COMPONENT	
Office of Operations Coordination and Planning	
Program Office	**Employee**
Current Operations Division, Interagency Modeling & Atmospheric Assessment Center (IMAAC)	(b) (6)
Telephone	**Location**
(b) (6)	Nebraska Avenue Complex Washington, DC

Dear (b) (6)

You are hereby appointed as the Contracting Officer's Technical Representative (COTR) for DHS Office of Procurement Operations Agreement/Contract number: HSHQDC-10-F-00080 awarded to General Dynamics Advanced Information Systems effective 12/15/2010.

HSHQDC-10-F-00080 is a: (check one below)

☐ Contract ☐ Purchase Order ☒ Task/Delivery Order

☐ Cooperative Agreement ☐ Grant ☐ Memorandum of Understanding (MOU)

☐ Interagency/Intra-agency Agreement

Under this COTR appointment, you are assigned responsibilities to assist the contracting officer in the administration of the Agreement/Contract referenced above. This appointment remains in effect for the duration of the contractual agreement, as long as your COTR certification remains current. This appointment can only be changed or rescinded in writing by the contracting officer.

Please carefully review the explanation of COTR authority and responsibilities herein and sign the last page of this document acknowledging your understanding and acceptance of this COTR appointment. After signing the last page of the COTR appointment letter, please return it to the DHS OPO Contracting Officer within ten (10) calendar days.

SCOPE OF AUTHORITY

I, (b) (6) understand and agree that:

1. The DHS Office of Procurement Operations contracting officer is the only agent with authority to enter into and administer contractual agreements. I have been delegated the authority to monitor delivery and performance under the contractual agreement as the Contracting Officer's Technical Representative. Other than the contracting officer, or the alternate COTR acting in my absence, I am the duly appointed Government employee assigned to provide technical direction for the contractual agreement between the Government and the contractor.

2. This appointment does not change or supersede the established line of authority and/or responsibility of any organization.

3. I shall notify the contracting officer immediately if I am unable to fulfill the responsibilities of this position for an extended period.

4. I shall protect the Government's interests while performing my COTR duties. I must avoid any action that places me in a real or apparent conflict of interest that may compromise security or impair public confidence in the integrity of DHS.

5. I have read DHS Management Directive 0480.1, Ethics/Standards of Conduct and discussed any questions I have regarding my understanding of the duties and obligations under this policy.

COTR RESPONSIBILITIES

1. **PREPARATION**

(a) The COTR must be knowledgeable of the terms and conditions, as well as the technical content in the contractual agreement. To understand the terms, the COTR must read the contractual agreement and discuss any unclear areas with the contracting officer. The following is a list of topics in the contractual agreement that the COTR is expected to understand and manage:

Contractual Agreement Type
Reports & Deliverable Items
Invoicing and Payment Procedures
Packaging and Markings
Quality Assurance
Government Furnished Assets and Information

Performance Standards & Metrics
Time, Place and Method of Delivery or Performance
Security Requirements
Inspection, Acceptance, and Special Clauses
Ordering Procedures

(b) While the official contractual agreement file is maintained by the contracting officer, the COTR must create and maintain a file to document COTR actions under this contractual agreement. The file should include:

- A complete copy of the contractual agreement, a copy of the COTR Letter of Appointment;
- Copies of any related correspondence;
- A record of both oral and written communications with the contractor;

- Signed invoices;
- All records of the contractor's performance, such as performance monitoring, inspection and service reports and other documents as applicable.

(c) In order to effectively monitor delivery and performance, the COTR must read and become very familiar with the contractual agreement's schedule of performance standards and metrics, deliveries, completion dates, invoice due dates, option renewal dates and other report or data submission dates. The COTR must also establish a log or tracking system for progress and completion, with delivery dates. The log or tracking system will contain inspection, testing and acceptance dates, as well as all reports and notifications to the contracting officer, project manager, and the contractor.

2. GENERAL ADMINISTRATION INFORMATION

(a) Determine the need, and ensure all requirements are met for contractor badges, background checks, and all other required clearances.

(b) Plan and coordinate as necessary with the local facilities managers, real estate personnel or appropriate points of contact for the OPS component.

(c) Obtain and maintain a list of employees who will be working at the N/A facility. Keep list current by making adjustments for new and terminated employees. This is important to the security of the facility. This list may be used to initiate background checks by the security office in the relevant location.

(d) Coordinate with the contracting officer to ensure all contractors (and subcontractor as applicable) have signed nondisclosure forms, as prudent or required.

(e) Safeguard the contractor's confidential business and technical information. Confidential information may include proposal pricing, technical documentation, or personnel data. Do not release any information without first consulting with the contracting officer to determine if release of such information is permissible.

(f) Maintain communications with the contractor and the contracting officer. Meet with the contractor or his/her designated representative at the beginning of the contract/ agreement period of performance to discuss working methods. Also, serve as the contact through which the contractor can relay questions and problems to the contracting officer.

(g) Ensure all contractor personnel identify themselves and their company affiliation in all communications (written, telephonic, and electronic) related to the contract/ agreement.

(h) Monitor the contractor's compliance with safety, security, labor and environmental law requirements.

(i) Report any observed fraud, waste, or opportunities to improve performance or cost efficiency to the contracting officer.

(j) Provide independent government cost estimates (IGCEs) and other supporting information as required by the contracting officer when changes to the contract/ agreement are required.

(k) Assist the contracting officer in negotiating supplemental agreements and coordinating with related contractors on other business arrangements.

(l) Complete/Initiate Contractor Performance Assessment in CPARS within thirty (30) days of the end of the performance period, or at least annually, with detailed narrative to support rating parameters.

(m) Keep the contracting officer fully informed of any technical, administrative or contractual difficulties encountered during the contract performance period and make recommendations as appropriate.

(n) Seek guidance from the contracting officer for specific situations not covered in this delegation.

(o) Ensure the condition, availability and tracking of Government-Furnished Equipment or Government-Furnished Property.

3. MONITORING AND SURVEILLANCE

(a) Perform surveillance of the contractor's performance under the contractual agreement and conduct inspections necessary to assure performance and compliance with the terms and conditions of the contractual agreement. Resolve day-to-day matters within the scope of COTR authority.

(b) Assist the contractor in interpreting the terms and conditions or performance requirements, provided that any interpretation or clarification is within the limitations prescribed within the COTR delegation/appointment letter.

(c) Immediately bring to the contractor's attention, any potentially hazardous working conditions. The contractor is always required to comply with Federal Occupational Safety and Health Administration (OSHA) guidelines, applicable labor and environmental laws, as well as any state or local requirements for workplace safety, whether in a Federal facility or other location. In addition, ensure that the contractor adheres to any specific safety clauses and/or the safety plan in the contract/ agreement.

(d) Immediately alert the contracting officer to any possible contractor deficiencies or questionable practices so that corrections can be made before the problems become significant. Advise the contracting officer of the following situations:

- Possible changes in contractor management and/or key personnel;
- Potential labor disputes or workforce problems;
- Disagreements with the contractor regarding performance of statement of work/objectives (SOW/SOO) requirements or other potential disputes with the contractor about technical or other business matters;
- Lack of performance that may jeopardize the cost or required schedule of the contractual agreement.

(e) Review contractor requests for travel, overtime, Government assets, or subcontracting in a timely manner and forward to the contracting officer for approval.

(f) Review and analyze the contractor's deliverables, service, and management reports.

(g) Provide feedback on contractor performance as input to the past performance data base or as otherwise requested by the contracting officer.

4. INSPECTION AND ACCEPTANCE

(a) Inspect deliverables and monitor services for conformance to the performance standards, and accept or reject them.

(b) Follow the guidance within the contractual agreement regarding inspection and acceptance. If there are any questions, contact the contracting officer.

5. INVOICES AND PAYMENT

(a) See FAR clauses 52.232-1, 52.232-7 and 52.232-25 for processing of invoices and adhere to those conditions.

(b) Report any discrepancies in payment vouchers to the contracting officer. Provide documentation to support the representation.

(c) Evaluate progress payment requests based on costs incurred and actual work accomplished.

(d) Interim Cost Vouchers: If this is a cost reimbursable agreement, the contractor is entitled to be reimbursed periodically for all reasonable costs incurred in performing the contractual agreement. You should review such vouchers to make sure charges are commensurate with observed performance. It is your responsibility to question or concur with direct charges such as labor, materials, travel, etc. Alert the contracting officer if the billing includes material or equipment charges for items that have not been delivered to the work site, or have been delivered to the Government, but were not identified in the contract. The contracting officer is responsible for verifying correctness of indirect rates, fringe benefits and fee, if any.

6. GOVERNMENT FURNISHED ASSETS: EQUIPMENT, MATERIALS AND FACILITIES

(a) You are ***not*** authorized to provide any Government-owned (or leased) equipment or supplies or use of Government space to the contractor, other than those specifically identified in the contractual agreement and authorized by the contracting officer.

(b) During performance, it is your responsibility to monitor the contractor's use and care of any Government-furnished assets. If you believe the contractor is using the item for unauthorized purposes or is not providing adequate maintenance or security for the property, you are required to bring your concerns to the contractor's attention. If the contractor does not agree to remedy the problem, or indicates that corrective action will impact the cost, performance or schedule, refer the matter to the contracting officer.

(c) Coordinate with the OPS Asset Manager regarding the completion of all required documentation for the acceptance, use and return of Government-furnished assets.

(d) Assist the OPS Asset Manager with the disposal of excess Government furnished assets and/or contractor acquired assets.

(e) Assist the OPS Asset Manager with the valuation of lost, damaged and destroyed Government furnished assets and/or contractor acquired assets.

(f) Alert the OPS Asset Manager and the contracting officer to any potential or existing Government asset issues.

7. CONFLICT OF INTEREST AND STANDARDS OF CONDUCT

(a) The COTR is required to complete an Office of General Counsel (OGC) ethics training course annually. Upon completion of the annual ethics training, the COTR shall submit documentation (e.g., certificate or e-mail) to the contracting officer indicating the annual ethics training requirement has been met.

(b) In order to maintain DHS COTR Certification, one (1) hour of procurement ethics training is required annually per MD 0780.1.

(c) If applicable, the COTR appointee must submit a disclosure, such as a Statement of Financial Interest and Outside Employment or Financial Disclosure Report, to the appropriate DHS confidential reporting system.

(d) COTR appointees must adhere to standards of conduct as prescribed in Federal statutes, laws, regulations, and Departmental guidelines.

8. EXCLUSIONS FROM COTR RESPONSIBILITIES

The COTR is expressly excluded from performing or being responsible for the following:

(a) Making or giving the appearance of being able to make commitments, modifications, or any other action that would commit the Government to a change in price, performance quality, quantity, or the delivery schedule.

(b) Providing guidance to the contractor, either orally or in writing, which might be interpreted as a change in the scope or terms of the contractual agreement.

(c) Signing any changes or modifications to contracts/agreements and/or task or delivery orders(s).

(d) Specifying how the contractor will accomplish performance.

(e) Imposing or placing a demand upon the contractor to perform any task or permitting any substitution not specifically provided for in the contractual agreement.

(f) Increasing the dollar limit of the contractual agreement or authorizing expenditures not specified under the contractual agreement.

(g) Engaging in conduct prejudicial to the Government.

(h) Making a Government decision outside official channels.

(i) Discussing procurement plans or any other advance acquisition information that may, in fact, provide preferential treatment to one firm.

The responsibilities, and exclusions set forth in this document are not intended to be all-

encompassing. As a COTR, you are required to consult with the contracting officer when there are questions on your authority. You are not authorized to re-delegate your authority. Violation or misuse of your authority could result in abuse of DHS policy and resources at a minimum or monetary loss to the COTR or firm involved, disciplinary actions, and other measures, depending on the extent of the offense.

(b) (6) Contracting Officer
Intelligence and Operations Acquisitions Division
Office of Procurement Operations

Date

The undersigned acknowledges the COTR appointment on Agreement/Contract Number: HSHQDC-10-F-00080 and accepts the duties, responsibilities and limitations described in the appointment letter.

The contracting officer reserves the authority to cancel COTR appointments in accordance with HSAM, Chapter 3001.

COTR Acknowledgement:

I, (b) (6) have read the COTR appointment letter herein for Agreement/Contract Number HSHQDC-10-F-00080 and fully understand and accept my responsibilities and the limitations of my delegated authority. I further understand that my performance as a COTR will be evaluated and documented on an annual basis by the contracting officer. I certify that I have taken the required training to obtain the DHS Acquisition Certification for COTRs or have received a waiver, based upon my previous related training and experience. In addition, I certify that I will take the mandatory skills currency training to maintain my certification during the duration of this appointment.

(b) (6)

Signature

15 Dec 2010.
Date

Supervisor Acknowledgement:

I, Daniel Lipka, have read the COTR appointment letter herein and fully understand, support and approve my employee's responsibilities and limitations as a COTR under the above referenced contract.

(b) (6)

Chief of Assessments, OPS Coordination
Operations Coordination and Planning

Dec 15, 2010
Date

Return no later than December 22, 2010 to: (b) (6) or fax to (b) (6)

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEM

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER: ROOP-10-00003

PAGE 1 OF 14

2. CONTRACT NO: GS-10F-0237L

3. AWARD/ EFFECTIVE DATE:

4. ORDER NUMBER: HSHQDC-10-F-00080

5. SOLICITATION NUMBER: HSHQDC-10-Q-00005

6. SOLICITATION ISSUE DATE: 04/07/2010

7. FOR SOLICITATION INFORMATION CALL: a. NAME (b) (6) b. TELEPHONE NUMBER *(No collect calls)* (b) (6)

8. OFFER DUE DATE/LOCAL TIME

9. ISSUED BY CODE DHS/OPO/IOAD

U.S. Dept. of Homeland Security
Office of Procurement Operations
Intel and Operations Acq. Division
245 Murray Lane, SW
Building 410
Washington DC 20528

10. THIS ACQUISITION IS ☒ UNRESTRICTED OR ☐ SET ASIDE: % FOR:
☐ SMALL BUSINESS ☐ EMERGING SMALL BUSINESS
☐ HUBZONE SMALL BUSINESS ☐ Sole Source
☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS ☐ 8(A)
NAICS: 541990
SIZE STANDARD: $6.5

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED ☐ SEE SCHEDULE

12. DISCOUNT TERMS: Net 30

13a. ☐ THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION ☐ RFQ ☐ IFB ☐ RFP

15. DELIVER TO CODE DHS

Department of Homeland Security
245 Murray Lane
Bldg. 410
Washington DC 20528

16. ADMINISTERED BY CODE DHS/OPO/IOAD

U.S. Dept. of Homeland Security
Office of Procurement Operations
Intel and Operations Acq. Division
245 Murray Lane, SW
Building 410
Washington DC 20528

17a. CONTRACTOR/ OFFEROR CODE 1718377300000 FACILITY CODE

GENERAL DYNAMICS ADVANCED INFORMATION SYSTEMS
12450 FAIR LAKES CIRCLE SUITE 800
FAIRFAX VA 220333865

TELEPHONE NO

18a. PAYMENT WILL BE MADE BY CODE FLETC-INV

DEPARTMENT OF HOMELAND SECURITY
FEDERAL LAW ENFORCEMENT TRNG CTR
1131 CHAPEL CROSSING ROAD
BDLG. 66 - FINANCE
ATTN: (b) (6)
GLYNCO GA 31524

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	DUNS Number: 171837730+0000 The Contractor shall provide media monitoring and social media/networking support services to the DHS Office of Operations Coordination and Planning. This is a hybrid Firm-Fixed Price/Time & Materials task order against the Contractor's General Services Administration (GSA) Mission Oriented Business Integrated Services (MOBIS) contract listed in Block 2. The period of				

(Use Reverse and/or Attach Additional Sheets as Necessary)

25. ACCOUNTING AND APPROPRIATION DATA: 2010 AM2010 40 4029 0000 2511

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*: $1,164,803.52

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☐ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN ______ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED HEREIN

☒ 29. AWARD OF CONTRACT REF ______ OFFER DATED ______. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR (b) (6)

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)* (b) (6)

30b. NAME AND TITLE OF SIGNER *(Type or print)* (b) (6)

30c. DATE SIGNED 5/27/10

31b. NAME OF CONTRACTING OFFICER *(Type or print)* (b) (6)

31c. DATE SIGNED 5/27/10

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE LEAD CONTRACTS SPECIALIST

19 ITEM NO	20 SCHEDULE OF SUPPLIES/SERVICES	21 QUANTITY	22 UNIT	23 UNIT PRICE	24 AMOUNT
	performance is one (1) six (6) month base period and four (4) twelve month option periods. Option Periods 2, 3 and 4 will only be exercised if the GSA Schedule Contract is renewed. The labor rates will be the lower of the rates identified in this task order or the new GSA Schedule Contract hourly rates. DO/DPAS Rating: NONE Period of Performance: 07/01/2010 to 12/31/2014				
0001	Base Period: Media Monitoring Support Services (Fixed Price) IAW SOW Section 4.1 Period of Performance: 07/01/2010 to 12/31/2010	6	MO	83,432.96	500,597.76
0002	Base Period: Social Media/Networking Support Services (Fixed Price) IAW SOW Section 4.2 Period of Performance: 07/01/2010 to 12/31/2010	6	MO	83,432.96	500,597.76
0003	Base Period: OPTIONAL TASK: Surge Support (Labor Hour) IAW SOW Section 4.3 NOT TO EXCEED $33,696 1 LO = Up to $33,696 of the following labor Continued ...	1	LO	33,696.00	33,696.00

32a. QUANTITY IN COLUMN 21 HAS BEEN

□ RECEIVED □ INSPECTED □ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED:

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32c. DATE

32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER

□ PARTIAL □ FINAL

34. VOUCHER NUMBER

35. AMOUNT VERIFIED CORRECT FOR

36. PAYMENT

□ COMPLETE □ PARTIAL □ FINAL

37. CHECK NUMBER

38. S/R ACCOUNT NUMBER

39. S/R VOUCHER NUMBER

40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT

41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER

41c. DATE

42a. RECEIVED BY *(Print)*

42b. RECEIVED AT *(Location)*

42c. DATE REC'D *(YY/MM/DD)*

42d. TOTAL CONTAINERS

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED GS-10F-0237L/HSHQDC-10-F-00080	PAGE 3 OF 14

NAME OF OFFEROR OR CONTRACTOR
GENERAL DYNAMICS ADVANCED INFORMATION SYSTEMS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	categories: Technical Associate II @ (b) (4) per hour Project Manager @ (b) (4) per hour The ceiling price shall not exceed $33,696. Award Type: Labor-hour Period of Performance: 07/01/2010 to 12/31/2010				
0004	Base Period: Task Order Management - Project Management (Fixed Price) IAW SOW Section 4.4.1 Period of Performance: 07/01/2010 to 12/31/2010	6	MO	21,152.00	126,912.00
0005	Base Period: Travel (Cost Reimbursement) IAW SOW Section 10 NOT TO EXCEED $3,000 Award Type: Cost Total Estimated Cost: $3,000.00 Period of Performance: 07/01/2010 to 12/31/2010 A General and Administrative rate and Facilities Capital Cost of Money will be applied to Travel				3,000.00
1001	Option Period 1: Media Monitoring Support Services (Fixed Price) IAW SOW Section 4.1 Amount: $1,011,780.00(Option Line Item) Period of Performance: 01/01/2011 to 12/31/2011	12	MO	84,315.00	0.00
1002	Option Period 1: Social Media/Networking Support Services (Fixed Price) IAW SOW Section 4.2 Amount: $1,011,780.00(Option Line Item) Period of Performance: 01/01/2011 to 12/31/2011	12	MO	84,315.00	0.00
1003	Option Period 1: OPTIONAL TASK: Surge Support (Labor Hour) IAW SOW Section 4.3 NOT TO EXCEED $63,772.80 1 LO = Up to $63,772.80 of the following labor categories: Continued ...	1	LO	63,772.80	0.00

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED GS-10F-0237L/HSHQDC-10-F-00080	PAGE 4 OF 14

NAME OF OFFEROR OR CONTRACTOR
GENERAL DYNAMICS ADVANCED INFORMATION SYSTEMS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Technical Associate II @ (b) (4) per hour Project Manager @ (b) (4) per hour The ceiling price shall not exceed $63,772.80. Award Type: Labor-hour Amount: $63,772.80(Option Line Item) Period of Performance: 01/01/2011 to 12/31/2011				
1004	Option Period 1: Task Order Management - Project Management (Fixed Price) IAW SOW Section 4.4.1 Amount: $258,624.00(Option Line Item) Period of Performance: 01/01/2011 to 12/31/2011	12	MO	21,552.00	0.00
1005	Option Period 1: Travel (Cost Reimbursement) IAW SOW Section 10 NOT TO EXCEED $5,000 Award Type: Cost Total Estimated Cost: $5,000.00 Amount: $5,000.00(Option Line Item) Period of Performance: 01/01/2011 to 12/31/2011 A General and Administrative rate and Facilities Capital Cost of Money will be applied to Travel				0.00
2001	Option Period 2: Media Monitoring Support Services (Fixed Price) IAW SOW Section 4.1 Amount: $1,047,170.40(Option Line Item) Period of Performance: 01/01/2012 to 12/31/2012	12	MO	87,264.20	0.00
2002	Option Period 2: Social Media/Networking Support Services (Fixed Price) IAW SOW Section 4.2 Amount: $1,047,170.40(Option Line Item) Period of Performance: 01/01/2012 to 12/31/2012	12	MO	87,264.20	0.00
2003	Option Period 2: OPTIONAL TASK: Surge Support (Labor Hour) IAW SOW Section 4.3 NOT TO EXCEED $66,262.10 1 LO = Up to $66,262.10 of the following labor categories: Technical Associate II @ (b) (4) per hour Continued ...	1	LO	66,262.10	0.00

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED GS-10F-0237L/HSHQDC-10-F-00080	PAGE 5 OF 14

