports shall be submitted to both the COTR and the Contract Specialist.

SOW/ Task #	Deliverable Title	Due Date
2.3	Software and System Architecture Work Schedule	3rd Business Day of the Month
3.1	Requirements-Definition Packages	30-365 calendar days after task order award
3.2	Software Lifecycle Management Processes	30-365 calendar days after task order award
4.1	Design and Test Coding	30-365 calendar days after task order award
4.2	Emergency Notification System	10 calendar days after task order award
4.3	Email Integration Plan	30-365 calendar days after task order award
5.1	NICC Web Page	30-365 calendar days after task order award
6.1	Mock-ups	30-365 calendar days after task order award
7.0	Work Flow Evaluation and Improvement	30-365 calendar days after task order award
8.2	Accountability Processes Document	Draft: 30 calendar days after Task Order Award Final: 45 calendar days after Task Order Award
8.2	Hardware/Software Inventory	5/31/2008 12/31/2008
8.3	System Architecture Documentation	Draft: 30 calendar days after Task Order Award Final: 45 calendar days after Task Order Award

SOW/ Task #	Deliverable Title	Due Date
8.4	Site Assessment Report	30 Day after Site Visit
8.5	Service Level Agreement	60 calendar days after Task Order Award
8.6	Software Lifecycle Management Process Documentation	60 calendar days after Task Order Award
8.7	Technical Evaluations and Studies	30-365 calendar days after task order award
All	Weekly Status/Progress Reports	Every Friday @ 4:00 PM
All	Monthly Status/Progress Reports	3rd Business Day of the Month
9.2	Project Status – NPPD OCIO	Monthly, on the 3rd Business Day of the Month
9.3	Quality Control Schedules	Monthly, on the 3rd Business Day of the Month
9.4	Meeting Minutes and Exception Reports	Within 5 working days after the subject meeting or event
10.1	Certification and Accreditation Documentation	30-365 calendar days after date of Task Order Award
10.2	Updates to Certification and Accreditation	30-365 calendar days after date of Task Order Award
11.4	Performance Report (Part of Monthly Report)	3rd Business Day of the Month
12.0	Final Transition Plan	20th calendar day after task order award
13.0	Final Project Management Plan	20th calendar day after task order award

7. GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION

A comprehensive inventory list including equipment name, date of purchase, model number, serial number, and quantity will be made available to the contractor upon award of the contract. The Government information identified below will be made available to the contractor upon award of the contract.

- System design documentation
- System architecture
- Certification & accreditation documentation (system security plan)
- Hardware & software inventory (**See Attachments**)
- System environment requirements
- Database schema
- Service level agreement
- Master Watch Control Log Historical Database

8. PLACE OF PERFORMANCE

The vast majority of work associated with this task order shall be performed at the contractor's site with some of the work being performed at various DHS facilities within the DC metropolitan area.

9. OTHER CONSIDERATIONS

The government estimates long-distance travel at a not-to-exceed amount of $10,000. Travel expenses occurred in the performance of this task order may be reimbursed as allowed by the Federal Travel Regulations (FTR) in effect at the time of travel when authorized as part of the scope of work, within task order ceiling, and when approved by the Government. Local travel will not be reimbursed within a 50-mile radius of worksite or travel costs from contractor worksite to DHS.

10. PERIOD OF PERFORMANCE

The period of performance for this task order is 365 calendar days after task order award.

ACCESSIBILITY - COMPLIANCE WITH SECTION 508

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

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

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

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

apply to fulfill functional performance criteria.

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

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

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

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

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

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

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

4010.2.

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

12.1 Contractor personnel shall be cleared at the SECRET level.

12.2 Contractor Employee Access (HSAR 3052.204-71)(JUN 2006)

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

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
(4) Any information that is designated "sensitive" or subject to other controls, safeguards or Protection in accordance with subsequently adopted homeland security information handling procedures.

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

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

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

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

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

Alternate I
(JUNE 2006)

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

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in the task order or approved by the COTR in writing as necessary for performance of the work under the task order. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the Statement of Work, other terms and conditions in the task order or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

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

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request

additional time or money under the task order for any delays resulting from unauthorized use or access.

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

(1) The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;
(2) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and
(3) The waiver must be in the best interest of the Government.
(4) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the task order. Any additions or deletions of non-U.S. citizens after task order award shall also be reported to the Task Order Contracting Officer.