NAME OF OFFEROR OR CONTRACTOR
GENERAL DYNAMICS ADVANCED INFORMATION SYSTEMS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Project Manager @ (b) (4) per hour The ceiling price shall not exceed $66,262.10. Amount: $66,262.10(Option Line Item) Period of Performance: 01/01/2012 to 12/31/2012				
2004	Option Period 2: Task Order Management - Project Management (Fixed Price) IAW SOW Section 4.4.1 Amount: $267,667.20(Option Line Item) Period of Performance: 01/01/2012 to 12/31/2012	12	MO	22,305.60	0.00
2005	Option Period 2: Travel (Cost Reimbursement) IAW SOW Section 10 NOT TO EXCEED $5,000 Award Type: Cost Total Estimated Cost: $5,000.00 Amount: $5,000.00(Option Line Item) Period of Performance: 01/01/2012 to 12/31/2012 A General and Administrative rate and Facilities Capital Cost of Money will be applied to Travel				0.00
3001	Option Period 3: Media Monitoring Support Services (Fixed Price) IAW SOW Section 4.1 Amount: $1,083,874.80(Option Line Item) Period of Performance: 01/01/2013 to 12/31/2013	12	MO	90,322.90	0.00
3002	Option Period 3: Social Media/Networking Support Services (Fixed Price) IAW SOW Section 4.2 Amount: $1,083,874.80(Option Line Item) Period of Performance: 01/01/2013 to 12/31/2013	12	MO	90,322.90	0.00
3003	Option Period 3: OPTIONAL TASK: Surge Support (Labor Hour) IAW SOW Section 4.3 NOT TO EXCEED $68,583.50 1 LO = Up to $68,583.50 of the following labor categories: Technical Associate II @ (b) (4) per hour Project Manager @ (b) (4) per hour The ceiling price shall not exceed $68,583.50. Continued ...	1	LO	68,583.50	0.00

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED GS-10F-0237L/HSHQDC-10-F-00080	PAGE 6 OF 14

NAME OF OFFEROR OR CONTRACTOR
GENERAL DYNAMICS ADVANCED INFORMATION SYSTEMS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Award Type: Labor-hour Amount: $68,583.50(Option Line Item) Period of Performance: 01/01/2013 to 12/31/2013				
3004	Option Period 3: Task Order Management - Project Management (Fixed Price) IAW SOW Section 4.4.1 Amount: $277,036.80(Option Line Item) Period of Performance: 01/01/2013 to 12/31/2013	12	MO	23,086.40	0.00
3005	Option Period 3: Travel (Cost Reimbursement) IAW SOW Section 10 NOT TO EXCEED $5,000 Award Type: Cost Total Estimated Cost: $5,000.00 Amount: $5,000.00(Option Line Item) Period of Performance: 01/01/2013 to 12/31/2013 A General and Administrative rate and Facilities Capital Cost of Money will be applied to Travel				0.00
4001	Option Period 4: Media Monitoring Support Services (Fixed Price) IAW SOW Section 4.1 Amount: $1,121,805.60(Option Line Item) Period of Performance: 01/01/2014 to 12/31/2014	12	MO	93,483.80	0.00
4002	Option Period 4: Social Media/Networking Support Services (Fixed Price) IAW SOW Section 4.2 Amount: $1,121,805.60(Option Line Item) Period of Performance: 01/01/2014 to 12/31/2014	12	MO	93,483.80	0.00
4003	Option Period 4: OPTIONAL TASK: Surge Support (Labor Hour) IAW SOW Section 4.3 NOT TO EXCEED $70,780.80 1 LO = Up to $70,780.80 of the following labor categories: Technical Associate II @ (b) (4) per hour Project Manager @ (b) (4) per hour The ceiling price shall not exceed $70,780.80. Amount: $70,780.80(Option Line Item) Period of Performance: 01/01/2014 to 12/31/2014 Continued ...	1	LO	70,780.80	0.00

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED	PAGE	OF
	GS-10F-0237L/HSHQDC-10-F-00080	7	14

NAME OF OFFEROR OR CONTRACTOR
GENERAL DYNAMICS ADVANCED INFORMATION SYSTEMS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
4004	Option Period 4: Task Order Management - Project Management (Fixed Price) IAW SOW Section 4.4.1 Amount: $286,732.80(Option Line Item) Period of Performance: 01/01/2014 to 12/01/2014	12	MO	23,894.40	0.00
4005	Option Period 4: Travel (Cost Reimbursement) IAW SOW Section 10 NOT TO EXCEED $5,000 Award Type: Cost Total Estimated Cost: $5,000.00 Amount: $5,000.00(Option Line Item) Period of Performance: 01/01/2014 to 12/31/2014 A General and Administrative rate and Facilities Capital Cost of Money will be applied to Travel				0.00
4006	OPTIONAL TASK: Task Order Management: Transition Closeout Plan (Fixed Price) IAW SOW Section 4.4.4 Amount: $11,506.40(Option Line Item) Period of Performance: 10/01/2014 to 11/30/2014	1	LO	11,506.40	0.00
4007	OPTIONAL TASK: Task Order Management: Transition Closeout Activities (Fixed Price) IAW SOW Section 4.4.5 Amount: $234,203.12(Option Line Item) Period of Performance: 12/01/2014 to 12/31/2014 The total amount of award: $11,319,234.64. The obligation for this award is shown in box 26.	1	LO	234,203.12	0.00

SECTION 1: SERVICES AND PRICES

1.1 Task Order Type

This is a hybrid firm-fixed price and time and material task order against the Contractor's General Services Administration (GSA) Mission Oriented Business Integrated Services (MOBIS) contract **GS-10F-0237L.**

1.2 Supplies and Services

The Contractor shall provide media monitoring and social media/networking support services to the DHS Office of Operations Coordination and Planning.

1.3 Price Schedule

See pages one (1) through seven (7) of this Task Order.

SECTION 2: STATEMENT OF WORK (SOW)

SEE ATTACHMENT 1

SECTION 3: PACKAGING AND MARKING

See SOW Section 5 for packaging and marking instructions for deliverables.

SECTION 4: INSPECTION AND ACCEPTANCE

An inspection, acceptance and receiving report shall be signed by an authorized Government representative to evidence receipt, inspection and acceptance. The report shall be completed at the place(s) specified in the task order for Government receipt and acceptance. DHS Form 700-21, Material Inspection and Receiving Report, will be used for this purpose.

DHS inspection and acceptance of services, reports and other required deliverables or outputs shall take place at:

U. S. Department of Homeland Security
Office of Coordination and Planning
245 Murray Lane, SW
Building 410
Washington, DC 20528

Or at any other location designated by the Contracting Officer's Technical Representative (COTR) where the services are performed and reports and deliverables or outputs are produced or submitted. The COTR, listed in Section 6.1.3, has been delegated authority to inspect and accept all services, reports, and required deliverables or outputs.

SECTION 5: DELIVERABLES OR PERFORMANCE

5.1 Period of Performance

The period of performance of this task order is for one (1) six (6) month base period and four (4) twelve (12) month option periods.

5.2 Place of Performance

The place of performance will be at the Contractor's facility.

5.3 Deliverables

See the Deliverable Table in Section 5.2 of the SOW.

SECTION 6: CONTRACT ADMINISTRATION

6.1 Points of Contact for this task order

6.1.1 (b) (6) Contracting Officer
U.S. Department of Homeland Security
Office of Procurement Operations (MGMT/OPO) / Stop 0115
245 Murray Lane
Washington, DC 20528-0115
(b) (6)

6.1.2 (b) (6) Contract Specialist
U.S. Department of Homeland Security
Office of Procurement Operations (MGMT/OPO) / Stop 0115
245 Murray Lane
Washington, DC 20528-0115
(b) (6)

6.1.3 (b) (6) Contracting Officer's Technical Representative (COTR)
U.S. Department of Homeland Security
Office of Operations Coordination and Planning
(b) (6)

6.2 Invoice and Payment Provisions

6.2.1 The original invoice shall be submitted to the following Finance office:

ATTN: (b) (6) Finance Division, Building 66
Department of Homeland Security
Federal Law Enforcement Training Center (FLETC)
1131 Chapel Crossing Road
Bldg. 66 – FINANCE
Glynco, GA 31524
(b) (6)

Copies of the invoice shall be submitted to FLETC, the Contracting Officer, Contract Specialist and the COTR concurrently. The invoice must contain the 1) contract number; 2) order number; and 3) applicable contract line item number(s) (CLIN).

To constitute a proper invoice, the invoices must include those items cited in FAR 52.232-1 Payments (APR 1984), FAR 52.232-7 Payments under Time-and Materials and Labor-Hour Contracts (FEB 2007) and FAR 52.232-25 Prompt Payment (OCT 2008), paragraphs (a)(3)(i) through (a)(3)(x).

6.2.2 Payment shall be made to the contractor upon delivery to and acceptance by the Government office requesting services in the following manner:

6.2.2.1 For CLINs 4006 and 4007, the contractor is authorized to bill, upon completion of the services, the associated unit price for the CLINs delineated in the Price schedule.

6.2.2.2 For CLINs 0001, 0002, 0004, 1001, 1002, 1004, 2001, 2002, 2004, 3001, 3002, 3004, 4001, 4002 and 4004, the contractor is authorized to bill, on monthly basis, the associated unit price for the CLINs delineated in the Price schedule.

6.2.2.3 For CLINs 0003, 1003, 2003, 3003 and 4003, the contractor is authorized to bill, on a monthly basis, for the direct labor hours performed at the rates delineated in the Price schedule.

6.2.2.4 For CLINs 0005, 1005, 2005, 3005 and 4005, the contractor is authorized to bill, on a monthly basis, for the travel costs associated with completed travel.

SECTION 7: SPECIAL CONTRACT REQUIREMENTS

7.1 Travel

Costs for transportation, lodging, meals and incidental expenses incurred by contractor personnel on official company business are allowable subject to FAR 31.205-46, Travel Costs. These costs will be considered to be reasonable and allowable only to the extent that they do not exceed on a daily basis the maximum per diem rates in effect at the time of travel as set forth in the Federal Travel Regulations. The contractor will not be reimbursed for travel expenses within a 50-mile radius of the worksite. Local travel expenses within the Washington Metropolitan area will not be reimbursed (this includes parking). All travel outside the Washington Metropolitan area must be approved by the COTR in advance. No travel will be reimbursed without prior approval from the COTR. Unless approved in advance by the CO, the contractor's travel shall not exceed the maximum per diem rates established by the General Services Administration.

7.2 Post Award Evaluation of Contractor Performance

7.2.1 Contractor Performance Evaluations

In accordance with FAR Subpart 42.1502, Policy, agencies are required to prepare an evaluation of contractor performance for each (non-construction/A&E) contract in excess of $100,000. An assessment must be prepared at least annually and at the conclusion of the contract. In addition, contracts with a period of performance exceeding one year (including option periods) require interim evaluations so as to document contractor performance and provide current information for source selection purposes.

7.2.2 Contractor Performance Assessment Reporting System (CPARS)

The U.S. Department of Homeland Security utilizes the Department of Defense's Contractor Performance Assessment Reporting System (CPARS), a web-enabled application that collects and manages the library of automated contractor performance assessments, to collect and maintain contractor performance assessments. An assessment evaluated evaluates a contractor's performance, both positive and negative, and provides a record on a given contractor during a specific period of time, under a specific contract or task order. CPARS is for UNCLASSIFIED use only.

7.2.3 Contractor Performance Information

The DHS Office of Procurement Operations' (OPO) assessments of contractor performance shall be accessed by the contractor electronically after completion of the assessment by logging onto CPARS at https://www.cpars.csd.disa.mil. Contractors shall be given a minimum of thirty days to submit comments, rebut statements, and/or provide additional information to the Government.

The OPO Assessing Official shall review the Assessing Official Representative's assessment and consider the potential for disagreements between the Government and the contractor. If the contractor's response to the report is contentious, the Assessing Official will forward the evaluation to the Reviewing Official, who will serve as the mediator and shall resolve any dispute between the contractor and Government. If the Reviewing Official cannot resolve the dispute, the matter shall be referred to the Deputy Director, Office of Procurement Operations, for decision and resolution.

Copies of the evaluation, contractor response, and review comments, if any, shall be retained as part of the evaluation. The evaluation may be used to support future award decisions. The release of the completed contractor evaluation shall be restricted to Government personnel and the contractor whose performance is being evaluated. Once the evaluation is completed, it is copied into the Past Performance Information Retrieval System (PPIRS), a web-enabled, government-wide application that provides timely and pertinent contractor past performance information to the Federal acquisition community for use in making source selection decisions, where it can be viewed by authorized personnel at any agency for source selection purposes.

SECTION 8: TASK ORDER CLAUSES

8.1 The Contractor's GSA MOBIS contract clauses are incorporated into this task order.

8.2 Federal Acquisition Regulation (FAR) and Homeland Security Acquisition Regulation (HSAR) Clauses

NOTICE LISTING CONTRACT CLAUSES INCORPORATED BY REFERENCE

The following contract clauses pertinent to this section are hereby incorporated by reference (by Citation Number, Title, and Date) in accordance with the clause at FAR "52.252-2 CLAUSES INCORPORATED BY REFERENCE" in Section I of this contract. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at these addresses: http://www.arnet.gov/far, http://farsite.hill.af.mil/VFHSARA.HTM.

CITATION NUMBER	TITLE	DATE
FAR 52.215-16	FACILITIES CAPITAL COST OF MONEY	JUN 2003
FAR 52.237-3	CONTINUITY OF SERVICES	JAN 1991
FAR 52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION	JAN 2009
HSAR 3052.222-70	STRIKES OR PICKETING AFFECTING TIMELY COMPLETION OF THE CONTRACT WORK	DEC 2003
HSAR3052.242-71	DISSEMINATION OF CONTRACT INFORMATION	DEC 2003
HSAR 3052.242-72	CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE	DEC 2003

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

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days of the end of the current period of performance.

If the Government exercises clause 52.217-8 to extend performance, the 52.217-8 option pricing will be the Task Order rates in effect at the time when the option is exercised.

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

(a) The Government may extend the term of this contract by written notice to the Contractor within 29 days of the end of the current period of performance; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 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 54 months.

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

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

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

The Key Personnel or Facilities under this Contract:

Project Manager –(b) (6)

SECTION 9: LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS

Attachment 1	Statement of Work (SOW) (11 pages)

STATEMENT OF WORK

1. PROJECT TITLE

Media Monitoring and Social Media/Networking Support Services for the Office of Operations Coordination and Planning's National Operations Center

2. BACKGROUND

The Department of Homeland Security's (DHS) Office of Operations Coordination and Planning (OPS) is responsible for monitoring the security of the United States on a daily basis and coordinating activities within the Department and with all homeland security partners which include Federal agencies, the Governors, state Homeland Security Advisors, law enforcement partners, private sector, critical infrastructure operators in all 50 States, territories, and possessions and international stakeholders.

The mission of the OPS is to integrate DHS and interagency planning and operations coordination in order to prevent, protect, respond to and recover from terrorist threats/attacks and other man-made or natural disasters. OPS maintains situational awareness by gathering, coordinating and sharing information among Federal, State, Local, Tribal, Private Sector and International Homeland Security partners.

Through the National Operations Center (NOC), the OPS provides real-time situational awareness and monitoring of the homeland, coordinates incidents and response activities, and, in conjunction with the Office of Intelligence and Analysis, issues advisories and bulletins concerning threats to homeland security, as well as specific protective measures. The NOC, which operates 24 hours a day, seven days a week, 365 days a year (24/7/365), coordinates information sharing to help deter, detect, and prevent terrorist acts and to manage domestic incidents.

3. OBJECTIVE

The objective of this effort is to provide media monitoring support and social media/networking support services to the NOC Operations on a 24/7/365 basis to enhance DHS OPS situational awareness, fusion and analysis and decision support to senior leaders.

4. TASKS

4.1 Media Monitoring

Media monitoring assists DHS frame the operational picture that open source media is reporting, uncover problem areas for incident management leadership to further evaluate, identify nascent or evolving situations and provide valuable information and imagery that can be used to corroborate and/or reconcile first reports. The Contractor shall monitor, collect, analyze, and distribute operationally relevant real-time open source information to homeland security issues 24/7/365.

The Contractor shall understand DHS Critical Information Requirements (CIR) and monitor open source news coverage for new incidents that relate to the CIRs (Items of Interest – IOI) and understand how a story may be related to other important ongoing events and DHS activities. The CIRs are as follows:

a. Potential threats and hazards to the homeland, DHS, other Federal agencies, state and local response units (i.e., first responders), facilities (e.g., dams, major bridges and buildings), and resources (e.g., water supply, H1N1 vaccine); Private sector; and Public safety (e.g., where the public is involved, football game);
b. Potential impact on DHS capability to accomplish the HSPD-5 mission;
c. Identify events with operational value (e.g., successful space shuttle landing) and/or corroborating critical information (i.e., subsequent reporting to the initial report);
d. Identifying media reports that reflect adversely on the U. S. Government, DHS (e.g., a coast guard ship collides with another or impacting DHS from accomplishing its mission) and the National planning scenarios.

4.1.1 The Contractor shall perform a broad open sources search for information on breaking news stories. The contractor shall:

4.1.1.1 Monitor major broadcast news networks
4.1.1.2 Monitor and review all Associated Press (AP) stories generated within the U.S. by each state's AP bureau
4.1.1.3 Monitor and receive alerts on other wire service stories via categorized/focused Really Simple Syndication (RSS) feeds.
4.1.1.4 Monitor and receive alerts on local and regional broadcast news via categorized/focused text/video feeds
4.1.1.5 Monitor appropriate Internet web sites on breaking situational events
4.1.1.6 Monitor and receive full motion video (FMV) or other streaming media

4.1.2 An Item of Interest (IOI) is determined by those events or activities that require DHS NOC steady state or update reporting, an event requiring the DHS NOC to prepare Phased reporting or the formation of a Crisis Action Team as directed by DHS leadership through the DHS NOC. In the event an incident has occurred and an (IOI) follow-on analysis is underway or research is ongoing on a National Security Situation/

International Security Situation (NSS/ISS), the contractor shall perform the following as determined by the DHS leadership:

4.1.2.1 Continue to monitor major broadcast news networks (cable service)

4.1.2.2 Query and search Associated Press (AP) stories for information specific to the incident

4.1.2.3 Query and search broadcast news via categorized/focused text/video feeds for information specific to the incident

4.1.2.4 Query and search RSS feeds for information specific to the incident

4.1.2.5 Query and search the Internet using other search engines such as Google and Yahoo

4.1.2.6 Monitor and receive full motion video (FMV) or other streaming media specific to the incident

4.1.2.7 Monitor and search web sites including those representing regional and local media outlets (TV stations, radio stations, and newspapers source)

4.1.2.8 Continue to monitor/review reports available via above open sources for information on other breaking news stories

4.1.3 The Contractor shall create NOC media monitoring reports, media summaries, daily media operational summaries and weekly data reports.

4.2 Social Media/Networking

The Contractor shall provide 24x7x365 Social Media/Networking (S/N) support to enhance DHS OPS situational awareness, fusion and analysis, and decision support to senior leaders. The Contractor shall:

4.2.1 Monitor, collect, analyze, and distribute operationally relevant S/N as part of the DHS National Operations Center (NOC).

4.2.2 Facilitate S/N support to provide:

4.2.2.1 Potential and emerging threats and hazards information for homeland security situational awareness, information sharing and decision support.

4.2.2.2 Evolving incidents, crisis management and other Homeland Security information available to the public to include public alerts and notifications both sent and received

4.2.2.3 Additional venues for the public to communicate critical information to the Department of Homeland Security that serve to corroborate or reconcile other reports or provide new information that has not come to the Department's attention

4.3 OPTIONAL TASK: Surge Support

The Contractor shall provide additional Media Monitoring and Social Media/Networking support when operational conditions require staffing to support OPS during emergency operations and national level exercises. Surge support temporarily increases the staffing level of Tasks 4.1 and 4.2.

The Task Order (TO) Contracting Officer's Technical Representative (COTR) will approve the time, place of performance and level of effort for surge support prior to execution.

4.4 Task Order Management

4.4.1 Project Management

The Contractor shall designate a single point of contact as the Project Manager (PM) with whom the TO COTR will communicate operational, technical and administrative issues relating to this task order. The PM shall ensure that: (1) the goals and objectives of the project and (2) problem resolution and customer satisfaction are accomplished within prescribed time frames and funding parameters. Key duties include planning, organizing, directing and controlling the project to ensure all contractual obligations are fulfilled, quality standards are met and associated expectations of performance achieved. Other duties include developing schedules, reviewing work discrepancies, communicating policies and managing and controlling resources. THIS IS A FULL-TIME POSITION.

4.4.1.1 Monthly Task Order Status Report

The Contractor shall create monthly status reports. The status reports shall contain a heading with the following information at a minimum:

4.4.1.1.1 Contractor Name, Project Manager's Name and Telephone Number
4.4.1.1.2 Task Order Number and Task Order Period of Performance
4.4.1.1.3 Scope of Task Order
4.4.1.1.4 Period of Performance Being Reported
4.4.1.1.5 Submission Date

The Contractor shall assist DHS in compiling useful data on work performed under this task order. Each status report will contain the following items.

4.4.1.1.6 A brief, factual summary description of technical progress;

4.4.1.1.7 For each task, provide: a summary of work completed, work in progress and work planned; and for labor hour tasks include hours/dollars expended for the reporting period and cumulatively and hours/dollars remaining;

4.4.1.1.8 Updated Project Management Plan;

4.4.1.1.9 Identify significant problems and their impacts, causes, proposed corrective actions; and the effect that such corrective actions will have on the accomplishments of the task order objectives;

4.4.1.1.10 The Schedule status or the degree of completion of tasks/activities by time intervals;

4.4.1.1.11 Upcoming events; and

4.4.1.1.12 Status of Travel, if any;

4.4.2 Post Award Orientation Meeting

A Post Award Orientation meeting will be scheduled within ten (10) business days after task order award. The orientation aids both the Government and Contractor personnel to (1) achieve a clear and mutual understanding of all task order requirements and (2) identify and resolve potential problems. Attendees will be at a minimum: TO CO, TO CS, TO COTR and the Contractor's Program Manager.

The Post Award Orientation will take place at 301 7th Street, SW, Washington, D.C. The TO CO will establish the time of the orientation, prepare the meeting agenda and notify the appropriate Government and Contractor representatives of the meeting.

4.4.3 Task Order Kick-Off Meeting

The Task Order Kick-Off meeting will take place after the Post Award Orientation meeting. The purpose of this meeting is to introduce team members and present their roles and responsibilities, present an overview of the requirement based on the contents of the SOW and discuss any administrative matters.

The TO COTR will establish the time and place of the meeting and notify the appropriate Government and Contractor representatives. The meeting agenda will be prepared by the Government.

4.4.4 Transition Planning

An incumbent Contractor is currently performing the services outlined in the Statement of Work. The Contractor shall develop transition plans for startup and closeout activities.

4.4.4.1 Final Transition Startup Plan

The final Transition Startup Plan shall be a refined and finalized version of the Draft Transition Startup Plan submitted with the Technical Quote submission.

4.4.4.2 Transition Startup Activities

In the event that the tasks described in the SOW are transferred to a new contractor or to the Government, the new contractor and/or the Government shall participate in meetings with the incumbent contractor for an orderly and efficient transition. DHS anticipates a 30 to 60 calendar day transitional period during which the incumbent and new Contractor will be under contract.

4.4.4.2.1 The Contractor shall initiate and accept the transfer of relevant information and data from the incumbent Contractor.

4.4.4.2.2 The Contractor shall begin such coordination activities on the effective date of the task order.

4.4.4.2.3 Within 30 calendar days after favorable Entry on Duty (EOD) is granted, the Contractor shall be fully operational on all tasks.

4.4.5 OPTIONAL TASK: Transition Closeout Plan

The Contractor shall develop and submit a Draft Transition Closeout Plan sixty (60) calendar days prior to the conclusion of the task order for transferring responsibility of the tasks described in the SOW to a new Contractor or the Government. The plan shall inventory the tasks required to perform each task and identify a transition team lead. A Final Transition Closeout Plan shall be prepared and submitted fifteen (15) calendar days after receipt of Government's comments on the Draft Transition Closeout Plan.

4.4.6 OPTIONAL TASK: Transition Closeout Activities

In the event that the tasks described in the SOW are transferred to a new Contractor or to the Government, the Contractor shall participate in meetings with the new Contractor and/or the Government for an orderly and efficient transition. DHS anticipates a thirty (30) calendar day transitional period during which the Contractor and the new Contractor will be under contract. The Contractor shall prepare a Final Transition Out Plan Briefing that shows the final status of all deliverables and tasks.

5. DELIVERABLES AND DELIVERY SCHEDULE

All deliverables shall be prepared using Microsoft Office Suite module tools and delivered electronically to the NOC Senior Watch Officer Inbox. All deliverables are due by 5 PM local time (Washington, D.C.) unless otherwise stated in the Deliverable Table.

Note: The Contractor shall send a copy of the monthly status report (Task 4.4.1.1) to the TO CO, TO CS and TO COTR. Deliverables shall be free of any known computer virus or defects. If the Government finds a virus or defect is found, the deliverable will not be accepted. The replacement file shall be provided within two (2) business days after notification of the presence of a virus.

In the event the Contractor anticipates difficulty in complying with any deliverable, the Contractor shall provide written notification immediately to the TO CO, TO CS and TO COTR. Each notification shall give pertinent details, including the date by which the Contractor expects to make delivery; provided that this data shall be informational only in character and that receipt thereof shall not be construed as a waiver by the Government of any task order delivery schedule, or any rights or remedies provided by law under the GSA contract.

5.1 Review of Deliverables

The Government will provide written acceptance, comments and/or change requests, if any, within five (5) business days from receipt by the Government of the deliverable. Upon receipt of the Government comments, the Contractor shall have two (2) business days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form. Deliverables will be assessed on: amount of revision required by the Government, timeliness, adherence to specified formatting and content requirements and accuracy (errors on part of vendor, revealed after acceptance).

5.2 Deliverable Table

DELIVERABLE TABLE		
Task Number	**Deliverable Title**	**Due Date**
4.1	NOC Media Monitoring Report	Daily, as events occur (historical average is 15)
4.1	NOC Media Monitoring Operational Summary (roll up of NOC Media Monitoring Reports from the previous 24 hours)	Daily, NLT 0600

DELIVERABLE TABLE		
Task Number	**Deliverable Title**	**Due Date**
4.1	Weekly Data Reports – A statistical report based upon the previous weeks reporting of Incidents of Interest. Other weekly summaries maybe required based upon other criteria as required by the NOC leadership	Monday for the prior week, or as required.
4.2	Social Network Summaries– A summary of an Item on Interest	Daily, as events occur
4.2	Daily Social Network Operational Summaries – Operational Summary (roll up of NOC Media Monitoring Reports from the previous 24 hours)	Daily, NLT 0600
4.2	Weekly Data Reports – A statistical report based upon the previous weeks reporting of Incidents of Interest. Other weekly summaries maybe required based upon other criteria as required by the NOC leadership	Monday for the prior week
4.4.1	Monthly Status Report	1st report - 5th business day after the end of the first 30 calendar days Subsequent reports – 5th business day after the end of the previous 30 calendar day period
4.4.4.1	Draft Transition Startup Plan	Submitted with the Technical Quote
4.4.4.1	Final Transition Startup Plan	15 calendar days after task order award
4.4.5	OPTIONAL TASK: Draft Transition Closeout Plan	Sixty (60) calendar days prior to the expiration of the Task Order

DELIVERABLE TABLE		
Task Number	**Deliverable Title**	**Due Date**
4.4.5	OPTIONAL TASK: Final Transition Closeout Plan	Fifteen (15) calendar days after receipt of Government's comments on the Draft Transition Closeout Plan
4.4.6	OPTIONAL TASK: Final Transition Out Plan Briefing	As directed by TO COTR

6. KEY PERSONNEL

The position that follows has been designated as Key Personnel.

6.1 Project Manager - THIS IS A FULL-TIME POSITION

The Project Manager shall perform the duties associated with task 4.4.1. The minimum qualifications are:

6.1.1 Five (5) to seven (7) years of specific experience in managing large, complex projects in a task order/contract environment; experience performing the day-to-day management of overall contract/task order support operations involving multiple projects and groups of personnel; experience organizing, directing and coordinating the planning and production of contract/task order support activities; excellent written and oral communication skills; experience managing the client interface at the senior levels of the client organization. Has the ability to establish and alter, as necessary, technical approach to directly effect contract support activities.

6.1.2 A Master's degree from an accredited institution of higher learning.

6.1.3 Two (2) or more years of specific experience in the Media and/or Social Networking field in a supervisory capacity.

6.2 Substitution of Key Personnel

The Contractor shall notify the TO CO and TO COTR prior to making any changes in Key Personnel. All proposed substitutes shall have qualifications equal to or better than the qualifications of the person to be replaced. The TO CO and TO COTR must be notified in writing of any proposed substitutions at least thirty (30) days in advance of the proposed substitution. The notification shall include:

6.2.1 An explanation of the circumstances necessitating the substitution; and
6.2.2 A resume of the proposed substitute.

The TO CO and the TO COTR will evaluate substitutions and notify the Contractor of their approval or disapproval in writing.

6.3 Removal of Contractor Employees

The Contracting Officer may require dismissal from work of those contractor employees which he/she deems incompetent, careless, insubordinate, unsuitable or otherwise objectionable, or whose continued employment he/she deems contrary to the public interest or inconsistent with the best interest of national security. The contractor must fill out, and cause each of its employees on the contract work to fill out, for submission to the Government, such forms as may be necessary for security or other reasons.

7. GOVERNMENT-FURNISHED EQUIPMENT (GFE) AND GOVERNMETN FURNISHED INFORMATION (GFI)

There will be no GFE or GFI provided under this task order.

8. PLACE OF PERFORMANCE

The place of performance will be at the contractor's facility.

9. PERIOD OF PERFORMANCE

The period of performance shall be for a base period of six (6) months with four (4) twelve (12) month option periods.

10. TRAVEL

Travel performed for personal convenience or daily travel to and from work at the Contractor's facility or local Government facility (i.e. designated work site) shall not be reimbursed. Travel will be reimbursed in accordance with the Federal Travel Regulations. Travel will not be reimbursed within a 50 mile radius of the designated worksite. The Contractor must get TO COTR approval prior to travel. All travel must comply with the Federal Travel Regulations. Unless approved in advanced by the TO CO, the Contractor's travel shall not exceed the maximum per diem rates established by the General Services Administration.

The Contractor shall coordinate specific travel arrangements with the TO COTR to obtain advance, written approval for the travel about to be conducted. The Contractor's request for travel shall be in writing and contain the dates, locations and estimated costs of the travel. If any travel arrangements cause additional costs to the task order that exceed those previously negotiated, written approval by Task Order modification issued by the TO CO is required prior to undertaking such travel.

The Contractor shall to the maximum practical extent, minimize overall travel costs by taking advantage of discounted airfare rates available through advance purchase and or existing Department transportation. Charges associated with itinerary changes and cancellations of nonrefundable airline tickets are reimbursable as long as the changes are approved by the TO CO.

11. TASK ORDER (TO) CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (COTR)

The TO COTR represents the TO CO by administration of technical details within the scope of the task order. The TO COTR performs functions under the task order such as review or inspection and acceptance of supplies, services and other functions of a technical nature. The TO COTR and Contractor may not make any representations or commitments on behalf of the TO CO or the Government. The Contractor may not construe TO COTR inquiries as direction to work outside of the scope of the statement of work. The TO COTR does not have authority to alter the Contractor's obligations or to change the task order specifications, price, terms or conditions. If, as a result of technical discussions, it is desirable to modify task order obligations or the specifications, changes will be issued in writing and signed by the TO CO. The Contractor may propose changes to existing task order by sending such request to the TO CO.

12. SECURITY REQUIREMENTS

This task order does not require a security clearance.

Determination and Findings

Per 5 U.S.C. 3109 as implemented by FAR 37.104, FAR 7.503, and the Department of Homeland Security (DHS) Management Action Directive: Workforce Assessment issued May 26, 2009, the DHS Office of Procurement Operations shall ensure that any awards for contracts or the exercise of options under existing contracts for professional services do not include inherently governmental or nearly inherently governmental requirements, personal service requirements, or requirements that impact core functions that must be performed by federal employees. The purpose of this Determination and Findings (D&F) is to grant authority to the DHS Office of Procurement Operations to award a new task order for media monitoring and social media/networking support services.

Findings

1. Agency: DHS
   Contracting Activity: Office of Procurement Operations
   Program Office: Office of Operations Coordination and Planning
   Proposed Contractor: To Be Determined

2. Description of Proposed Services: Issue one new task order against a General Services Administration Schedule 874, Mission Oriented Business Integrated Services, contract
   Estimated Annual Value: $1,683,903.20
   Estimated Total Contract Value: $9,058,870.40

3. The proposed professional services with To Be Determined are not inherently governmental or nearly inherently governmental professional services as described in FAR 7.503.

4. The proposed professional services with To Be Determined are not for personal services as described in FAR 37.104. In accordance with FAR 37.104(c) (2), the Operations Coordination Division will not exercise relatively continuous supervision and control over the contractor personnel performing the contracts.

5. The proposed professional services with To Be Determined are not for the services of individual experts or consultants as provided in FAR 37.104(f).

6. The proposed professional services with To Be Determined will not impact the Operations Coordination Division's core functions that must be performed by federal employees in accordance with DHS Management Action Directive: Workforce Assessment issued May 26, 2009.

7. Within the Office of Operations Coordination and Planning, the Operations Coordination Division's ratio of all Federal employees to all contractor employees, including those under this action, is fifty-five (55) federal employees to thirty-five (35) contractors.

8. Program Office Contracting Officer Technical Representative (COTR) Information:
   Proposed COTR Official: (b) (6)
   COTR Certification and Training: (b) (6) is certified as of October 23, 2006 and is current with the required training.
   COTR responsibilities: This is an ancillary duty for the COTR whose primary responsibility is as an Operations Manager. In addition to the proposed task order, the COTR currently manages one contract. Although the COTR's responsibilities are ancillary, the COTR has suffient time and resources to adequately manage and oversee the proposed task order.

Determination

Based on the above findings, under the authority of FAR 7.503(e), and in accordance with the Department of Homeland Security Acquisition Manual Subchapter 3007.5, Inherently Governmental Functions, I have determined that the acquisition of the proposed professional services do not include inherently governmental or nearly inherently governmental requirements, personal service requirements, or requirements that impact core functions that must be performed by federal employees. Further, the number of Federal employees within the Office of Operations Coordination and Planning, Operations Coordination Division is sufficient to provide adequate direction and oversight to the professional service contractor employees.

(b) (6)

10/27/09

Donald Triner, Director
Current Operations
Office of Operations Coordination & Planning

Date

(b) (6) Contracting Officer
Intelligence and Operations Acquisitions Division

Date

APPROVAL:
(for actions with an annual value greater than $1 million but not exceeding $50 million)

(b) (6)
Director Office of Procurement Operations

Date

Determination and Findings

Per 5 U.S.C. 3109 as implemented by FAR 37.104, FAR 7.503, and the Department of Homeland Security (DHS) Management Action Directive: Workforce Assessment issued May 26, 2009, the DHS Office of Procurement Operations shall ensure that any awards for contracts or the exercise of options under existing contracts for professional services do not include inherently governmental or nearly inherently governmental requirements, personal service requirements, or requirements that impact core functions that must be performed by federal employees. The purpose of this Determination and Findings (D&F) is to grant authority to the DHS Office of Procurement Operations to exercise a task order option with General Dynamics Advanced Information Systems for media monitoring and social media/networking support services to support the mission of the DHS, Operations Coordination Division.

Findings

1. Agency: DHS
   Contracting Activity: Office of Procurement Operations
   Program Office: Office of Operations Coordination and Planning (OPS)
   Proposed Contractor: General Dynamics Advanced Information Systems, 12450 Fair Lakes Circle, Suite 800, Fairfax, VA 22033-3865

2. Description of Proposed Services: Media monitoring support and social media/networking support services to the National Operations Center (NOC) on a 24/7/365 basis to enhance DHS OPS situational awareness, fusion and analysis and decision support to senior leaders.
   Contract No: GS-10F-0237L/HSHQDC-10-F-00080
   Exercise Option Period One (1) of the task order
   Estimated Annual Value: $2,515,385.48
   Estimated Total Contract Value: $11,319,234.64
   Advance Acquisition Plan (AAP) No: 68786

3. The proposed professional services are not inherently governmental or nearly inherently governmental professional services as described in FAR 7.503.

4. The proposed professional services are not for personal services as described in FAR 37.104. In accordance with FAR 37.104(c) (2), the Operations Coordination Division will not exercise relatively continuous supervision and control over the contractor personnel performing the contracts.

5. The proposed professional services are not for the services of individual experts or consultants as provided in FAR 37.104(f) (see limitations of the Classification Act).

6. The proposed professional services will not impact the Operations Coordination Division's core functions that must be performed by federal employees in accordance with DHS Management Action Directive: Workforce Assessment issued May 26. 2009.

7. Within the Office of Operations Coordination and Planning the Operations Coordination Division's ratio of all Federal employees to all contractor employees, including those under this action, is three (3) federal employees to one (1) contractor.

8. Within the Office of Operations Coordination and Planning the Operations Coordination Division, the estimated number of Federal employee(s) providing oversight to the service contractor is one (1) who is assigned to oversee the contractor on a part-time basis. The information regarding: 1) the number of full-time/part-time Federal employee(s) working to oversee the contractor; and 2) whether the Federal employee(s) assigned to oversee the service contractor will work at the contractor's worksite is listed in the table below:

Contract Number/TO Number	Performance Location (if FTE will work at Contractor worksite)	Number of Federal Employee(s)	Full-Time or Part-Time Oversight
GS-10F-0237L /HSHQDC-10-F-00080	No	1	Part-Time
Fill in TOTALS:		1	#FT: 0 #PT: 1

9. Program Office Contracting Officer Technical Representative (COTR) Information:
Proposed COTR Official: (b) (6)
COTR Certification and Training: (b) (6) is certified as of October 26, 2006, and current with required training COTR responsibilities: This is an ancillary duty for the COTR whose primary responsibility is the (b) (6). In addition to this task order, the COTR currently manages two (2) other contracts. Although the COTR's responsibilities are ancillary, the COTR has sufficient time and resources to adequately manage and oversee this task order. The other contract vehicles currently administered by the COTR are listed in the table below:

Contract Number	Task Order Number	Contractor Name	Dollar Value
HSHQDC-09-X-00598		SPAWAR	$1,521,282.00
HSHQDC-09-X-00644		MACE	$890,715.23

10. The services that the contractor will perform for DHS will relate to the mission of Office of Operations Coordination and Planning, Operations Coordination Division by providing media monitoring support and social media/networking support services to the National Operations Center (NOC) on a 24/7/365 basis to enhance DHS OPS situational awareness, fusion and analysis and decision support to senior leaders. The NOC coordinates

information sharing to help deter, detect, and prevent terrorist acts and to manage domestic incidents.

11. The Federal employee supports the mission of the Office of Operations Coordination and Planning, Operations Coordination Division by overseeing the Battle Lab which monitors world situations and events.

Determination

Based on the above findings, under the authority of FAR 7.503(e), and in accordance with the Department of Homeland Security Acquisition Manual (HSAM), Subchapter 3007.5, Inherently Governmental Functions, I have determined that the acquisition of the proposed professional services do not include inherently governmental or nearly inherently governmental requirements, personal service requirements, or requirements that impact core functions that must be performed by federal employees. Further, the number of Federal employees within the Office of Operations Coordination and Planning, Operations Coordination Division is sufficient to provide adequate direction and oversight to the professional service contractor employees.

(b) (6)
Director, Battle Lab

11/30/10
Date

(b) (6)
Contracting Officer

Date

APPROVAL:
(For actions with an annual value greater than $1 million but not exceeding $50 million)

(b) (6)
Executive Director, Office of Procurement Operations
Head of Contracting Activity

Date

Sample: Proposal Evaluation Plan

Basis of Evaluation (check one):

X Best Value Trade-Off
□ Lowest-Price, Technically Acceptable
□ Other

Non-Cost Factors

Evaluation factors and significant subfactors shall be listed, and their relative order of importance cited in adjectival terms Numerical ratings shall not be used in the evaluation of delivery order proposals.

List the specific areas of your technical requirements to be evaluated. These areas should correspond with, and relate to, specific requirements

1. Technical Approach

The contractor will be evaluated on its effort to provide unclassified, open source, multi-media technical and analytical support services for NOC Operations which operates 24 hours a day, seven (7) days a week, and 365 days a year (24x7x365). These are two 24x7x365 functions, one to specialize in Media Monitoring and other to specialize in Social Networks. Shifts shall be developed by the contractor to ensure that each desk is covered at all times.

List the specific areas of your management requirements to be evaluated. These areas should correspond with, and relate to, specific requirements

2. Management Approach and Key Personnel

The contractor's proposal shall indicate the labor category and FTE hours (broken out by respective task areas). Additionally, the contract's proposal should identify subject matter experience/qualifications/certifications proposed for each FTE in each task area identified in this SOW. The contractor will be evaluated based on experience conducting outreach and providing support to DHS National Operations Center(NOC) Media Monitoring Capability support, Office of Operations Coordination and Planning, Department of Homeland Security

List the specific areas of your past performance requirements to be evaluated. These areas should relate to specific work statement requirements.

3. Past Performance

The contractor will be evaluated on the quality of past performance by, and relevant experience of, its own staff and/or the staff of partners/subcontractors in each task order area (strategic outreach and communications planning; ability to conduct awareness and communications campaigns; ability to execute mission integration engagements to include evaluating and initiating engagements with users, gathering user requirements and communicating requirements to the development team, training users, providing support and assistance to users in furtherance of fostering positive user experiences and relationships with DHS); and the degree of flexibility in previous engagements. Past performance will not be limited to the submitted past performance references. Past performance by offerors or their team members with incumbent performance on similar DHS or other government agency programs will be verified and considered as part of the past performance evaluation.

List any other evaluation criteria important to you, and their relative order of importance below.

Order of Importance of Technical Factors

List the order of importance with regards to corporate experience, technical/management approach and any other non-cost criteria for which you may want to evaluate contractor proposals. Examples: a) Factor 1 is more important that Factor 2; Factor 2 is more important that Factor 3; b) Factor 1 and Factor 2 are equal; Factors 1 and 2 are more important than Factor 3.

Past performance is more important than technical approach and management approach and key personnel when combined.

Cost Factor

Note that balancing cost against the non-cost factors is how you make your best value trade-off decision, and as a result, a percentage is not applied to the cost factor. Indicate whether all non-cost evaluation factors, when combined:

□ Are significantly more important than: X More important than: □ Comparatively equal to:

...the cost factor

Task	Description	Eagle Labor Category	6 MONTH Base	Year 1 Labor Rate	Year 2 Labor Rate	Year 3 Labor Rate	Year 4 Labor Rate	Base Labor Hours	Option Labor Hours	Unit	6 MONTH Base Year	Year 1	Year 2	Year 3	Year 4
4.1	Media Monitoring	Functional Analyst	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	4800	9600	Hours	$ [redacted]	[redacted]	[redacted]	[redacted]	[redacted]
4 2	Social Networking	Functional Analyst	[redacted]	[redacted]	(b) (4) [redacted]	[redacted]	[redacted]	4800	9600	Hours	$ [redacted]	[redacted]	(b) (4) [redacted]	[redacted]	[redacted]
	SURGE		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	400	730	Hours	$ [redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	Travel							1		LT	$ [redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	Total										$ [redacted]	[redacted]	(b) (4) [redacted]	[redacted]	[redacted]

Total	$	8,220,367.20

MARKET RESEARCH REPORT

Authority

Market research is required in accordance with:

- FAR 7.102, Acquisition Planning Policy.
- FAR 10.001, Market Research Policy.
- POP 203, Conducting Market Research

Background Information

Describe the background of the procurement and circumstances/events leading up to the requirement.