12.3 HSAR 3052.204-70 Security Requirements for Unclassified Information Technology Resources (June 2006)

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

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

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.
(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.
(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer

systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include:
   (1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and
   (2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

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

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

12.4 HSAR 3004.470-2

(a) DHS's policies and procedures on contractor personnel security requirements are 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.

(b) The contractor must not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the contract.

12.5 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/IP/NICC data or the function of computer systems operated on behalf of DHS/IP/NICC, and to preserve evidence of computer crime.

12.6 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.

13. DHS ENTERPRISE ARCHITECTURE COMPLIANCE

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures as it relates to this Statement of Work (SOW). 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.

In compliance with OMB mandates, all network hardware shall be IPv6 compatible without modification, upgrade, or replacement.

The Contractor shall implement all systems according to the architectural standards and technical requirements of the DHS Enterprise Architecture, and in conformance with the DHS Enterprise Transition Strategy, the DHS Enterprise Architecture, and the DHS Geospatial Information Infrastructure design. All datasets developed under the program shall be made available across the Department and to its collaborating partners within the limitations of security classification and 6 CFR Part 27.400 (Chemical-terrorism Vulnerability Information (CVI)). All geospatial data shall be modeled within the current version of the DHS geospatial data model and shall include Federal Geographic Data Committee (FGDC) compliant metadata to ensure robust discovery and catalog services. All data and related artifacts generated by the program shall reside within the DHS geospatial information infrastructure within one or more of the DHS enterprise data center(s).

The contractor shall use standards-based software development practices and conform to current industrial standards and practices for Service-Oriented Architectures, and shall follow the guidance set forth by the DHS SOA Working Group.

14. DATA CENTER COMPLIANCE

The contractor shall also support the potential for the migration/hosting of all IT applications to/at the DHS Consolidated Data Center. Support shall include:

- Development and documentation of a transition plan, to include identification of risks and mitigation plans.
- Development of system take down, standup, operation, and maintenance standard operating procedures (SOPs) to sufficient detail to enable competent third-party support of the system(s) at the authorized DHS Data Center.
- Physical packaging of the system, and – if so directed by the government – ground transport of the system(s) to the DHS Data Center(s).
- Temporary on-site presence at the DHS data center(s) to provide sufficient system stand-up and operational verification support.

15. SYSTEM LIFE CYCLE (SLC) COMPLIANCE

All contracting work shall adhere to the NPPD CIO SLC. The contractor shall work with the NPPD CIO or designated representative(s) to determine documentation and SDLC Phase Review requirements throughout each IT system's lifecycle. SLC Phase Reviews and Control Gate Reviews shall be regularly scheduled and integrated into the contractor's and program manager's project plan(s).

16. STATEMENT OF WORK ATTACHMENTS

1. Hardware and Software Inventory (Software Binder List, Development Environment Inventory, and Production Prizm Inventory) - 15 pages

Software Inventory List

Sw - Number	Binder Name	Software Description
[redacted]		

(b)(4)

Sw - Number	Binder Name	Software Description
[redacted]		

(b)(4)

Sw - Number	Binder Name	Software Description

(b)(4)

Sw - Number	Binder Name	Software Description
[redacted]		

(b)(4)

Sw - Number	Binder Name	Software Description
[redacted]		

(b)(4)

Sw - Number	Binder Name	Software Description
[redacted]		

(b)(4)

Sw - Number	Binder Name	Software Description	
[redacted]			

(b)(4)

Sw - Number	Binder Name	Software Description
(b)(4)		

Sw - Number	Binder Name	Software Description
(b)(4)		

	A	B	C	D	E	F	G	I
1	PART NUMBER	SERIAL NUMBER	INVENTORY TAG	SERVICE TAG	DESCRIPTION	QTY	EQUIPMENT	TYPE

(b)(4)

(b)(4)

(b)(4)

(b)(4)

	A	B	C	D	E	F	G	I	M
1	PART NUMBER	SERIAL NUMBER	INVENTORY TAG	[redacted]	[redacted]				

(b)(4)

(b)(4)

REQUIRED CLAUSES

All terms and conditions outlined in your EAGLE contract are applicable to this solicitation and any resulting awards made as a result of this solicitation in addition to the following:

1. Clauses Incorporated by Reference (Feb 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be access electronically at this/these address(es):

http://www.arnet.gov/far

http://farsite.hill.af.mil

FAR 52.204-2	Security Requirements (Aug 1996)
FAR 52.204-9	Personal Identify Verification of Contractor Personnel

2. Special Clauses

a. Holidays and Administrative Leave

U. S. Department of Homeland Security personnel observe the following days as holidays:

New Year's Day
Martin Luther King's Birthday
Presidents' Day
Memorial Day
Independence Day
Labor Day
Columbus Day
Veteran's Day
Thanksgiving Day
Christmas Day

Any other day designated by Federal statute, by Executive Order or by the President's proclamation.