The Operations Coordination Division of the Office of Operations Coordination and Planning has a requirement for Media Monitoring Center support services. The period of performance shall be for one twelve (12) month base period and four (4) twelve month option periods. The requirement has an estimated value of $9.2 million. Also, the contractor is required to have a Secret facility clearance and contractor personnel are required to have a Secret clearance. Market research was conducted for this requirement from June 1, 2008 through January 1, 2009.

The services are currently provided by SPAWAR through Interagency Agreement (IAA) HSHQDC-07-X-00816. The IAA expires on 31 December 2009.

The Program Office Point of Contact is (b) (6) The Acquisition Team members are listed in the following chart.

Name	Title	Office	Telephone	Email Address
(b) (6)	Senior Watch Officer	Operations Coordination (OPS)	202-282(b) (6)	(b) (6) @dhs.gov
(b) (6)	Management & Program Analyst	Budget and Acquisition	202-282(b) (6)	(b) (6) @dhs.gov
(b) (6)	Contract Specialist	Office of Procurement Operations (OPO)	202-447(b) (6)	(b) (6) @dhs.gov
(b) (6)	Contracting Officer	Office of Procurement Operations (OPO)	202-447(b) (6)	(b) (6) @dhs.gov

Initial Requirements (as identified by the Program Office)

- Describe the essential physical and performance characteristics/functions required to meet the Government's needs. Describe what the product or service must do.

The Media Monitoring Center (MMC) is designed to monitor, collect, analyze, and forward operationally relevant open source information to the DHS National Operations Center (NOC). The Social Media/Networking (S/N) initiative involves advising the Director of Operations Coordination and Planning on the integration of Social Media/Networking into DHS OPS operations in order to enhance DHS OPS situational awareness, fusion and analysis, and decision support to senior leaders.

- Describe the performance requirements (i.e., the qualities and attributes of the product or service)

Provide 24 hour 7 day a week support, timely dissemination of information.

- Describe distinguishing characteristics

None

- Describe physical characteristic requirements

None

- Address any cost effectiveness issues associated with requirements

The method of gathering and digesting information and the reporting method will potentially cost more and be a tradeoff to the government.

- Describe schedule requirements

Contract needs to be awarded mid November to allow security clearances to be transferred and the POP to start 1/1/2010.   Once awarded the contractor will have to staff 24x7x365

- Identify DHS Advance Acquisition Plan including AAP number, when plan was published to the public, if part of the DHS Forecast of Small Business Opportunities

Participants in Market Research

Describe the involvement of the individual Acquisition Team members and any other participants in the market research effort.

Name	Title	Office	Telephone	Email Address	Role in Market Research
(b) (6)	Program Official	OPS	202-282(b) (6)	(b) (6)@dhs.gov	Assisted in the preparation of the Market Research Report
(b) (6)	Contracting Officer	OPO	202-447(b) (6)	(b) (6)@dhs.gov	Approve Market Research Report
(b) (6)	Contract Specialist	OPO	202-447(b) (6)	(b) (6)@dhs.gov	Assist Program Staff in documenting requirement
(b) (6)	Small Business Specialist	OPO	202- 447(b) (6)	(b) (6)@dhs.gov	Review Market Research Report to determine acquisition's potential inclusion into the socioeconomic program
(b) (6)	Management & Program Analyst	OPS	202-828(b) (6)	(b) (6)@dhs.gov	Prepare Market Research Report

Market Research Techniques and Sources

Indicate techniques and sources used during market research investigation. The following table may help structure and summarize the techniques used in the market research.

Check if part of research	Sources Used in Market Research	Details of Research/Comments
	Research Sources	
	DHS Advance Acquisition Plan reviewed	
X	Acquisition history reviewed	
	Other recent market research reviewed	
	Interviewed knowledgeable individuals in industry	
X	Interviewed knowledgeable individuals in Government	
X	Government databases reviewed	www.ccr.gov; GSA Advantage; www.epls.gov
	Commercial databases reviewed	
	Participated/Attended Tradeshows and Industry Conferences	
	Professional Journals reviewed	
	Source Lists of DHS and Other Government agencies	

Check if part of research	Sources Used in Market Research	Details of Research/Comments
	reviewed	
	Catalog and Product Literature reviewed	
	Participated in DHS Small Business Vendor Outreach Sessions	
	Reviewed requirement with OPO Small Business Specialist	
	Other __________________	
	Other __________________	
	Other __________________	
	Mandatory Sources Reviewed	
	Products: Agency inventories	Requirement is not for a product
	Products: Excess from other agencies	Requirement is not for a product
	Products: Federal Prison Industries at www.unicor.gov	Requirement is not for a product
	Products: Procurement list maintained by the Committee for Purchase from People who are Blind or Severely Disabled (Ability One (formerly Javits-Wagner-O'Day (JWOD)) Program at www.jwod.gov/procurementlist	Requirement is not for a product
	Products: Wholesale supply sources (such as GSA)	Requirement is not for a product
	Products: Mandatory Federal Supply Schedules (GSA Advantage) at www.gsaadvantage.gov	Requirement is not for a product
	Products: Optional Use Federal Supply Schedules (GSA Advantage) at www.gsaadvantage.gov	Requirement is not for a product
	Products: Commercial sources	Requirement is not for a product
X	Services: Procurement list maintained by the Committee for Purchase from People who are Blind or Severely Disabled (AbilityOne (formerly Javits-Wagner-O'Day (JWOD) Program)	Services not provided by source
NA	Services: Mandatory Federal Supply Schedules (FSS)	Services not listed in mandatory FSS
X	Services: Optional Use Federal Supply Schedules	OPS would like to use an optional FSS
NA	Services: Federal Prison Industries	Services not provided by source
	Mandatory sources reviewed (per FAR Part 9) if applicable for: • Public utility services • Printing and related supplies • Leased motor vehicles • Helium	Requirement is not for any of these items or services
	Other __________________	
	References/Sources Checked	
X	Central Contractor Registration (CCR) at www.ccr.gov	Checked for registration in CCR

Check if part of research	Sources Used in Market Research	Details of Research/Comments
X	Department of Labor provides Service Contract Act (SCA) and Davis-Bacon Act (DBA) wage determinations information at www.wdol.gov	Professional Services, not covered under SCA
	Past Performance Information Retrieval System (PPIRS) at www.ppirs.gov	
X	Excluded Parties List System (EPLS) at www.epls.gov	Suggested sources not listed on EPLS
	Other __________________	
	Contracting Officer-led Activities	
	Industry Conferences	
	Sources Sought Notices: Requests for Information (RFIs)	
	Sources Sought Notices: RFI published in an Industry or Association Publication	
	Sources Sought Notices: FedBizOpps at www.fedbizopps.gov	
	Pre-Solicitation Conferences	
	Pre-proposal conference	
	Site Visits	
	One-on-one Vendor Discussions	
	Other __________________	

Available Sources and Characteristics of their Product/Service

- Identify potential sources contacted (and date contacted) or known

None Contacted

- Identify potential brand name products known

None

- Identify business category of each potential source

Business Category	Name of Potential Sources
Large business	Booz Allen - GS-23F-9755H Mantech - GS-23F-9819H General Dynamics - GS-10F-0237L
Small business	Kadix Systems - GS-10F-0278R Tech and Management Resourcing - GS-10F-0336P
Small/disadvantaged business	

Business Category	Name of Potential Sources
Section 8(a) business	
Woman-owned business	
HUBZone Small Business	
Veteran Owned Small Business	
Service Disabled Veteran Owned Small Business	

- If sole source, describe efforts to locate additional sources
- Summarize the information obtained from each source contacted including a summary of their product/service characteristics & capabilities

None contacted but reviewed vendor websites

<u>Extent of the Commercial Marketplace</u>

- Describe marketplace
- Assess Government's leverage in marketplace
- Describe nature of other market participants, e.g. other governments (foreign, state/local), commercial firms, etc.
- Identify availability of commercial or non-developmental items that satisfy requirement (value or shortcomings of each) and sub components

This service is used in the government and private sectors; therefore it is not a unique requirement and should be available in the commercial marketplace.

<u>Prevalent Business Practices</u>

- Identify standard/customary terms & conditions and industry business practices (include information on payment, freight delivery, acceptance, and warranties).

General commercial terms and conditions, invoice monthly.

- Identify generally accepted business practices that differ from standard Government practices

None

- Identify if contract financing is applicable. If so, ensure compliance with FAR 32.202-3, Conducting Market Research About Financing Terms

None

Market and Pricing Issues

- Identify pricing issues, price ranges, and price variations

Service is requested using the GSA schedule labor categories/pricing

- Identify trends - technical/pricing/business/etc.

None

Other Considerations

- Identify other considerations gathered from market research, e.g., opportunities to "unbundle" requirements to enable more contracts or subcontracts to small, small disadvantaged and other socio-economic procurement categories
- Quality factors, including such issues as past performance, references, product testing or evaluation, customer satisfaction, warranties, and quality problems
- What are the environmental concerns?
- What is the extent of recovered materials used in market products?
- What are the energy efficiency standards in the marketplace?

Not applicable

Market Analysis Summary

- Analyze the data gathered during market research
- Summarize the market analysis
- Provide market research conclusions and recommendations
- Document the decision and rationale to satisfy the agency's need with a commercial item/services, if market research so warrants
- Document the decision and rationale if the agency's need *cannot* be satisfied with a commercial item/services
- Document the actions taken as a result of the market research

The following table provides a checklist for the Market Analysis Summary information.

Yes	No	N/A	Market Analysis Summary
X			Are there sources capable of satisfying the government's requirements?
X			Are commercial items/services available: To meet requirements?
		X	Are commercial items available: That could be modified to meet requirements?
		X	Are commercial items available: That could meet requirements if the requirements are modified to a reasonable extent?
	X		Are available items used exclusively for governmental purposes?
		X	If commercial items are not available, are non-developmental items available to meet requirements?

Yes	No	N/A	Market Analysis Summary
		X	If commercial items are not available, are non-developmental items available that could be modified to meet requirements?
		X	If commercial items are not available, are non-developmental items available that could meet requirements if the requirements are modified to a reasonable extent?
		X	Could commercial items or non-developmental items be incorporated at the component level?
	X		Provided: Customary industry terms and conditions including warranties, buyer financing, discounts
	X		Provided: Requirements of any laws and regulations unique to the item being acquired
	X		Provided: Extent of competitive environment
	X		Provided: Environmental concerns
	X		Provided: Extent of recovered materials used in market products
	X		Provided: Energy efficiency standards in the marketplace
	X		Provided: Distribution and support capabilities of potential vendors, including alternative arrangements and cost estimates
X			Provided: Size and status of potential sources (including small business status and if use of the source is required by the FAR Part 8)
	X		Provided: Identification of available commercial items and describes the respective merits and shortcomings of each.
	X		Provided: Description of any market conditions that may be time sensitive or changes in supply or demand, technology, laws, and supplier costs, etc.
	X		Provided: Identification of Potential sources. Description of capabilities of individual vendors; pricing information, delivery schedules, and standard terms and conditions, such as incentives and warranties.
	X		Provided: Any market surveys developed by industry or other Federal agencies.
	X		Provided: Pricing issues, price ranges, and price variations
	X		Provided: Description of industry/market trends - technical/pricing/business/etc.

Statement of Work (SOW)

1. PROJECT TITLE: National Operations Center (NOC) Media Monitoring Capability support, Office of Operations Coordination and Planning, Department of Homeland Security.

2. BACKGROUND

The DHS Office of Operations Coordination and Planning (OPS) is responsible for monitoring the overall security situation of the United States on a daily basis and coordinating activities within the Department and with all homeland security partners to include Federal agencies, the Governors, state Homeland Security Advisors, law enforcement, private sector, critical infrastructure operators in all 56 U.S. States, territories, and possessions and international.

DHS OPS mission is to integrate DHS and interagency planning and operations coordination in order to prevent, protect, respond to and recover from terrorist threats/attacks or threats from other man-made or natural disasters. In particular, DHS OPS collects, fuses and shares information, from a variety of sources, with Federal, state, local, tribal, territorial, private sector and international partners

The mission of the NOC is to be the primary national-level hub for domestic situational awareness, common operating picture, information fusion, information sharing, communications, and operations coordination pertaining to the prevention of terrorist attacks and domestic incident management._The NOC is an integrated watch function staffed 24x7 and in conjunction with the Office of Intelligence and Analysis (I&A), issues homeland security threat advisories and bulletins, as well as specific protective measures, to all homeland security partners.

3. SCOPE

The objectives of this effort are to provide unclassified, open source, multi-media technical and analytical support services for NOC Operations which operate 24 hours a day, seven (7) days a week, and 365 days a year (24x7x365). There are two 24x7x365 functions, one to specialize in Media Monitoring and the other to specialize in Social Networks. Shifts shall be developed by the contractor to ensure that each desk is covered at all times.

4. TASKS

4.1 The Contractor shall design a Media Monitoring Capability (MMC) to monitor, collect, analyze, and distribute operationally relevant open source information as part of the DHS National Operations Center (NOC). The operational hours of the MMC will be 24x7x365 a year. The MMC helps frame the operational picture that open source media is reporting, uncover problem areas for incident management leadership to further evaluate, identify nascent or evolving situations, and provide valuable information/imagery that can be used to corroborate and/or reconcile first reports. The Contractor shall understand DHS critical information requirements and monitor open sources news coverage for new incidents (Items of Interest – IOI) and with a perspective of how a story may be related to other important ongoing events and DHS activities. The Critical Information Requirements (CIR) are: Potential threats and hazards to the homeland, to DHS, other Federal agencies, state and local response units, facilities, and resources; Private sector; Public safety; Potential impact on DHS capability to accomplish the HSPD-5 mission; Identifying events with operational value and/or corroborating critical information; Identifying media reports that reflect adversely on the U. S. Government, DHS or prevent, protect, respond or recovery activities; The National planning scenarios.

4.1.1 The contractor shall perform a broad open sources search for information on breaking news stories. The contractor shall:

4.1.1.1 Monitor major broadcast news networks
4.1.1.2 Monitor and review all Associated Press (AP) stories generated within the U.S. by each state's AP bureau
4.1.1.3 Monitor and receive alerts on other wire service stories via categorized/focused Really Simple Syndication (RSS) feeds.
4.1.1.4 Monitor and receive alerts on local and regional broadcast news via categorized/focused text/video feeds
4.1.1.5 Monitor appropriate Internet web sites on breaking situational events
4.1.1.6 Monitor and receive full motion video (FMV) or other streaming media

4.1.2 In the event an incident has occurred and an Items of Interest (IOI) follow-on analysis is underway or research is ongoing on a National Security Situation/ International Security Situation (NSS/ISS), the contractor shall:

4.1.2.1 Continue to monitor major broadcast news networks (cable service)
4.1.2.2 Query and search Associated Press (AP) stories for information specific to the incident
4.1.2.3 Query and search broadcast news via categorized/focused text/video feeds for information specific to the incident
4.1.2.4 Query and search RSS feeds for information specific to the incident
4.1.2.5 Query and search the Internet using other search engines such as Google and Yahoo
4.1.2.6 Monitor and receive full motion video (FMV) or other streaming media specific to the incident

4.1.2.7 Monitor and search web sites including those representing regional and local media outlets (TV stations, radio stations, and newspapers source)

4.1.2.8 Continue to monitor/review reports available via above open sources for information on other breaking news stories

4.2 The Contractor shall provide Social Media/Networking (S/N) support to enhance DHS OPS situational awareness, fusion and analysis, and decision support to senior leaders. The Contractor shall:

4.2.1 Monitor, collect, analyze, and distribute operationally relevant S/N as part of the DHS National Operations Center (NOC).

4.2.2 Facilitate S/N support to provide:

4.2.2.1 Potential and emerging threats and hazards information for homeland security situational awareness, information sharing and decision support.

4.2.2.2 Evolving incidents, crisis management and other Homeland Security information available to the public to include public alerts and notifications both sent and received

4.2.2.3 Additional venues for the public to communicate critical information to the Department of Homeland Security that serve to corroborate or reconcile other reports or provide new information that has not come to the Department's attention

4.3 Task Order Management – Monthly Status Reports

The Contractor shall create monthly status reports. The status reports shall contain a heading with the following information at a minimum:

4.3.1 Contractor Name, Project Manager's Name and Telephone Number
4.3.2 Task Order Number and Task Order Period of Performance
4.3.3 Scope of Task Order
4.3.4 Period of Performance Being Reported
4.3.5 Submission Date

The Contractor shall assist DHS in compiling useful data on work performed under this task order. Each status report will contain the following items.

4.3.6 For each task, provide a summary of work completed
4.3.7 Identify any significant problems and their causes and impacts, proposed corrective actions
4.3.8 Travel, if any

5. DELIVERABLES AND DELIVERY SCHEDULE

All deliverables shall be prepared using Microsoft Office Suite tools and delivered electronically to the NOC Senior Watch Officer Inbox. Note: The Contractor shall include the Contracting Officer's Technical Representative (COTR), Contracting Officer and the Contract Specialist on the distribution of the monthly status report (Task 4.3).

Task Number	Deliverable Title	Due Date
4.1	NOC Media Monitoring Reports	As information emerges; 24/7/365 in accordance with NOC procedures
4.1	Media Summaries – historical average is 15	Daily, NLT 1700
4.1	Daily Media Operational Summaries	Daily
4.1	Weekly Data Reports	NLT Monday for the prior week
4.2	NOC Social Networking Reports	As information emerges; 24/7/365 in accordance with NOC procedures
4.2	Social Network Summaries	Daily, NLT 1700
4.2	Daily Social Network Operational Summaries	Daily
4.2	Weekly Data Reports	NLT Monday for the prior week
4.3	One (1) Monthly Status Report	Monthly, NLT the 5th business day of each month for the previous monthly period.

6. GOVERNMENT-FURNISHED EQUIPMENT (GFE) AND INFORMATION (GFI)

There will be no GFE or GFI provided under this task order.

7. PLACE OF PERFORMANCE

The place of performance will be at the contractor's facility.

8. PERIOD OF PERFORMANCE

The period of performance will be for a base period of twelve (12) months with four (4) twelve (12) month option periods.

9. SECURITY:

This task order does not require a security clearance. However, employees of the contractor working on media monitoring shall be a US citizen or maintain lawful resident status.

10. **CONFIDENTIALITY OF DATA AND INFORMATION**

The contractor may have access to information in the possession of the Government for which the Government's right to use and disclose the data and information is restricted, or which may be of a nature that its dissemination or use, other than in the performance of this contract, would be adverse to the interests of the Government or other parties. Therefore, the contractor agrees to abide by any restrictive use conditions on such data and not to:

(1) Knowingly disclose such data and information to others without written authorization from the Contracting Officer, unless the Government has made the data and information available to the public;

(2) Use for any purpose other than the performance of this contract.

The contractor agrees to hold the Government harmless and indemnify the Government from any cost/loss resulting from the unauthorized use or disclosure of third party data or software by the contractor, its employees, Sub-Contractors, or agents. While subcontracts are not anticipated under this Statement of Work, if deemed appropriate by both the Government and the contractor, the contractor agrees to include the substance of this provision in all subcontracts awarded under this contract.

Except as the Contracting Officer specifically authorizes in writing, upon completion of all work under the contract, the contractor shall return all such data and information obtained from the Government, including all copies, modifications, adaptation, or combinations thereof, to the Contracting Officer. Any data obtained from another company shall be disposed of in accordance with the contractor's agreement with that company, or, if the agreement makes no provision for disposition, shall be returned to that company. The contractor shall further certify in writing to the Contracting Officer that all copies, modifications, adaptations or combinations of such data or information which cannot reasonably be returned to the Contracting Officer (or to a company), have been deleted from the contractor's (and any Sub-Contractor's) records and destroyed.

READ NSTRUCTIONS ON NEXT PAGE

REQUISITION

PROCUREMENT REQUEST NO.
ROOP-10-00003/000006

REQUISITION DATE
05/19/2010

1. NAME, PHONE NUMBER, AND ROUTING SYMBOL OF PERSON TO CONTACT
(b) (6)

2. TYPE OF REQUEST (Check one)
A. □ NEW REQUEST
B. ☒ CHANGE TO PENDING PR NO. ROOP-10-00003
C. □ MODIFICATION TO CONTRACT OR ORDER NO.

3. ORIGINATING OFFICE DATA
Directorate of Operations

4. ADDITIONAL INFORMATION (Suggested supply sources, security data, etc.)

5. APPROVALS

APPROVING OFFICIALS (A)	ROUTING SYMBOL (B)	DATE (C)	INTERNAL ROUTING INITIALS (D)	INTERNAL ROUTING ROUTING SYMBOL (E)
(1) AUTHORIZED REQUISITIONER (b) (6)	OPS			
(2)				
(3)				
(4)				

6. CONSIGNEE AND DESTINATION
Department of Homeland Security
245 Murray Lane
Bldg. 410
Washington DC 20528

7. DATE(S) REQU RED

8. GOVERNMENT FURNISHED PROPERTY
□ YES ☒ NO (If "yes," see par. 8 of instructions on next page.)

9. DESCRIPTION OF ITEMS OR SERVICES

ITEM NO. (A)	ITEM OR SERVICE (Include Specifications and Special Instructions) (B)	QUANTITY (C)	UNIT (D)	ESTIMATED COST UNIT (E)	ESTIMATED COST AMOUNT (F)
	AAP Number: 55533 Grant Request: No LIST OF CHANGES: Total Amount for this Amendment: $1,164,803.52 Committed Amount for this Amendment: $290,122.24 CHANGES FOR LINE ITEM NUMBER: 1 Total Amount changed from $370,978.24 to $500,597.76 Committed Amount for this amendment: $129,619.52 CHANGES FOR LINE ITEM NUMBER: 2 Total Amount changed from $370,978.24 to $500,597.76 Committed Amount for this amendment: $129,619.52 CHANGES FOR LINE ITEM NUMBER: 4 Total Amount changed from $96,028.80 to $126,912.00 Committed Amount for this amendment: $30,883.20 Continued ...				
				TOTAL ESTIMATED COST	$290,122.24

10. ACCOUNT NG DATA
See Schedule

ITEM NO. (A)	ITEM OR SERVICE (Include Specifications and Special Instructions) (B)	QUANTITY (C)	UNIT (D)	ESTIMATED COST	
				UNIT PRICE (E)	AMOUNT (F)
	FOB: Destination Period of Performance: 05/24/2010 to 11/23/2011				

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEM

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER

PAGE 1 OF 20

2. CONTRACT NO.

3. AWARD/ EFFECTIVE DATE

4. ORDER NUMBER

5. SOLICITATION NUMBER HSHQDC-10-Q-00005

6. SOLICITATION ISSUE DATE 01/22/2010

7. FOR SOLICITATION INFORMATION CALL ▶ a. NAME (b) (6) b. TELEPHONE NUMBER *(No collect calls)* 2 (b) (6)

8. OFFER DUE DATE/LOCAL TIME 02/05/2010 1000 ES

9. ISSUED BY CODE DHS/OPO/IOAD

U.S. Dept. of Homeland Security
Office of Procurement Operations
Intel and Operations Acq. Division
245 Murray Lane, SW
Building 410
Washington DC 20528

10. THIS ACQUISITION IS ☒ UNRESTRICTED OR ☐ SET ASIDE: % FOR:

☐ SMALL BUSINESS ☐ EMERGING SMALL BUSINESS

NAICS: 541990 ☐ HUBZONE SMALL BUSINESS ☐ Sole Source

SIZE STANDARD: $6.5 ☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS ☐ 8(A)

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED ☐ SEE SCHEDULE

12. DISCOUNT TERMS

☐ 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION ☒ RFQ ☐ IFB ☐ RFP

15. DELIVER TO CODE

16. ADMINISTERED BY CODE DHS/OPO/IOAD

U.S. Dept. of Homeland Security
Office of Procurement Operations
Intel and Operations Acq. Division
245 Murray Lane, SW
Building 410
Washington DC 20528

17a. CONTRACTOR/ OFFEROR CODE FACILITY CODE

TELEPHONE NO.

18a. PAYMENT WILL BE MADE BY CODE

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	The U.S. Department of Homeland Security (DHS) intends to issue a hybrid firm-fixed price/time and material task order against a Contractor's General Services Administration (GSA) Mission Oriented Business Integrated Services (MOBIS) contract under Special Item Number (SIN) 874-1 (Consulting Services) for media monitoring and social media/ networking support services to the DHS Office of Operations Coordination and Planning. The period of performance for this task order is for one seven (7) month base period				

(Use Reverse and/or Attach Additional Sheets as Necessary)

25. ACCOUNTING AND APPROPRIATION DATA

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☐ 27b. CONTRACT/PURCHASE ORDER NCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☒ 28. CONTRACTOR IS REQU RED TO SIGN THIS DOCUMENT AND RETURN 1 COP ES TO ISSU NG OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE DENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED HEREIN.

☐ 29. AWARD OF CONTRACT REF. ____________ OFFER DATED ____________. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*

30b. NAME AND TITLE OF SIGNER *(Type or print)*

30c. DATE SIGNED

31b. NAME OF CONTRACTING OFFICER *(Type or print)* (b) (6)

31c. DATE SIGNED

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	and four (4) twelve (12) month option periods. One (1) award will be made to the Offeror whose quote is determined to best meet the needs of the Government after consideration of all factors, that is, the quote that provides the best value to the Government. Best value is defined as the offer that results in the most advantageous acquisition decision for the Government as determined by trade off analysis among the non-price and price factors.				
0001	Base Period: Media Monitoring Support Services (Fixed Price) IAW SOW Section 4.1	7	MO		
0002	Base Period: Social Media/Networking Support Services (Fixed Price) IAW SOW Section 4.2	7	MO		
0003	Base Period: OPTIONAL TASK: Surge Support (Labor Hour) IAW SOW Section 4.3 NOT TO EXCEED $35,802 1 LO = Up to $35,802 of the following labor categories: TO BE DETERMINED AT AWARD Continued ...	1	LO		

32a. QUANTITY IN COLUMN 21 HAS BEEN

□ RECEIVED □ INSPECTED □ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED:

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32c. DATE

32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAIL NG ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32g. E-MA L OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER

□ PARTIAL □ FINAL

34. VOUCHER NUMBER

35. AMOUNT VERIFIED CORRECT FOR

36. PAYMENT

□ COMPLETE □ PARTIAL □ FINAL

37. CHECK NUMBER

38. S/R ACCOUNT NUMBER

39. S/R VOUCHER NUMBER

40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT

41b. SIGNATURE AND TITLE OF CERTIFY NG OFFICER

41c. DATE

42a. RECEIVED BY *(Print)*

42b. RECEIVED AT *(Location)*

42c. DATE REC'D *(YY/MM/DD)*

42d. TOTAL CONTAINERS

NAME OF OFFEROR OR CONTRACTOR

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	The ceiling price shall not exceed $35,802. (Option Line Item)				
0004	Base Period: Task Order Management - Project Management (Fixed Price) IAW SOW Section 4.4.1	7	MO		
0005	Base Period: Travel (Cost Reimbursement) IAW SOW Section 10 NOT TO EXCEED $3,000				
1001	Option Period 1: Media Monitoring Support Services (Fixed Price) IAW SOW Section 4.1 (Option Line Item)	12	MO		
1002	Option Period 1: Social Media/Networking Support Services (Fixed Price) IAW SOW Section 4.2 (Option Line Item)	12	MO		
1003	Option Period 1: OPTIONAL TASK: Surge Support (Labor Hour) IAW SOW Section 4.3 NOT TO EXCEED $63,772.80 1 LO = Up to $63,772.80 of the following labor categories: TO BE DETERMINED AT AWARD The ceiling price shall not exceed $63,772.80. (Option Line Item)	1	LO		
1004	Option Period 1: Task Order Management - Project Management (Fixed Price) IAW SOW Section 4.4.1 (Option Line Item)	12	MO		
1005	Option Period 1: Travel (Cost Reimbursement) IAW SOW Section 10 NOT TO EXCEED $5,000 (Option Line Item)				
2001	Option Period 2: Media Monitoring Support Services (Fixed Price) Continued ...	12	MO		

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
HSHQDC-10-Q-00005

NAME OF OFFEROR OR CONTRACTOR

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	IAW SOW Section 4.1 (Option Line Item)				
2002	Option Period 2: Social Media/Networking Support Services (Fixed Price) IAW SOW Section 4.2 (Option Line Item)	12	MO		
2003	Option Period 2: OPTIONAL TASK: Surge Support (Labor Hour) IAW SOW Section 4.3 NOT TO EXCEED $66,262.10 1 LO = Up to $66,262.10 of the following labor categories: TO BE DETERMINED AT AWARD The ceiling price shall not exceed $66,262.10. (Option Line Item)	1	LO		
2004	Option Period 2: Task Order Management - Project Management (Fixed Price) IAW SOW Section 4.4.1 (Option Line Item)	12	MO		
2005	Option Period 2: Travel (Cost Reimbursement) IAW SOW Section 10 NOT TO EXCEED $5,000 (Option Line Item)				
3001	Option Period 3: Media Monitoring Support Services (Fixed Price) IAW SOW Section 4.1 (Option Line Item)	12	MO		
3002	Option Period 3: Social Media/Networking Support Services (Fixed Price) IAW SOW Section 4.2 (Option Line Item)	12	MO		
3003	Option Period 3: OPTIONAL TASK: Surge Support (Labor Hour) IAW SOW Section 4.3 NOT TO EXCEED $68,583.50 1 LO = Up to $68,583.50 of the following labor Continued ...	1	LO		

NAME OF OFFEROR OR CONTRACTOR

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	categories: TO BE DETERMINED AT AWARD The ceiling price shall not exceed $68,583.50. (Option Line Item)				
3004	Option Period 3: Task Order Management - Project Management (Fixed Price) IAW SOW Section 4.4.1 (Option Line Item)	12	MO		
3005	Option Period 3: Travel (Cost Reimbursement) IAW SOW Section 10 NOT TO EXCEED $5,000 (Option Line Item)				
4001	Option Period 4: Media Monitoring Support Services (Fixed Price) IAW SOW Section 4.1 (Option Line Item)	12	MO		
4002	Option Period 4: Social Media/Networking Support Services (Fixed Price) IAW SOW Section 4.2 (Option Line Item)	12	MO		
4003	Option Period 4: OPTIONAL TASK: Surge Support (Labor Hour) IAW SOW Section 4.3 NOT TO EXCEED $70,780.80 1 LO = Up to $70,780.80 of the following labor categories: TO BE DETERMINED AT AWARD The ceiling price shall not exceed $70,780.80. (Option Line Item)	1	LO		
4004	Option Period 4: Task Order Management - Project Management (Fixed Price) IAW SOW Section 4.4.1 (Option Line Item)	12	MO		
4005	Option Period 4: Travel (Cost Reimbursement) IAW SOW Section 10 Continued ...				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
HSHQDC-10-Q-00005

NAME OF OFFEROR OR CONTRACTOR

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	NOT TO EXCEED $5,000 (Option Line Item)				
4006	OPTIONAL TASK: Task Order Management: Transition Closeout Plan (Fixed Price) IAW SOW Section 4.4.4 (Option Line Item)	1	LO		
4007	OPTIONAL TASK: Task Order Management: Transition Closeout Activities (Fixed Price) IAW SOW Section 4.4.5 (Option Line Item)	1	LO		

SECTION 1: SERVICES AND PRICES

1.1 Task Order Type

This is a hybrid firm-fixed price and time and material task order against the Contractor's General Services Administration (GSA) Mission Oriented Business Integrated Services (MOBIS) contract TO BE DETERMINED AT AWARD.

1.2 Supplies and Services

The Contractor shall provide media monitoring and social media/networking support services to the DHS Office of Operations Coordination and Planning.

1.3 Price Schedule

See pages one (1) through six (6) of this Request for Quote.

SECTION 2: STATEMENT OF WORK (SOW)

SEE ATTACHMENT 1

SECTION 3: PACKAGING AND MARKING

See SOW Section 5 for packaging and marking instructions for deliverables.

SECTION 4: INSPECTION AND ACCEPTANCE

An inspection, acceptance and receiving report shall be signed by an authorized Government representative to evidence receipt, inspection and acceptance. The report shall be completed at the place(s) specified in the task order for Government receipt and acceptance. DHS Form 700-21, Material Inspection and Receiving Report, will be used for this purpose.

DHS inspection and acceptance of services, reports and other required deliverables or outputs shall take place at:

U. S. Department of Homeland Security
Office of Coordination and Planning
245 Murray Lane, SW
Building 410
Washington, DC 20528

Or at any other location designated by the Contracting Officer's Technical Representative (COTR) where the services are performed and reports and deliverables or outputs are produced or submitted. The COTR, listed in Section 6.1.3, has been delegated authority to inspect and accept all services, reports, and required deliverables or outputs.

SECTION 5: DELIVERABLES OR PERFORMANCE

5.1 Period of Performance

The period of performance of this task order is for one (1) seven (7) month base period and four (4) twelve (12) month option periods.

5.2 Place of Performance

The place of performance will be at the Contractor's facility.

5.3 Deliverables

See the Deliverable Table in Section 5.2 of the SOW.

SECTION 6: CONTRACT ADMINISTRATION

6.1 Points of Contact for this task order

6.1.1 (b) (6) Contracting Officer
U.S. Department of Homeland Security
Office of Procurement Operations (MGMT/OPO) / Stop 0115
245 Murray Lane
Washington, DC 20528-0115
(b) (6)

6.1.2 (b) (6) Contract Specialist
U.S. Department of Homeland Security
Office of Procurement Operations (MGMT/OPO) / Stop 0115
245 Murray Lane
0115
(b) (6)

6.1.3 Contracting Officer's Technical Representative (COTR)

TO BE DETERMINED AT AWARD

6.2 Invoice and Payment Provisions

6.2.1 The original invoice shall be submitted to the following Finance office:

ATTN: (b) (6) Finance Division, Building 66
Department of Homeland Security
Federal Law Enforcement Training Center (FLETC)
1131 Chapel Crossing Road
Bldg. 66 – FINANCE
Glynco, GA 31524
(b) (6) (phone)
(b) (6)

Copies of the invoice shall be submitted to FLETC, the Contracting Officer, Contract Specialist and the COTR concurrently. The invoice must contain the 1) contract number; 2) order number; and 3) applicable contract line item number(s) (CLIN).

To constitute a proper invoice, the invoices must include those items cited in FAR 52.232-1 Payments (APR 1984), FAR 52.232-7 Payments under Time-and Materials and Labor-Hour Contracts (FEB 2007) and FAR 52.232-25 Prompt Payment (OCT 2008), paragraphs (a)(3)(i) through (a)(3)(x).

6.2.2 Payment shall be made to the contractor upon delivery to and acceptance by the Government office requesting services in the following manner:

6.2.2.1 For CLINs 4006 and 4007, the contractor is authorized to bill, upon completion of the services, the associated unit price for the CLINs delineated in the Price schedule.

6.2.2.2 For CLINs 0001, 0002, 0004, 1001, 1002, 1004, 2001, 2002, 2004, 3001, 3002, 3004, 4001, 4002 and 4004, the contractor is authorized to bill, on monthly basis, the associated unit price for the CLINs delineated in the Price schedule.

6.2.2.3 For CLINs 0003, 1003, 2003, 3003 and 4003, the contractor is authorized to bill, on a monthly basis, for the direct labor hours performed at the rates delineated in the Price schedule.

6.2.2.4 For CLINs 0005, 1005, 2005, 3005 and 4005, the contractor is authorized to bill, on a monthly basis, for the travel costs associated with completed travel.

SECTION 7: SPECIAL CONTRACT REQUIREMENTS

7.1 Travel

Costs for transportation, lodging, meals and incidental expenses incurred by contractor personnel on official company business are allowable subject to FAR 31.205-46, Travel Costs. These costs will be considered to be reasonable and allowable only to the extent that they do not exceed on a daily basis the maximum per diem rates in effect at the time of travel as set forth in the Federal Travel Regulations. The contractor will not be reimbursed for travel expenses within a 50-mile radius of the worksite. Local travel expenses within the Washington Metropolitan area will not be reimbursed (this includes parking). All travel outside the Washington Metropolitan area must be approved by the COTR in advance. No travel will be reimbursed without prior approval from the COTR. Unless approved in advance by the CO, the contractor's travel shall not exceed the maximum per diem rates established by the General Services Administration.

7.2 Post Award Evaluation of Contractor Performance

7.2.1 Contractor Performance Evaluations

In accordance with FAR Subpart 42.1502, Policy, agencies are required to prepare an evaluation of contractor performance for each (non-construction/A&E) contract in excess of $100,000. An assessment must be prepared at least annually and at the conclusion of the contract. In addition, contracts with a period of performance exceeding one year (including option periods) require interim evaluations so as to document contractor performance and provide current information for source selection purposes.

7.2.2 Contractor Performance Assessment Reporting System (CPARS)

The U.S. Department of Homeland Security utilizes the Department of Defense's Contractor Performance Assessment Reporting System (CPARS), a web-enabled application that collects and manages the library of automated contractor performance assessments, to collect and maintain contractor performance assessments. An assessment evaluated evaluates a contractor's performance, both positive and negative, and provides a record on a given contractor during a specific period of time, under a specific contract or task order. CPARS is for UNCLASSIFIED use only.

7.2.3 Contractor Performance Information

The DHS Office of Procurement Operations' (OPO) assessments of contractor performance shall be accessed by the contractor electronically after completion of the assessment by logging onto CPARS at https://www.cpars.csd.disa.mil. Contractors shall be given a minimum of thirty days to submit comments, rebut statements, and/or provide additional information to the Government.

The OPO Assessing Official shall review the Assessing Official Representative's assessment and consider the potential for disagreements between the Government and the contractor. If the contractor's response to the report is contentious, the Assessing Official will forward the evaluation to the Reviewing Official, who will serve as the mediator and shall resolve any dispute between the contractor and Government. If the Reviewing Official cannot resolve the dispute, the matter shall be referred to the Deputy Director, Office of Procurement Operations, for decision and resolution.

Copies of the evaluation, contractor response, and review comments, if any, shall be retained as part of the evaluation. The evaluation may be used to support future award decisions. The release of the completed contractor evaluation shall be restricted to Government personnel and the contractor whose performance is being evaluated. Once the evaluation is completed, it is copied into the Past Performance Information Retrieval System (PPIRS), a web-enabled, government-wide application that provides timely and pertinent contractor past performance information to the Federal acquisition community for use in making source selection decisions, where it can be viewed by authorized personnel at any agency for source selection purposes.

SECTION 8: TASK ORDER CLAUSES

8.1 The Contractor's GSA MOBIS contract clauses are incorporated into this task order.

8.2 Federal Acquisition Regulation (FAR) and Homeland Security Acquisition Regulation (HSAR) Clauses

NOTICE LISTING CONTRACT CLAUSES INCORPORATED BY REFERENCE

The following contract clauses pertinent to this section are hereby incorporated by reference (by Citation Number, Title, and Date) in accordance with the clause at FAR "52.252-2 CLAUSES INCORPORATED BY REFERENCE" in Section I of this contract. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at these addresses: http://www.arnet.gov/far, http://farsite.hill.af.mil/VFHSARA.HTM.

CITATION NUMBER	**TITLE**	**DATE**
FAR 52.237-3	CONTINUITY OF SERVICES	JAN 1991
FAR 52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION	JAN 2009
HSAR 3052.222-70	STRIKES OR PICKETING AFFECTING TIMELY COMPLETION OF THE CONTRACT WORK	DEC 2003
HSAR3052.242-71	DISSEMINATION OF CONTRACT INFORMATION	DEC 2003
HSAR 3052.242-72	CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE	DEC 2003

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

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days of the end of the current period of performance.

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

(a) The Government may extend the term of this contract by written notice to the Contractor within 29 days of the end of the current period of performance; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 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 55 months.

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

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

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

The Key Personnel or Facilities under this Contract:

Project Manager - NAME TO BE INSERTED AT AWARD

SECTION 9: LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS

Attachment 1	Statement of Work (SOW) (11 pages)
Attachment 2	Past Performance Questionnaire (5 pages)

SECTION 10: MEDIA MONITORING DEMONSTRATION (MINIMUM REQUIREMENT)

Media Monitoring Demonstration

The offeror's summary sheet submissions will be evaluated based on the following:

a. Relevance of the Critical Information Requirements provided.
b. Accuracy of the information provided in the summary.
c. Inclusion of the following required minimum information:

   i. Identify the location of the event;
   ii. Identify the title of the event;
   iii. Identify which Critical Information Requirement is being summarize; and
   iv. Provide an Excerpt/Summary of a media story, media source and the link to media source if applicable.

d. Provide at least ten (10) Items of Interest (IOI) with at least eight (8) of those IOIs identifying print media as the source.

The Government will not further evaluate and will not consider for award quotes that contain summary sheet submissions that do not meet all of the above listed criteria. If the offeror successfully passes the minimum requirement, the offeror will be evaluated against criteria identified in Section 11 Evaluation Factors.

SECTION 11: EVALUATION FACTORS

The evaluation factors for this requirement are as follows:

1. Technical Approach
2. Management Approach
3. Personnel/Key Personnel
4. Past Performance
5. Price (not rated)

Factor 1, Factor 2, Factor 3, and Factor 4 are non-price evaluation factors.

Relative Importance of the Evaluation Factors

The non-price evaluation factors are equally important; and when combined together they are significantly more important than price, which is not rated.

SECTION 12: BASIS FOR AWARD

One (1) award will be made to the Offeror whose quote is determined to best meet the needs of the Government after consideration of all factors, that is, the quote that provides the best value to the Government. Best value is defined as the offer that results in the most advantageous acquisition decision for the Government as determined a trade off between the non-price and price factors.

As the evaluations of the non-price evaluation factors become more equal between the Offerors, price becomes more important in making the award determination. In the event that two or more offers are determined not to have any substantial technical differences (i.e., are substantially equivalent with respect to the non-price factors), award may be made to the lower priced offer. It should be noted that award may be made to other than the lower priced offer if the Government determines that a price premium is warranted due to technical merit. The Government may also award to other than the highest rated offer, if the Government determines that a price premium is not warranted.

The Government intends to award upon the basis of initial quotations, without holding discussions, although the Government reserves the right to hold discussions at the sole discretion of the Contracting Officer. Quoters are therefore cautioned that each initial quotation should contain the Offeror's best offer.

SECTION 13: EVALUATION CRITERIA

Quotes submitted in response to this RFQ will be evaluated based on the following criteria:

Factor 1: Technical Approach

The offeror's quote will be evaluated to determine if the offeror has demonstrated a thorough understanding of the requirements of the Statement of Work and has clearly articulated how each task will be accomplished.

Factor 2: Management Approach

The offeror's overall management approach demonstrates an effective approach to managing the requirements in the Statement of Work.

Factor 3: Personnel/Key Personnel

The offeror's quote will be evaluated to determine the offeror's ability to properly staff the requirement and the availability of personnel.

Factor 4: Past Performance

The Offeror's quote will be evaluated to determine the extent to which their performance demonstrates the likelihood of successful performance in providing requirements similar in size and scope to this solicitation. The Government may choose to evaluate publicly available reports, and/or data from the Past Performance Information Retrieval System (PPIRS). The Government may use present and/or past performance data obtained from a variety of sources, not just those contracts identified by Offeror. The information gathered for past performance may also be used in the responsibility determination.

The Government will review all past performance data submitted with the quote and may contact all of the referenced companies/organizations and others to verify past performance information.

If the Government receives a "poor" or "unsatisfactory" rating from a reference or negative past performance information from any other source on which the Offeror has not had a previous opportunity to comment, the Offeror will be afforded the opportunity to comment on the negative information.

If the Offeror is a new entity and none of its principals have ever performed work for others that is similar to the requirement in this solicitation, the Offeror will be rated neutral on the past performance factor.