When any such day falls on a Saturday, the preceding Friday is observed. When any such day falls on a Sunday, the following Monday is observed. Observance of such days by Government personnel shall not be cause for an extension to the delivery schedule or period of performance or adjustment to the price, except as set forth in the contract.

Except for designated around-the-clock or emergency operations, contractor personnel will not be able to perform on-site under this contract on holidays set forth above. The contractor shall not charge any holiday as a direct charge to the contract. In the event contractor personnel work during a holiday other than those above, no form of holiday or other premium compensation will be reimbursed as either a direct or indirect cost. However, this does not preclude reimbursement for authorized overtime work.

In the event DHS grants administrative leave to its Government employees at the site, on-site contractor personnel shall also be dismissed if the site is being closed. However, the contractor shall continue to provide sufficient staff personnel to perform around-the-clock requirements of critical efforts already in progress or scheduled and shall be guided by the instructions issued by the Contracting Officer or his/her duly appointed representative. In each instance when the site is closed to contractor personnel as a result of inclement weather, potentially hazardous conditions, or other special circumstances; the contractor will direct its staff as necessary to take actions such as reporting to its own site(s) or taking appropriate leave consistent with its policies. The cost of salaries and wages to the contractor for the period of any such site closure are a reimbursable item of direct cost under the contract for employees whose regular time is normally a direct charge if they continue to perform contract work; otherwise, costs incurred because of site closure are reimbursable as indirect cost in accordance with the contractor's established accounting policy.
(End)

b. IDENTIFICATION OF CONTRACTOR PERSONNEL

The contractor shall ensure that its employees will identify themselves as employees of their respective company while working on DHS/OPO contracts. For example, contractor personnel shall introduce themselves in person and in voice-mail, and sign attendance logs as employees of their respective companies, and not as DHS employees. The contractor shall ensure that their personnel use the following format signature on all official e-mails generated by DHS computers:

Name
Position or Professional Title
Company name
Supporting the _____ division/office of DHS
Phone
Fax
Other contact information as desired
(End)

c. Non-Personal Services

(a) The Government and the Contractor understand and agree that the services delivered by the Contractor to the Government are non-personal services. The parties also recognize and agree that no employer-employee or master-servant relationship exists or will exist between the Government and the Contractor. The Contractor and the Contractor's employees are not employees of the Federal Government and are not eligible for entitlement and benefits given federal employees.

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

(End)

d. Advertisements, Publicizing Awards, and News Releases

(a) All press releases or announcements about agency programs, projects, and contract 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.

(b) 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.

e. Post Award Conference

The Contractor shall participate in a post award conference that will be held approximately fifteen (15) business days after contract award. The purpose of the post award conference is to aid both the Contractor and the Government in achieving a clear and mutual understanding of all contract requirements and identify and resolve potential problems (See FAR Subpart 42.5).

The COTR is responsible for establishing the time and place of the conference and will notify the appropriate Government representatives and the Contractors. The COTR will designate or act as the chairperson at the conference. The chairperson of the conference shall conduct the meeting.

The conference will be conducted at a location within the Washington DC commuting area at the Government's discretion. The post award conference will establish work level points of contact, determine the administration strategy, roles, and responsibilities and ensure prompt payment and close out.

Homeland Security Acquisition Regulations Clauses

3052.209-72 ORGANIZATIONAL CONFLICT OF INTEREST (JUN 2006)

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting ["**No conflicts have been identified**"].

(b) If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to avoid,

neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated, or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

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

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

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

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

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

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

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

3052.245-7 GOVERNMENT PROPERTY REPORTS (JUN 2006)

(a) The Contractor shall prepare an annual report of Government property in its possession and the possession of its subcontractors.

(b) The report shall be submitted to the Contracting Officer not later than September 15 of each calendar year on DHS Form 0700-5, Contractor Report of Government Property.