Factor 5: Price

In evaluating price, the Government will consider the level of effort and the mix of labor proposed to perform a specific task being ordered, and for determining that the total price is reasonable in accordance with FAR 8.405-2 (d).

The Government expects to receive price competition through the submission of price quotations from multiple vendors.

The Government will validate that any information provided in other parts of the quotation is consistent with the information provided in the price quotation. Any inconsistencies will be noted and may adversely affect the quotation evaluation.

The Government will evaluate quotations for award purposes by adding the total price for all options to the price for the base requirement. Evaluation of options does not oblige the Government to exercise the options.

The Government will consider the option at 52.217-8 to have been evaluated through the evaluation of rates proposed for all contract periods. Offerors should assume that if the

Government exercises clause 52.217-8 to extend performance, that the option will be priced at the rates in effect when the option is exercised.

SECTION 14: INSTRUCTIONS

Each Quoter shall electronically submit its quotation to (b) (6) **at** (b) (6) **and** (b) (6) **by <u>10 A.M. Eastern Standard Time (EST) on February 5, 2010</u>.** Hand delivered and faxed quotes will not be accepted.

The technical and price quotes shall be separate documents so that the evaluation of each part may be conducted independently. The page limitations for each quote are as follows:

Volume 1: Technical Quote – Limited to 15 Pages (excluding cover letter, table of contents, resumes, past performance references and past performance questionnaires)

Volume 2: Price Quote – No Page Limitation

MEDIA MONTORING DEMONSTRATION (PASS/FAIL)

The offeror shall demonstrate their understanding of DHS critical information requirements and ability to monitor open sources of news coverage for the designated twenty-four (24) hour period beginning at 6:00 AM EST on February 1, 2010 and ending at 6:00 AM EST February 2, 2010. The offeror shall identify any new incidents and Items of Interest (IOI) with a perspective of how a story may be related to any important ongoing events and DHS activities.

The offeror shall provide written summaries of all Items of Interest (IOI) discovered during the designated time period. Items of Interest (IOI) discovered during the 24- hour period, shall meet the following Critical Information Requirements:

a. Report any potential threats or hazards to DHS Homeland Security, Federal Agencies, State and Local Governments and emergency response units, facilities and resources.
b. Identify any potential threats or hazards to public and private sector safety.
c. Identify any potential impact on DHS capacity to accomplish the HSPD-5 mission.
d. Report any media reports that reflect adversely on the U.S. Government and the Department of Homeland Security (DHS) ability to prevent, protect, and respond, to recovery efforts or activities related to any crisis or events which impact National Planning Scenarios.

The individual Item of Interest (IOI) summary sheet shall be no longer than one (1) page in length and shall include the following information at a minimum:

i. Identify the location of the event.
ii. Identify the title of the event.
iii. Identify which Critical Information Requirement is being summarize.

iv. Provide an Excerpt/Summary of a media story, media source and the link to media source if applicable and briefly discuss how potential threat or hazard can compromise the security of the homeland.

Electronically submit written summaries to [redacted] (b) (6) and [redacted] (b) (6) by <u>9 AM EST on February 2, 2010</u>. Please note that this date precedes the quote deadline.

<u>Volume 1: Technical Quote</u>

NOTE: The <u>technical quote must not contain any pricing information</u> but reference to resource information such as data concerning labor hours, labor categories, materials, subcontractors, etc. must be provided so that the Offeror's understanding of the requirements may be evaluated.

<u>Section A: Technical Approach</u>

The technical approach shall demonstrate the offeror's understanding of the requirements of the statement of work (SOW) and demonstrate the approach to accomplishing the tasks in the SOW.

<u>Section B: Management Approach</u>

The management approach shall demonstrate the offeror's approach to staffing, recruitment and replacement of personnel and subcontracting, if any. Also, the approach shall demonstrate the offeror's lines of authority for coordination and supervision of personnel including subcontractors, if any, and interfacing with the Government. Also, include a draft Transition Startup Plan that identifies all transition activities.

NOTE: A final version of the Draft Transition Startup Plan will be a separate deliverable due fifteen (15) calendar days after task order award.

<u>Section C: Personnel/Key Personnel</u>

The offeror's quote shall demonstrate that the proposed personnel have the skill levels, education, training and prior experience to perform the work required by the SOW. Identify the number of people and skill level mix for the period of performance. Identify the critical skills required to accomplish the effort and describe the personnel qualifications that will be required of these people. Provide a list of all subcontractors, if any, and identify the effort that they will be contracted to perform. The Offeror shall provide a staffing plan that identifies the labor categories along with the SOW tasks that they will be assigned to perform.

The Offeror shall provide resumes of the Key Personnel listed in SOW Section 6.1. The resumes shall contain, at a minimum, the company name and address, telephone number, point of contact, overview of duties and the dates employed. **A company overview, prepared by the offeror, is not considered a resume and will thus not meet this requirement.**

The quote shall also contain a job description of the proposed key personnel's duties as it relates to this requirement. Describe the availability and existing commitments of key personnel. Letters of commitment must be submitted for contingency hires, defined as persons not currently employed but who have executed a letter of commitment for employment with offeror, if the offeror receives award under subject solicitation. All information proposed will be evaluated to assure relevant technical experience, specialized training and time availability for the project as it relates to this requirement.

Section D: Past Performance

Identify at least three (3) contracts, task orders and/or delivery orders, either on-going or completed within the past thirty six (36) months prior to this solicitation issue date, including federal, state and local government and the private sector, that demonstrate at least satisfactory performance that is similar to this requirement. The Offeror may submit performance as a subcontractor, part of a team, joint venture or as part of a predecessor organization. Discuss any negative performance issues that occurred during the performance of the identified contracts and/or task orders and any corrective actions taken.

For each past performance reference submitted, provide the following information, in the format provided:

PAST PERFORMANCE	
Contract Type and Number (or Identifier)	
Name and Address of Company/Agency	
Contact Person	
Telephone and Fax Number of Contact Person	
E-mail Address of Contact Person	
Identify if you were the Prime or Subcontractor	
Period of Performance (e.g. start date and completion date)	
Contract Value	
Description of Work (Types of work performed, problems encountered and their resolutions, any subcontractors or partnerships…)	

Provide the Past Performance Questionnaire (see Attachment 2) to each reference; request that the reference complete the questionnaire and provide it to (b) (6) or by fax to (b) (6) by the quote deadline.

Volume 2: Price Quote

Each Offeror shall submit a price quote separate from the technical quote.

The Offeror’s price quote may be compared to the response to the technical approach to determine the Offeror’s (1) understanding of the work to be performed; and (2) capability and capacity to perform the required work and provide the required resources.

The price quote shall include the following:

a. Proposed labor categories that are consistent with the Offeror’s GSA Schedule contract. **The hourly rates shall not exceed the GSA Schedule contract rates. Offerors are strongly encouraged to offer discounts off of their published contract rates.** Identify by percent any discounts or price reductions offered.

b. Identification of the prime contractor’s rates and the subcontractor’s rates, if any.

c. A copy of the Offeror’s GSA Schedule contract that includes the hourly rates.

d. If an Offeror intends to recover indirect costs on travel, the price quote shall include a narrative statement which identifies the indirect rate(s) to be utilized and supporting independent documentation (e.g. DCAA audit) that substantiates the rate and states recovering indirect costs on travel is in accordance with the Offeror’s established accounting practices. Otherwise, the quote shall contain a statement that the Offeror does not intend to recover indirect costs on travel. The requirement for a narrative statement does not require the calculation of travel costs. Offerors shall not include a profit or fee on travel.

e. For each period of performance, provide a breakdown for each contract line item number (CLIN) that identifies 1) the labor categories proposed, 2) the corresponding hourly labor rate for each labor category, 3) total hours proposed for each labor category, 4) the total price for the CLIN, 5) the total price for the period of performance (e.g. base period and option period. Also provide a summary that shows the total price for each period of performance and the total price of the task order.

Contract Line Item Types

a. The following tasks in the SOW will be Firm-Fixed Price:

Task 4.1 - Media Monitoring
Task 4.2 - Social Media/Networking
Task 4.4.1 - Task Order Management – Project Management
Task 4.4.5 - OPTIONAL TASK – Task Order Management: Transition Closeout Plan
Task 4.4.6 - OPTIONAL TASK – Task Order Management: Transition Closeout Activities

b. The following tasks in the SOW will be Labor Hour:

Task 4.3 - OPTIONAL TASK – Surge Support

c. The following section in the SOW will be Cost Reimbursement:

Section 10 – Travel

Surge Support

The Government estimates surge support at:

- $35,802 for the base period;
- $63,772.80 for option period 1;
- $66,262.10 for option period 2;
- $68,583.50 for option period 3; and
- $70,780.80 for option period 4.

These amounts will serve as the surge support cost for the designated performance periods of the task order. Offerors, however, shall propose labor categories and labor rates for the surge support. The Task Order Contracting Officer's Technical Representative (COTR) will approve the time, place of performance and level of effort (hours) (b) or surge support prior to execution.

Travel

Travel will be reimbursed at cost. The Government estimates travel at $3,000 for the base period and $5,000 for each option period. These amounts will serve as the evaluated travel cost for the designated periods of the task order. Travel will be reimbursed in accordance with the Federal Travel Regulations. Travel must be approved in advance and in writing by the Task Order COTR.

> **REMINDER:** If an Offeror intends to recover indirect costs on travel, the price quote shall include a narrative statement which identifies the indirect rate(s) to be utilized and supporting documentation (e.g. DCAA audit) that substantiates the rate and states recovering indirect costs on travel is in accordance with the Offeror's established accounting practices. Otherwise, the quote should contain a statement that the Offeror does not intend to recover indirect costs on travel.

Thank you for your consideration of submitting a response to this request. If you have any questions, please contact (b) (6) Contract Specialist at (b) (6) or (b) (6)

STATEMENT OF WORK

1. PROJECT TITLE

Media Monitoring and Social Media/Networking Support Services for the Office of Operations Coordination and Planning's National Operations Center

2. BACKGROUND

The Department of Homeland Security's (DHS) Office of Operations Coordination and Planning (OPS) is responsible for monitoring the security of the United States on a daily basis and coordinating activities within the Department and with all homeland security partners which include Federal agencies, the Governors, state Homeland Security Advisors, law enforcement partners, private sector, critical infrastructure operators in all 50 States, territories, and possessions and international stakeholders.

The mission of the OPS is to integrate DHS and interagency planning and operations coordination in order to prevent, protect, respond to and recover from terrorist threats/attacks and other man-made or natural disasters. OPS maintains situational awareness by gathering, coordinating and sharing information among Federal, State, Local, Tribal, Private Sector and International Homeland Security partners.

Through the National Operations Center (NOC), the OPS provides real-time situational awareness and monitoring of the homeland, coordinates incidents and response activities, and, in conjunction with the Office of Intelligence and Analysis, issues advisories and bulletins concerning threats to homeland security, as well as specific protective measures. The NOC, which operates 24 hours a day, seven days a week, 365 days a year (24/7/365), coordinates information sharing to help deter, detect, and prevent terrorist acts and to manage domestic incidents.

3. OBJECTIVE

The objective of this effort is to provide media monitoring support and social media/networking support services to the NOC Operations on a 24/7/365 basis to enhance DHS OPS situational awareness, fusion and analysis and decision support to senior leaders.

4. TASKS

4.1 Media Monitoring

Media monitoring assists DHS frame the operational picture that open source media is reporting, uncover problem areas for incident management leadership to further evaluate, identify nascent or evolving situations and provide valuable information and imagery that can be used to corroborate and/or reconcile first reports. The Contractor shall monitor, collect, analyze, and distribute operationally relevant real-time open source information to homeland security issues 24/7/365.

The Contractor shall understand DHS Critical Information Requirements (CIR) and monitor open source news coverage for new incidents that relate to the CIRs (Items of Interest – IOI) and understand how a story may be related to other important ongoing events and DHS activities. The CIRs are as follows:

a. Potential threats and hazards to the homeland, DHS, other Federal agencies, state and local response units (i.e., first responders), facilities (e.g., dams, major bridges and buildings), and resources (e.g., water supply, H1N1 vaccine); Private sector; and Public safety (e.g., where the public is involved, football game);
b. Potential impact on DHS capability to accomplish the HSPD-5 mission;
c. Identify events with operational value (e.g., successful space shuttle landing) and/or corroborating critical information (i.e., subsequent reporting to the initial report);
d. Identifying media reports that reflect adversely on the U. S. Government, DHS (e.g., a coast guard ship collides with another or impacting DHS from accomplishing its mission) and the National planning scenarios.

4.1.1 The Contractor shall perform a broad open sources search for information on breaking news stories. The contractor shall:

4.1.1.1 Monitor major broadcast news networks
4.1.1.2 Monitor and review all Associated Press (AP) stories generated within the U.S. by each state's AP bureau
4.1.1.3 Monitor and receive alerts on other wire service stories via categorized/focused Really Simple Syndication (RSS) feeds.
4.1.1.4 Monitor and receive alerts on local and regional broadcast news via categorized/focused text/video feeds
4.1.1.5 Monitor appropriate Internet web sites on breaking situational events
4.1.1.6 Monitor and receive full motion video (FMV) or other streaming media

4.1.2 An Item of Interest (IOI) is determined by those events or activities that require DHS NOC steady state or update reporting, an event requiring the DHS NOC to prepare Phased reporting or the formation of a Crisis Action Team as directed by DHS leadership through the DHS NOC. In the event an incident has occurred and an (IOI) follow-on analysis is underway or research is ongoing on a National Security Situation/

International Security Situation (NSS/ISS), the contractor shall perform the following as determined by the DHS leadership:

4.1.2.1 Continue to monitor major broadcast news networks (cable service)

4.1.2.2 Query and search Associated Press (AP) stories for information specific to the incident

4.1.2.3 Query and search broadcast news via categorized/focused text/video feeds for information specific to the incident

4.1.2.4 Query and search RSS feeds for information specific to the incident

4.1.2.5 Query and search the Internet using other search engines such as Google and Yahoo

4.1.2.6 Monitor and receive full motion video (FMV) or other streaming media specific to the incident

4.1.2.7 Monitor and search web sites including those representing regional and local media outlets (TV stations, radio stations, and newspapers source)

4.1.2.8 Continue to monitor/review reports available via above open sources for information on other breaking news stories

4.1.3 The Contractor shall create NOC media monitoring reports, media summaries, daily media operational summaries and weekly data reports.

4.2 Social Media/Networking

The Contractor shall provide 24x7x365 Social Media/Networking (S/N) support to enhance DHS OPS situational awareness, fusion and analysis, and decision support to senior leaders. The Contractor shall:

4.2.1 Monitor, collect, analyze, and distribute operationally relevant S/N as part of the DHS National Operations Center (NOC).

4.2.2 Facilitate S/N support to provide:

4.2.2.1 Potential and emerging threats and hazards information for homeland security situational awareness, information sharing and decision support.

4.2.2.2 Evolving incidents, crisis management and other Homeland Security information available to the public to include public alerts and notifications both sent and received

4.2.2.3 Additional venues for the public to communicate critical information to the Department of Homeland Security that serve to corroborate or reconcile other reports or provide new information that has not come to the Department’s attention

4.3 OPTIONAL TASK: Surge Support

The Contractor shall provide additional Media Monitoring and Social Media/Networking support when operational conditions require staffing to support OPS during emergency operations and national level exercises. Surge support temporarily increases the staffing level of Tasks 4.1 and 4.2.

The Task Order (TO) Contracting Officer’s Technical Representative (COTR) will approve the time, place of performance and level of effort for surge support prior to execution.

4.4 Task Order Management

4.4.1 Project Management

The Contractor shall designate a single point of contact as the Project Manager (PM) with whom the TO Contracting Officer (CO), TO Contract Specialist (CS) and the TO COTR will communicate technical and administrative issues relating to this task order. The PM shall ensure that: (1) the goals and objectives of the project and (2) problem resolution and customer satisfaction are accomplished within prescribed time frames and funding parameters. Key duties include planning, organizing, directing and controlling the project to ensure all contractual obligations are fulfilled, quality standards are met and associated expectations of performance achieved. Other duties include developing schedules, reviewing work discrepancies, communicating policies and managing and controlling resources. THIS IS NOT A FULL-TIME POSITION.

4.4.1.1 Monthly Task Order Status Report

The Contractor shall create monthly status reports. The status reports shall contain a heading with the following information at a minimum:

4.4.1.1.1 Contractor Name, Project Manager’s Name and Telephone Number
4.4.1.1.2 Task Order Number and Task Order Period of Performance
4.4.1.1.3 Scope of Task Order
4.4.1.1.4 Period of Performance Being Reported
4.4.1.1.5 Submission Date

The Contractor shall assist DHS in compiling useful data on work performed under this task order. Each status report will contain the following items.

4.4.1.1.6 A brief, factual summary description of technical progress;

4.4.1.1.7 For each task, provide: a summary of work completed, work in progress and work planned; and for labor hour tasks include hours/dollars expended for the reporting period and cumulatively and hours/dollars remaining;

4.4.1.1.8 Updated Project Management Plan;

4.4.1.1.9 Identify significant problems and their impacts, causes, proposed corrective actions; and the effect that such corrective actions will have on the accomplishments of the task order objectives;

4.4.1.1.10 The Schedule status or the degree of completion of tasks/activities by time intervals;

4.4.1.1.11 Upcoming events; and

4.4.1.1.12 Status of Travel, if any;

4.4.2 Post Award Orientation Meeting

A Post Award Orientation meeting will be scheduled within ten (10) business days after task order award. The orientation aids both the Government and Contractor personnel to (1) achieve a clear and mutual understanding of all task order requirements and (2) identify and resolve potential problems. Attendees will be at a minimum: TO CO, TO CS, TO COTR and the Contractor's Program Manager.

The Post Award Orientation will take place at 301 7th Street, SW, Washington, D.C. The TO CO will establish the time of the orientation, prepare the meeting agenda and notify the appropriate Government and Contractor representatives of the meeting.

4.4.3 Task Order Kick-Off Meeting

The Task Order Kick-Off meeting will take place after the Post Award Orientation meeting. The purpose of this meeting is to introduce team members and present their roles and responsibilities, present an overview of the requirement based on the contents of the SOW and discuss any administrative matters.

The TO COTR will establish the time and place of the meeting and notify the appropriate Government and Contractor representatives. The meeting agenda will be prepared by the Government.

4.4.4 Transition Planning

An incumbent Contractor is currently performing the services outlined in the Statement of Work. The Contractor shall develop transition plans for startup and closeout activities.

4.4.4.1 Final Transition Startup Plan

The final Transition Startup Plan shall be a refined and finalized version of the Draft Transition Startup Plan submitted with the Technical Quote submission.

4.4.4.2 Transition Startup Activities

In the event that the tasks described in the SOW are transferred to a new contractor or to the Government, the new contractor and/or the Government shall participate in meetings with the incumbent contractor for an orderly and efficient transition. DHS anticipates a 30 to 60 calendar day transitional period during which the incumbent and new Contractor will be under contract.

4.4.4.2.1 The Contractor shall initiate and accept the transfer of relevant information and data from the incumbent Contractor.

4.4.4.2.2 The Contractor shall begin such coordination activities on the effective date of the task order.

4.4.4.2.3 Within 30 calendar days after favorable Entry on Duty (EOD) is granted, the Contractor shall be fully operational on all tasks.

4.4.5 OPTIONAL TASK: Transition Closeout Plan

The Contractor shall develop and submit a Draft Transition Closeout Plan sixty (60) calendar days prior to the conclusion of the task order for transferring responsibility of the tasks described in the SOW to a new Contractor or the Government. The plan shall inventory the tasks required to perform each task and identify a transition team lead. A Final Transition Closeout Plan shall be prepared and submitted fifteen (15) calendar days after receipt of Government's comments on the Draft Transition Closeout Plan.

4.4.6 OPTIONAL TASK: Transition Closeout Activities

In the event that the tasks described in the SOW are transferred to a new Contractor or to the Government, the Contractor shall participate in meetings with the new Contractor and/or the Government for an orderly and efficient transition. DHS anticipates a thirty (30) calendar day transitional period during which the Contractor and the new Contractor will be under contract. The Contractor shall prepare a Final Transition Out Plan Briefing that shows the final status of all deliverables and tasks.

5. DELIVERABLES AND DELIVERY SCHEDULE

All deliverables shall be prepared using Microsoft Office Suite module tools and delivered electronically to the NOC Senior Watch Officer Inbox. All deliverables are due by 5 PM local time (Washington, D.C.) unless otherwise stated in the Deliverable Table.

Note: The Contractor shall send a copy of the monthly status report (Task 4.4.1.1) to the TO CO, TO CS and TO COTR. Deliverables shall be free of any known computer virus or defects. If the Government finds a virus or defect is found, the deliverable will not be accepted. The replacement file shall be provided within two (2) business days after notification of the presence of a virus.

In the event the Contractor anticipates difficulty in complying with any deliverable, the Contractor shall provide written notification immediately to the TO CO, TO CS and TO COTR. Each notification shall give pertinent details, including the date by which the Contractor expects to make delivery; provided that this data shall be informational only in character and that receipt thereof shall not be construed as a waiver by the Government of any task order delivery schedule, or any rights or remedies provided by law under the GSA contract.

5.1 Review of Deliverables

The Government will provide written acceptance, comments and/or change requests, if any, within five (5) business days from receipt by the Government of the deliverable. Upon receipt of the Government comments, the Contractor shall have two (2) business days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form. Deliverables will be assessed on: amount of revision required by the Government, timeliness, adherence to specified formatting and content requirements and accuracy (errors on part of vendor, revealed after acceptance).

5.2 Deliverable Table

DELIVERABLE TABLE		
Task Number	**Deliverable Title**	**Due Date**
4.1	NOC Media Monitoring Report	Daily, as events occur (historical average is 15)
4.1	NOC Media Monitoring Operational Summary (roll up of NOC Media Monitoring Reports from the previous 24 hours)	Daily, NLT 0600

DELIVERABLE TABLE

Task Number	Deliverable Title	Due Date
4.1	Weekly Data Reports – A statistical report based upon the previous weeks reporting of Incidents of Interest. Other weekly summaries maybe required based upon other criteria as required by the NOC leadership	Monday for the prior week, or as required.
4.2	Social Network Summaries– A summary of an Item on Interest	Daily, as events occur
4.2	Daily Social Network Operational Summaries – Operational Summary (roll up of NOC Media Monitoring Reports from the previous 24 hours)	Daily, NLT 0600
4.2	Weekly Data Reports – A statistical report based upon the previous weeks reporting of Incidents of Interest. Other weekly summaries maybe required based upon other criteria as required by the NOC leadership	Monday for the prior week
4.4.1	Monthly Status Report	1st report - 5th business day after the end of the first 30 calendar days Subsequent reports – 5th business day after the end of the previous 30 calendar day period
4.4.4.1	Draft Transition Startup Plan	Submitted with the Technical Quote
4.4.4.1	Final Transition Startup Plan	15 calendar days after task order award
4.4.5	OPTIONAL TASK: Draft Transition Closeout Plan	Sixty (60) calendar days prior to the expiration of the Task Order

DELIVERABLE TABLE		
Task Number	**Deliverable Title**	**Due Date**
4.4.5	OPTIONAL TASK: Final Transition Closeout Plan	Fifteen (15) calendar days after receipt of Government's comments on the Draft Transition Closeout Plan
4.4.6	OPTIONAL TASK: Final Transition Out Plan Briefing	As directed by TO COTR

6. KEY PERSONNEL

The position that follows has been designated as Key Personnel.

6.1 Project Manager - THIS IS NOT A FULL-TIME POSITION

The Project Manager shall perform the duties associated with task 4.4.1. The minimum qualifications are:

6.1.1 Five (5) to seven (7) years of specific experience in managing large, complex projects in a task order/contract environment; experience performing the day-to-day management of overall contract/task order support operations involving multiple projects and groups of personnel; experience organizing, directing and coordinating the planning and production of contract/task order support activities; excellent written and oral communication skills; experience managing the client interface at the senior levels of the client organization. Has the ability to establish and alter, as necessary, technical approach to directly effect contract support activities.

6.1.2 A Bachelor's degree from an accredited institution of higher learning.

6.2 Substitution of Key Personnel

The Contractor shall notify the TO CO and TO COTR prior to making any changes in Key Personnel. All proposed substitutes shall have qualifications equal to or better than the qualifications of the person to be replaced. The TO CO and TO COTR must be notified in writing of any proposed substitutions at least thirty (30) days in advance of the proposed substitution. The notification shall include:

6.2.1 An explanation of the circumstances necessitating the substitution; and
6.2.2 A resume of the proposed substitute.

The TO CO and the TO COTR will evaluate substitutions and notify the Contractor of their approval or disapproval in writing.

6.3 Removal of Contractor Employees

The Contracting Officer may require dismissal from work of those contractor employees which he/she deems incompetent, careless, insubordinate, unsuitable or otherwise objectionable, or whose continued employment he/she deems contrary to the public interest or inconsistent with the best interest of national security. The contractor must fill out, and cause each of its employees on the contract work to fill out, for submission to the Government, such forms as may be necessary for security or other reasons.

7. GOVERNMENT-FURNISHED EQUIPMENT (GFE) AND GOVERNMETN FURNISHED INFORMATION (GFI)

There will be no GFE or GFI provided under this task order.

8. PLACE OF PERFORMANCE

The place of performance will be at the contractor's facility.

9. PERIOD OF PERFORMANCE

The period of performance shall be for a base period of seven (7) months with four (4) twelve (12) month option periods.

10. TRAVEL

Travel performed for personal convenience or daily travel to and from work at the Contractor's facility or local Government facility (i.e. designated work site) shall not be reimbursed. Travel will be reimbursed in accordance with the Federal Travel Regulations. Travel will not be reimbursed within a 50 mile radius of the designated worksite. The Contractor must get TO COTR approval prior to travel. All travel must comply with the Federal Travel Regulations. Unless approved in advanced by the TO CO, the Contractor's travel shall not exceed the maximum per diem rates established by the General Services Administration.

The Contractor shall coordinate specific travel arrangements with the TO COTR to obtain advance, written approval for the travel about to be conducted. The Contractor's request for travel shall be in writing and contain the dates, locations and estimated costs of the travel. If any travel arrangements cause additional costs to the task order that exceed those previously negotiated, written approval by Task Order modification issued by the TO CO is required prior to undertaking such travel.

The Contractor shall to the maximum practical extent, minimize overall travel costs by taking advantage of discounted airfare rates available through advance purchase and or existing Department transportation. Charges associated with itinerary changes and cancellations of nonrefundable airline tickets are reimbursable as long as the changes are approved by the TO CO.

11. TASK ORDER (TO) CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (COTR)

The TO COTR represents the TO CO by administration of technical details within the scope of the task order. The TO COTR performs functions under the task order such as review or inspection and acceptance of supplies, services and other functions of a technical nature. The TO COTR and Contractor may not make any representations or commitments on behalf of the TO CO or the Government. The Contractor may not construe TO COTR inquiries as direction to work outside of the scope of the statement of work. The TO COTR does not have authority to alter the Contractor's obligations or to change the task order specifications, price, terms or conditions. If, as a result of technical discussions, it is desirable to modify task order obligations or the specifications, changes will be issued in writing and signed by the TO CO. The Contractor may propose changes to existing task order by sending such request to the TO CO.

12. SECURITY REQUIREMENTS

This task order does not require a security clearance.

PAST PERFORMANCE QUESTIONNAIRE

Name of Proposed Contractor:

In Response to Solicitation Number: HSHQDC-10-Q-00005

Name of Rater: **Phone Number:**

Contract Type:

Place Of Performance:

Performance Period:

Description of Work:

Performance Grades:

Exceptional - The Contractor's performance exceeded all contract requirements. The contractual performance of the element or sub-element being assessed was accomplished with no problems.

Very Good – The Contractor's performance exceeded most contract requirements. The contractual performance of the element or sub-element being assessed was accomplished with problems for which corrective actions taken by the Contractor were effective.

Satisfactory – The Contractor's performance met contract requirements. The contractual performance of the element or sub-element being assessed was accomplished with problems for which corrective actions taken by the Contractor were adequate.

Marginal – The Contractor's performance did not meet some contract requirements. The contractual performance of the element or sub-element being assessed contains problems for which the Contractor's corrective actions were partially effective.

Unsatisfactory – The Contractor's performance did not meet contract requirements. The contractual performance of the element or sub-element being assessed contains problems(s) for which the Contractor's corrective actions were ineffective.

Return the completed questionnaire in response to solicitation number HSHQDC-10-Q-00005 to (b) (6) **at** (b) (6) **or fax number** (b) (6) **by the quote deadline.**

Please circle each of the areas below of the contractor's past performance based on the comments provided by the customer.

1. Customer Satisfaction Commitment: To what degree was the Contractor considered responsive to and cooperative with customer personnel?

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

2. Quality of Service: This area of the questionnaire deals with compliance of contract requirements, to include appropriateness of personnel and technical excellence.

2.a. Overall compliance with contract terms and conditions:

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

2.b. Effectiveness and reliability of Contractor's Key Personnel.

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

2.c. Adequacy of maintaining and controlling Government equipment.

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

Return the completed questionnaire in response to solicitation number HSHQDC-10-Q-00005 (b) (6) at (b) (6) or fax number (b) (6) by the quote deadline.

3. Timeliness of Performance: This is the area that deals with the contractor's ability to meet milestones and delivery schedule, to include responsiveness to technical direction, completion of efforts on time including wrap-up and contract administration.

3.a. Overall performance in planning, schedule, and monitoring.

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

3.b. Completion of major milestones on schedule:

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

3.c. Responsiveness to contract changes from a contract administration perspective.

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

3.d. Responsiveness to changes in technical direction.

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

3.e. Timely completion of efforts within period of performance.

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

Return the completed questionnaire in response to solicitation number HSHQDC-10-Q-00005 to (b) (6)
at (b) (6) **v or fax number (** (b) (6) **by the quote deadline.**

3.f. Responsiveness/capability to respond to urgent/short term requirements.

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

3.g. Efficiency in meeting cost targets without experiencing overruns.

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

3.h. Ability to control costs through use of evolving technology and Commercial Off-The-Shelf technology, and such efficiency are share with the Government,

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

3.i. Effectively assess impacts of changes on other associated projects, task and efforts.

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

3.j. Appropriately choose effective subcontractors and teaming partners and maintain good business relationships.

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

Return the completed questionnaire in response to solicitation number HSHQDC-10-Q-00005 to (b) (6)
at (b) (6) **v or fax number (** (b) (6) **by the quote deadline.**

3.k. Ability to solve contract performance problems without extensive guidance from Government personnel.

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

3.l. Effectiveness in interfacing with Government personnel.

Unsatisfactory Marginal Satisfactory Very Good Exceptional

Comments:

3.m. Has the Contractor ever been given a cure notice, a show cause notice, suspension of progress payments, or other letters directing the correction of a performance problem?

Yes_________ No___________

If yes, please explain:

3.n. Changes in contract dollars value throughout the life of the contract are/were attributable, for the most part, to ( ) Government-issued change orders; ( ) claims submitted by the Contractor, ( ) other Government actions, ( ) other contractor actions.

Please explain:

3.o. Based on this Contractor's overall performance, would you award this Contractor another Government contract?

Yes____________ No___________

If no, please explain:

Return the completed questionnaire in response to solicitation number HSHQDC-10-Q-00005 to (b) (6) at (b) (6) or fax number (b) (6) by the quote deadline.

AWARD DECISION MEMORANDUM

MEDIA MONITORING AND SOCIAL MEDIA/NETWORKING SUPPORT SERVICES FOR THE OFFICE OF OPERATIONS COORDINATION AND PLANNING'S NATIONAL OPERATIONS CENTER

RFQ HSHQDC-10-Q-00005

1. Decision Statement

As the Selection Official for this acquisition, I have determined that the solution proposed by General Dynamics Advanced Information Systems (GDAIS) provides the best overall value to satisfy the DHS Office of Operations Coordination and Planning's (OPS) needs. In making this determination, I considered the factors established in the solicitation and my integrated assessment and comparison of the strengths, weaknesses and risks of each of the quotes submitted in response to the Request for Quote (RFQ). As part of the decision making process, I reviewed the technical evaluation report and considered the recommendations made by the Contracting Officer. This memorandum documents the basis for my decision.

The table that follows summarizes the results of the technical evaluation conducted by the Technical Evaluation Team (TET):

	(b)(3), (b)(4)	(b)(3), (b)(4)	General Dynamics Advanced Information Systems (GDAIS)	(b)(3), (b)(4)
Minimum Requirement: Media Monitoring Demonstration	Pass	Pass	Pass	Fail
Evaluation Factors:				
Technical Approach	Good	Acceptable	Outstanding	Technical and Price quotes were not submitted
Management Approach	Good	Acceptable	Outstanding	
Personnel/Key Personnel	Good	Good	Outstanding	
Past Performance	Good	Good	Outstanding	
Overall Rating	**Good**	**Good**	**Outstanding**	
Total Price	(b)(3), (b)(4)	(b)(3), (b)(4)	**$11,319,234.64**	

2. Best Value Analysis

GDAIS submitted the highest rated quote; it received Outstanding ratings for technical approach, management approach, personnel/key personnel and past performance for an overall rating of Outstanding. (b)(3), (b)(4) oth received overall ratings of Good; (b)(3), (b)(4) received Good ratings for technical approach, management approach, personnel/key personnel and past performance while (b)(3), (b)(4) eceived Good ratings for personnel/key personnel and past performance and Acceptable ratings for technical approach and management approach.

The TET determined that (b)(3), (b)(4) proposed approach/solution, when implemented, is expected to result in superior achievement of the Government's objectives with minimal risk. GDAIS' ability to integrate news and social networking, exploit lesser known and emerging technologies and mitigate the risk of inaccuracies in addition to the existing knowledge and understanding of the NOC’s information requirements indicates that it will successfully perform the requirements. GDAIS specified how it intends to maintain 24/7/365 service during disruptions due to weather and other emergencies. This planning and foresight demonstrates that it fully understands the statement of work and the environment in which it will be working. It also demonstrates that GDAIS has the ability to provide superior performance to the Government regardless of disruptions to facilities or utilities. All proposed personnel, fiom the subcontractor, are currently working in the DHS Media Monitoring and Social Networking Center. Their experience and knowledge gained fiom working in the Center will provide the Government superior performance.

The TET determined that (b)(3), (b)(4) pproach/solution when implemented is expected to result in the full achievement of the Government's objectives with minimal risk. Its (b)(3), (b)(4) system and the (b)(3), (b)(4) system utilized by the firm on a similar project with DHS provide the Government confidence that it has the necessary technical ability to provide media monitoring services. Furthermore, (b)(3), (b)(4) understands the challenges of handling PII and the need to eliminate it from its products which is a further indication that it grasps the details of the SOW requirements. (b)(3), (b)(4) however, did not state the number of personnel that make up a team or how they would be rotated in an out which could be a risk if (b)(3), (b)(4) staffs teams with an inadequate number of personnel. Furthermore, none of (b)(3), (b)(4) proposed personnel have experience working with social networking sites or information which is critical to ensuring the correct assimilation and dissemination of appropriate information.

The TET determined that (b)(3), (b)(4) approach/solution when implemented is expected to meet the Government's objectives with minimal risk. (b)(3), (b)(4) demonstrated a lack of thorough understanding of the social networking requirement because it did not reference the challenges of personally identifiable information. Also, it did not address how its social networking process will interface with the media monitoring effort which shows a potential lack of understanding of the utility and employment of the information by the Government. Furthermore, none of (b)(3), (b)(4) proposed personnel have experience working with social networking sites or information which is critical to ensuring the correct assimilation and dissemination of appropriate information.

The TET has determined that GDAIS's quote will result in superior achievement of the Government's objectives as evidenced by the Outstanding ratings it received for each of the four technical evaluation factors. The GDAIS quote demonstrates an outstanding understanding of the statement of work requirements and demonstrates how the teams will be organized. Also, all proposed personnel have media monitoring and social networking experience. GDAIS' record of past performance in projects of similar size and scope indicates that the Government may expect superior performance and customer satisfaction. The TET determined that the other offeror's quotes would result in only full achievement of the Government's objectives or just meeting them.

(b)(3), (b)(4) proposes the lowest price in the amount of (b)(3), (b)(4) followed by (b)(3), (b)(4) with a price of (b)(3), (b)(4) and GDAIS proposes the highest price of $11,319,234.64. The price difference among the (b)(3), (b)(4) and GDAIS quotes is significant. GDAIS' proposed price is (b)(3), (b)(4) higher than the (b)(3), (b)(4) proposed prices. Since the level of effort was provided in the solicitation, a price comparison of the price quotes revealed that the difference appears to result from staffing approaches. GDAIS proposes the use of more experienced personnel to perform all of the statement of work (SOW) requirements which results in higher hourly rates. In contrast, (b)(3), (b)(4) proposes a mixture of lower level and junior level personnel to perform SOW requirements, with most of the tasks performed by lower level personnel. As a result, it proposes lower hourly rates. (b)(3), (b (b)(3), (b proposes a mixture of lower level and senior level personnel to perform the requirements, with most of the tasks performed by the lower level personnel. Like BAE, (b)(3), (b)(4) proposes lower hourly rates. GDAIS' proposed hourly rates and overall price are higher than (b)(3), (b)(4) rates and overall prices.

The RFQ stated that all non-price factors are equally important and when combined together they are significantly more important than the price factor. Although GDAIS submitted the highest price quote, the TET thinks it warrants a price premium of (b)(3), (b)(4) d (b)(3), (b)(4) over the (b)(3), (b)(4) quotes, respectively, due to the technical merit of the quote; the Government is expected to get superior achievement of its objectives based on its technical quote. The TET determined that the GDAIS quote represents the best value to the Government.

3. Best Value Summary

Quote selection was made in accordance with the guidelines provided in the Federal Acquisition Regulation, the Department of Homeland Security Acquisition Regulation for Best Value awards and the evaluation criteria specified in the RFQ. Accordingly, the evaluation was based on best value principles which recommend that award be made to the Offeror whose quote represents the best overall value to the Government, price and other factors considered.

After consideration of the information provided to me by the Contracting Officer and my independent assessment, it is my determination that GDAIS offers the best value quote for fulfilling the media monitoring and social media/networking support services requirement.

I found that GDAIS' quote warranted the payment of a price premium because based on the GDAIS quote the Government expects to get superior achievement of its objectives.

In my opinion, GDAIS' quote generated the best overall value to the Government. For these reasons, as the Selection Official, I have decided to award the task order to GDAIS at the price of $11,319,234.64 which includes all DHS OPS requirements including option periods.

(b) (6) ________________ 5/21/2010
Date

Acting Director, National Operations Center
Office of Operations Coordination and Planning
Selection Official

Determination and Findings

Per 5 U.S.C. 3109 as implemented by FAR 37.104, FAR 7.503, and the Department of Homeland Security (DHS) Management Action Directive: Workforce Assessment issued May 26, 2009, the DHS Office of Procurement Operations shall ensure that any awards for contracts or the exercise of options under existing contracts for professional services do not include inherently governmental or nearly inherently governmental requirements, personal service requirements, or requirements that impact core functions that must be performed by federal employees. The purpose of this Determination and Findings (D&F) is to grant authority to the DHS Office of Procurement Operations to Exercise an option with General Dynamics for Media Monitoring and Social Media/Networking Support Services to the Department of Homeland Security (DHS) Office of Coordination and Planning.

Findings

1. Agency: DHS
   Contracting Activity: Office of Procurement Operations
   Program Office: Office of Coordination and Planning.
   Proposed Contractor: General Dynamics Advanced Information Systems, 12450 Fair Lakes Circle, Suite 800, Fairfax, Virginia 22033.

2. Description of Proposed Services: The Department of Homeland Security is responsible for monitoring the security of the United States on a daily basis the National Operations Center (NOC), Ops provides real-time situational awareness and monitoring of the homeland, coordinates incidents and response activities, and, in conjunction with the Office of Intelligence and Analysis, issues advisories and bulletins concerning threats to the homeland security, as well as specific protective measures. The NOC operates 24 hours a day, seven days, seven days a week, 365 days a year (24/7/365), coordinates information sharing to help deter, detect, and prevent terrorist acts and to manage domestic incidents.

   DHS Task Order No: HSHQDC-10-F-00080; Exercise Option Period One (1) of the Task Order.
   Estimated Annual Value: $2,350,956.80
   Estimated Total Contract Value: $11,319,234.64
   Advance Acquisition Plan (AAP) No: 68786

3. The proposed professional services **are not** inherently governmental or nearly inherently governmental professional services as described in FAR 7.503.

4. The proposed professional services **are not** for personal services as described in FAR 37.104. In accordance with FAR 37.104(c) (2), the Office of Coordination and Planning Division will not exercise relatively continuous supervision and control over the contractor personnel performing the contracts.

5. The proposed professional services **are not** for the services of individual experts or consultants as provided in FAR 37.104(f) (see limitations of the Classification Act).

6. The proposed professional services **will not** impact the Office of Coordination and Planning Division's core functions that must be performed by federal employees in accordance with DHS Management Action Directive: Workforce Assessment issued May 26, 2009.

7. Within the Office of Coordination and Planning the National Operations Center Division's ratio of all Federal employees to all contractor employees, including those under this action, is three (3) Federal employees to one (1) contractor employees.

8. Within the Office of Coordination and Planning the National Operations Center (NOC), the estimated number of Federal employee(s) providing oversight to the service contractor is One federal employee is assigned to oversee the contractor on a part-time basis. The information regarding 1) the number of full-time/part-time Federal employee(s) working to oversee the contractor; and 2) whether the Federal employee(s) assigned to oversee the service contractor will work at the contractor's worksite is listed in the table below:

Contract Number/TO Number	Performance Location (if FTE will work at Contractor worksite)	Number of Federal Employee(s)	Full-Time or Part-Time Oversight
GS-10F-0237L/HSHQDC-10-F-00080	No	1	Part-Time
Fill in TOTALS:		1	#FT: _____ #PT: __1___

9. Program Office Contracting Officer Technical Representative (COTR) Information: Proposed COTR Official: (b) (6), COTR Certification and Training: (b) (6) certified as of 10/1/2009 and current with required training COTR responsibilities: The COTR has been delegated the authority to monitor delivery and performance under the business agreement, as the Contracting Officer's Technical Representative. This is an ancillary duty for the COTR whose primary responsibility is a program manager. In addition to the proposed contract, the COTR currently manages two (2) other contracts. Although the COTR's responsibilities are ancillary, the COTR has sufficient time and resources to adequately manage and oversee this contract. The contract vehicles currently administered by the COTR are listed in the table below:

Contract Number	Task Order Number	Contractor Name	Dollar Value
HSHQDC-09-F-00207		General Dynamics	$4,946,146.73
HSHQDC-10-C-00072		Alutiiq, LLC	$5,811,964.23

10. The services that the contractor will perform for DHS will relate to the mission of Office of Operations Coordination, through the national Operations (NOC), the OPS provides real-time situational awareness and monitoring on the homeland, coordinates incidents and response activities, and, in conjunction with the Office of Intelligence and Analysis, issues advisories and bulletins concerning threats to the homeland security, as well as specific protective measures. The NOC, which operates 24 hours day, seven days a week, 365 days a year (24/7/365), coordinates information sharing to help deter, detect, and prevent terrorist acts and to manage domestic incidents.

11. The Federal employee(s) support the mission of DHS Office of Operations Coordination and Planning, through the National Operations Center (NOC). Monitor day-to-day activity of the contractor and their performance through receiving all deliverables and working directly with project key personnel.

Determination

Based on the above findings, under the authority of FAR 7.503(e), and in accordance with the Department of Homeland Security Acquisition Manual (HSAM), Subchapter 3007.5, Inherently Governmental Functions, I have determined that the acquisition of the proposed professional services do not include inherently governmental or nearly inherently governmental requirements, personal service requirements, or requirements that impact core functions that must be performed by federal employees. Further, the number of Federal employees within the Office of Operations and Coordination, National Operations Center Division is sufficient to provide adequate direction and oversight to the professional service contractor employees.

(b) (6)

15 Dec 2010
Date:

Director, IMMAC

(b) (6)
Contracting Officer

Date:

APPROVAL:
(For actions with an annual value greater than $1 million but not exceeding $50 million)

____________________________________ ________________________
(b) (6) Date
Executive Director, Office of Procurement Operations
Head of Contracting Activity

Social Networking/Media Capability Analyst Handbook

February 2010

Social Networking/Media Capability Analyst Handbook February 2010

Table of Contents

SNMC Products - Version 2.2, 2010

(New Format Templates listed in subsequent pages)

TIP Page 2

Tip to MMC (TIP)

This is the TIP format used to send a media link to the MMC via email. TIPs are also given verbally.

GAR Page 3

Guardian Advisory Report (GAR)

The GAR format is a format meant to be written and sent to alert the NOC of a breaking event or incident. Should be written and sent ASAP, composed of a bulleted summary and the general source of the information (eg. Twitter, Blog).

GIR Page 4

Guardian Information Report (GIR)

The GIR format is similar to our previous IOI format. The GIR will include analysis and sources. A break line will provide a visual marker separating the summary and important information from the sources, links, etc.

GSR Page 6

Guardian Special Report (GSR) - senior reviewed, timed

Special Reports are reports or summaries of varied length that are either requested by the NOC or senior TSI staff, or are "topics of interest" that the SNMC has identified as emerging trends. Examples: Haiti and Winter Olympics GSRs.

G24 Page 7

Guardian 24-Hour Summary (G24) - internal, report on shift by analysts

The G24 is a daily report that provides a digest of the SNMC's past 24 hours of activity. Each NOC priority will be listed along with summarized information from any TIP, GIR, or GAR that has been produced. Items not pertaining to a NOC priority will also be listed. This document will be prepared by 0400 each morning.

W Page 10

SNMC Weekly Report (TSI Only)

The SNMC will provide a weekly internal report providing basic metrics, performance analysis, and optional case studies highlighting events/incidents that illustrate the value of the SNMC to the NOC.

M Page 14

SNMC Monthly Report (TSI Only)

The SNMC will provide a monthly internal report providing basic metrics, performance analysis, and optional case studies highlighting events/incidents that illustrate the value of the SNMC to the NOC.

TIP Example

DISTRIBUTION LIST
FROM: NOC Media Monitoring
TO: (b) (6)

Email Subject: Title of Media Article/Story - City, State(country if needed, and never redundant location info)--NOC MMC-TIP #000-MM/YY

-Title: Title of Article

-Source Name
http:// media link goes here

--
Name
Operations Analyst
DHS NOC Media Monitoring
(b) (6)

Guardian Advisory Report Example

DISTRIBUTION LIST
FROM: NOC Media Monitoring
BCC: [IOI distro list: see your Outlook e-mail from (b)(6), (b)(7)(C)

Email Subject: Concise, Capitalized and Not Dramatic - City, State--NOC MMC-GAR #000-MM/YY (country if needed, and never redundant location info)

[Alternative for Steady States, GAR reflects the original GAR being updated:]
Email Subject: (Steady-State Update - NOC Title for SS) Concise, Capitalized and Not Dramatic - City, State--NOC MMC-GAR #000-MM/YY (country if needed, and never redundant location info)

[Alternative for follow-ups; GAR # reflects the original GAR being updated:]
Email Subject: (FOLLOW-UP #1) Concise, Capitalized and Not Dramatic - City, State--NOC MMC-GAR #000-MM/YY (country if needed, and never redundant location info)

DHS NOC Social Networking/Media Capability
Guardian Advisory Report (GAR)

Location: [very descriptive location]

NOC CIR #3: Identifying events with operational value...corroborating critical information.

Summary:

- According to multiple Twitter postings, Aeromexico plane flight 576 that left from Cancun, Mexico has been hijacked but safely landed in Mexico City
- Three armed men were responsible for the hijacking

Additional Information: (Entirely optional, based on necessity)

Important blog or SN comment that gives granularity, photo or video with description, or sentiment analysis

--------------------------------BREAK LINE------------------------------------
Sources (some page content may change or be updated over time):

-Twitter
--"[quote]" -00 Jan 10, 23:59

-Blog
--"[quote]" -00 Jan 10, 23:59 [url]

--
Name
Operations Analyst

Guardian Information Report Example

DISTRIBUTION LIST
FROM: NOC Media Monitoring
BCC: [IOI distro list: see your Outlook e-mail from (b)(6), (b)(7)(C)

Example Email Subject: Concise, Capitalized and Not Dramatic - City, State(country if needed, and never redundant location info)--NOC MMC-GIR #000-MM/YY

[Alternative for Steady States; GIR # reflects the original GIR being updated:]
Email Subject: (Steady-State Update - NOC Title for SS) Concise, Capitalized and Not Dramatic - City, State--NOC MMC-GIR #000-MM/YY (country if needed, and never redundant location info)

[Alternative for follow-ups; GIR # reflects the original GIR being updated:]
Email Subject: (FOLLOW-UP #1) Concise, Capitalized and Not Dramatic - City, State--NOC MMC-GIR #000-MM/YY (country if needed, and never redundant location info)

DHS NOC Social Networking/Media Capability
Guardian Information Report (GIR)

Location: [very descriptive location]

NOC CIR #3: Identifying events with operational value...corroborating critical information.

Summary:

- Both official and unofficial alerts were posted to Twitter in an effort to update the public about a H1N1 vaccine clinic held at Fairfax, Virginia Government Center
- Alerts included how long the clinic would be open and how long someone would need to wait in line to get the vaccine
- The line at its peak took about 90 minutes
- Updates were also sent out by CapitalAlert.gov; an official web site, Twitter account and ability to send cell phone text messages, was created by a partnership of 17 local governments in the National Capital Region
- Neighboring Arlington County also helped spread the information through their official alerts on the County's web site and Twitter
- Public comments on Twitter about the clinic were generally positive, one first time expecting mother, said "Fairfax County, VA did a great job organizing and executing it". There were some complaints about the long lines

Additional Information: (Entirely optional, based on necessity)
Important blog or SN comment that gives granularity, photo or video with description, or sentiment analysis

Happy sunrise at the fairfax flu clinic, with line stretching around ginormous county bldg

------------------------------------BREAK LINE------------------------------------

Sources (some page content may change or be updated over time):

-Blog

-- "Quoted pertinent material from Blog." -00 Jan 10, 23:59

-Twitter

-- Scores Reported Dead in China After Riots. State media reporting that 156 people have been killed. Yikes. http://su.pr/34N2UY [Wall Street Journal] - Mon 6 Jul 13:53

-- See the example above. Note the source link and the full business name of the media source (if the tweet has one), then the date and time -00 Jan 10, 23:59

-Photos

-- Brief Description of photo and attach it to the email. Check that attachments are correctly labeled and are attached to email, eg. (IOI/TIP#002-06-09-Photo1.jpg) -00 Jan 10, 23:59

-YouTube

-- Brief Description of video, screen capture the video if possible, containing no PII. Link to video if no PII is revealed. -00 Jan 10, 23:59

--
Name
Operations Analyst
DHS NOC Media Monitoring

(b) (6)

Guardian Special Report Example
Month DD, YYYY

DHS NOC Social Networking/Media Capability
Guardian Special Report (GSR)

[Title]

[Executive Summary]

[Body]

Works Cited

[Sources]

--
NAME
Operations Analyst
DHS NOC Social Media Monitoring
Phone (b) (6)
Cell:

Guardian 24 Hour Summary Example

DISTRIBUTION LIST
FROM: NOC Media Monitoring
TO: (b) (6),
(b) (6)
CC: (b) (6)

Example Email Subject: G24 Summary Report--NOC MMC--DD Month YYYY
December 10, 2009

DHS NOC Media Monitoring
Social Networking/Media Guardian 24 Hour Summary (G24)

This NOC Social Networking/Media Capability Operational Summary provides the most recent social network and social media coverage for NOC Priorities and Monitoring Report requirements.

NOC Priorities and Events of Interest:

1. NOC Priority 1657-09: Disruptions to 2009 Holiday Season - Public Events
NTR

2. Steady State NOC 0655-09: 2009 H1N1 Flu

Cluster of Cases Indicate H1N1 and H5N1 Are Co-Circulating in Vietnam (GIR #071)

- Health research blog, Recombinomics, is reporting that the Director of the Institute of Hygiene and Epidemiology has privately confirmed that deaths in Dien Bien, Vietnam were caused by the H5N1 bird flu
- Translated from Vietnamese sources, the blog reports that a separate family living in the same area has tested positive for both H5N1 and H1N1. Poultry belonging to the family has also tested positive for H5N1
- These findings indicate that Vietnam represents a "hot zone" where H1N1 and H5N1 are co-circulating
- Additionally, the findings linked to poultry suggest that Vietnam is an environment for co-infections in a wide range of hosts, including humans and several species of mammals

GOOD

3. NOC 0003-09: US / Mexico Border Violence

Mexican Authorities Kill Kidnappers During Hostage Rescue –Cuencame, Mexico (GIR #069)

- Ten People were killed and three injured during a raid between police, army and "20 gunmen". Two reports says some of the kidnappers escaped in pick-up trucks
- Some reports say six alleged kidnap victims were rescued Tuesday. One source was not sure the number of victims that were rescued
- One source that said police acting on a phone tip went to a house and that only the kidnappers were killed. Another source said, the raid was on a 10-vehicle convoy, but that could be part of another story that happened in Michoacan. The article went on to say that those killed in the raid were "civilians" travelling in a 10-vehicle convoy that included the kidnap victims
- The incident turned into a four-hour standoff before the six victims were secured
- Police and several army officers were injured in the shootout. Durgango state attorney said that a helicopter carrying an investigator and his body guard were shot at

Cut everything beyond the basic "need to know" info. Highlighted lines are the ones I would cut.

State Department Considering Text-Messaging Service for Public to Report Mexican Violence (GIR #072)

- Online technology journal, Nextgov, is reporting that Secretary of State Hillary Clinton is considering the development of a text-messaging service that would enable Mexicans to anonymously report incidents of drug-related violence
- In October 2009 a team of U.S. technologists, including the chairman of Twitter, flew to Mexico City to discuss funding for a free text-messaging system
- The message service would be designed to strip witnesses' text messages of personally identifiable information and transmit them to a central office for response. Descriptions and locations of the incidents would be geographically displayed to a public website
- After receiving the reports, police would be held accountable for responding within a certain timeframe, follow-up information will be required to be posted to the website
- The motivation behind the text-message plan is to increase accountability for violent acts, and to promote transparency in law enforcement

Cut

Zetas Evolving Into a Business Oriented and Strategic Organization (GIR #073)

- An investigative journalist, who specializes in Latin America and the drug trade, is reporting that Mexican drug cartel the Zetas are constantly evolving
- The organization began as a group of elite bodyguards and has become an elite criminal organization that is moving away from the black market and into more "gray" or "white" market activities
- Two men now control the Zetas:
    - Heriberto Lazcano: the main leader, who has a business oriented and long-term strategy for the gang
    - Miguel Triveno: a traditional Mexican drug lord
- The Zetas were initially engaged in black market activity: drug and human trafficking, kidnapping, and extortion. The author believes that the Zetas are moving into the "gray market of protection;" working as specialized security guards and mercenaries for criminals and even well positioned business men who need protection from criminals, the police, and rivals
- The Dallas Morning News recently reported that the Zetas were engaging in "the white, or legal, side of business in Mexico and abroad." The author asserts that this report is accurate, and that the Zetas were even attempting to gain political influence in a number of regions
- The Zetas now use a strategy titled, "La Compania," which differentiates between less violent activities and more traditional criminal acts. The author predicts that the Zetas will only continue to evolve, and will therefore become more menacing to security and safety since they will be operating and a joint criminal and legitimate operation

All pretty strong points, but would be good to try to edit it down somehow

4. NOC 0998-09: Guantanamo Bay Detainee Transfers
NTR

Recent Guardian Advisory Reports distributed by the SNMC:
Wisconsin Governor Orders State of Emergency, Closure of Government Offices & Schools for Blizzard (GAR #032)

- Governor Jim Doyle of Wisconsin declared a state of emergency for the entire state on Wednesday morning because of a blizzard
- Governor Doyle also ordered the closure of all state government and University of Wisconsin campuses for public business

- The National Weather Service issued a blizzard warning until midnight on Wednesday night

Reports of Explosion, Smoke, Possibly from Refinery - Pasadena, TX (GAR #033)
This should be an update, as opposed to a regurgitation of the GAR that was sent out. Bullets should be more like:

- Twitter users reported a loud explosion at a chemical refinery in Pasadena, TX
- All employees of surrounding facilities are accounted for and no injuries have been reported

- Twitter users are reporting a loud explosion in the area of Pasadena, TX, near La Porte, Red Bluff, and Seabrook
- They are also saying there's a lot of smoke
- It is likely to be an explosion at an oil refinery
- This site is near the Lyndon B. Johnson Space Center
- There is no word on injuries or damage yet

I would cut any previous summary info that is speculative or incomplete, like the above 5 points.

Good pic

National Guard Assisting Police in Rescuing Stranded Iowa Drivers from Blizzard (GAR #034)

- "Hundreds" of motorists were stranded overnight Tuesday and Wednesday morning in Iowa after intense snowfall
- The National Guard is sharing HMMWVs with police in Iowa because 4wheel drive vehicles are having difficulty in the deep Iowa snow of up to 17 inches of snow with 50 mph wind gusts
- Plowing of roads has ceased because of these conditions
- The National Weather Service issued a blizzard warning until 6PM
- 1 driver has died as a result of veering off US 75 into an oncoming semi

All pretty pertinent

5 Missing Muslim Students Possibly Detained in Pakistan - Washington, DC (GIR #067)

- 5 Muslim students from the DC area being searched for by the FBI have turned up detained at a safe house in Pakistan
- A house in Sargodha, Pakistan was raided by an anti-organized crime team, the house being owned by Khalid Farooqi, an activist of banned group Jaish-e-Muhammad
- 5 foreigners were detained and their names match the students missing from the DC area:

(b) (6)

- A group made on Facebook by friends trying to find them has yet to receive many comments after the news of their arrests has hit

Probably unneeded info as far as the NOC is concerned

Student Stabbed Suffering Minor Injuries; School On Lockdown– Toledo, OH (GAR #035)

- A student was stabbed at Maumee High School in Toledo, Ohio
- The student suffered minor injuries, but the school is now in lockdown
- The suspect ran from the scene, but officials have not determined if the suspect is still in the school

Was the lockdown lifted? Current status?

Evacuation Terminal 2 San Diego Airport – CA (GAR #036)

- Two people have reported on Twitter that an alarm and evacuation has occurred at San Diego Airport
- People were asked to leave the building, but no one is sure what is happening

Post Event Summary: No follow-up information has been posted on this incident by either the media or social network users.

Cut this one entirely. We do not need to include bomb threats/evacs/ lockdowns that do not develop into something bigger.

Possible Explosion Near MARTA Station Downtown Atlanta- GA (GAR #037)

- The public is posting messages to Twitter that the police, fire trucks and bomb squad have responded to a possible bomb threat
- Two different individuals are reporting that a loud explosion was heard downtown near the MARTA station
- One person just posted that he received an email from building management that police are responding to a suspicious package
- Metropolitan Atlanta Rapid Transit Authority (MARTA)
- "MARTA police have determined a black canvas bag found at the Arts Center train station was not dangerous"
- Twitter messages said that reports are the police had detonated the suspicious package and that was the cause of the explosion heard

Cut all.

This summary should be edited to present the most updated info earlier and more concise like this:

- Twitter users reported that police, fire and bomb squad responded to a suspicious package in the Arts Center station of Atlanta's MARTA subway system
- The bomb squad detonated the suspicious package and determined that the package was not dangerous

Photos:

Photo 1 – "Bomb squad at the MARTA station"

Subway Service Halted Due to Downed Wires-San Francisco, CA (GAR #039)

- Reports indicate that there is a subway power outage in San Francisco
- All service on the Municipal Railway (Muni) has been stopped between Embarcadero and Castro Stations and will resume on Thursday morning
- Authorities report that overhead wires have fallen crews will be on the scene for the next several hours to fix the problem

Edit down to:

- A subway power outage in San Francisco stopped service between the Embarcadero and Castro stations on Wednesday
- Overhead wires had fallen, and crews had to stop trains to clear them
- Service is to be restored by Thursday morning

Recent Guardian Information Reports distributed by the SNMC: (Subject Lines)

- FBI Investigating 5 Missing Muslim Students - Washington, DC (GIR #067)
- (FOLLOW-UP #1) 5 Missing Muslim Students Possibly Detained in Pakistan - Washington, DC (GIR #067)
- US to Resume Hunt for Bin Laden (GIR #068)
- 19,000 Matches To Terrorist Screening Lists In 2009 (GIR #068)
- TSA Utilizes Blog to Reassure Public About Safety After Discovery of Leaked Security Document (GIR #070)

TIPS to Media Monitoring Center (Media tips could be the same topic as SNMC reports):

- Sessions Urges Holder to Suspend Gitmo Detainee Transfers to Saudi Arabia – Washington, DC (TIP #065)
- Blizzard Paralyzes Much Of Midwest; 15,000 Without Power In Wisconsin (TIP #066)
- Level One hazmat at Ontario Business Park-Wayne County, NY (TIP #067)
- Wires Down at Muni Stations; Service Disrupted-San Francisco, CA (TIP #068)

--

NAME
Operations Analyst
DHS NOC Media monitoring
(b) (6)

Weekly Report Example

Social Networking/Media Capability (SNMC) Weekly Report: August 17-August 23, 2009

This weekly report examines events of interest that were reported by the SNMC. At this point in our developmental work, we are searching for information to support the Media Monitoring Center (MMC) and developing our own reporting niche for Items of Interest (IOIs). Absolutely no Personally Identifiable Information (PII) is being used or stored during this operation.

Statistics on IOI and TIP Production

Number of SNMC IOIs produced: 130
Number of TIPS produced: 18
Number of TIPS that led to MMC IOIs: 4

Performance Analysis

A brief analysis of selected reports from the OPS/NOC Social Networking/Media Capability (SNMC) highlights the value of compressing the timeline from incident to informing the OPS/NOC, while providing granularity and situational awareness. In this report, we provide an Event Case Study on a tornado that touched down in Minneapolis, Minnesota. This selection of reports exhibits the SNMC's ability to provide in-depth visual information via photographs generated by social networking users. Additionally, we analyze three selected event reports that demonstrate the capacity for social networking media to provide enhanced granularity, report on aberrations detected by local populations, and capture public reaction to major governmental proposals with homeland security implications.

SNMC Case Study Event: Tornado Touches Down in Downtown Minneapolis, MN

Analysis of Case Study Event - SN tools can provide enhanced granularity through user generated photographs.

- In two reports on the event, SNMC included nine photographs from social networking users. The photographs provided significant first-hand visual details on the tornado and the damages that it caused
- The photographs captured the following items:
  - Traffic stopped after debris strewn across I-35 West (three photographs).
  - Uprooted tree resting on car.
  - Uprooted tree resting on house.
  - People taking cover in tornado shelter.
  - Damage to front of downtown church.
  - Damage to back of downtown church, including outdoor event area.
  - Flooding in residential street.
  - Funnel cloud over I-35.
- Three of these photographs are included below.

SNMC Selected Event Reports - ***Providing Enhanced Granularity, Capturing Public Reaction, and Reporting Aberrations Detected by Local Populations***

Propane Tank Explosion Closes I-15 in Both Directions-San Diego, CA–SNMC IOI #151-152 – 20 August 2009

- In two reports on the event, SNMC included three photographs from social networking users and one photograph from a television news helicopter. The photographs provided enhanced granularity that illustrated the aftermath of the explosion.
- The photographs captured the following items:
    - Smoke plumes rising just off of I-15 (Three photographs).
    - A shot of the fire itself.
- One of these photographs is included below.

Residents Voice Opposition Over Possible Plan To Bring Guantanamo Detainees To Local Prison-Standish, MI-SNMC IOI #153 - 21 August 2009

- SNMC employed multiple SN tools to capture the reaction of residents to a possible plan to bring Guantanamo detainees to a local prison in Standish, MI. SNMC utilized Facebook, Twitter, three different blogs, and reader comments on a mainstream media source.
- On the whole, residents were opposed to the plan. The SNMC report highlighted public sentiments in extensive detail. Two examples are included below.
  - Facebook: "Obama wants to move GITMO POWs to a Standish, MI prison... #1 - Standish, MI is 2 hours from the nation's largest Arab community. Think about it! #2 - This will make Standish and the rest of Michigan a target for terrorist attacks. #3 - WHY NOT JUST LEAVE THEM ... IN GITMO??!?"
  - 9/11 Families for a Safe & Strong America [Blog]: "Nearly every speaker during the two-hour gathering denounced the idea, many arguing that the 229 detainees should remain where they are, despite Obama's pledge to close the Guantanamo complex by 2010. "They are enemy combatants," said the chief steward for the union representing prison workers at Standish Maximum Correctional Facility. "They want to kill you, they want to kill me, they want to kill our families.""
- SNMC also captured a minority perspective: several users characterized the concerns of the community becoming a target of terrorists with the detainees at the prison as based in "hysteria" and "fear-saturated" beliefs. Two examples are included below.
  - Facebook: "[Name] who runs a Standish car dealership, said he could accept the Guantanamo detainees if adequate provisions were made for public safety. He said foes' dire warnings reminded him of the "hysteria" that arose before the state prison was opened two decades ago. "It turned out to be a good neighbor.""
  - Washington Post User Comment: "What is there to worry about? These guys weren't in Guantanamo because they were supermen who could leap over tall buildings or walls, they were there to keep them in a legal limbo. I guess rural America just wants to take welfare payments, but not the slightest risk."

Unidentified Foul Odor Reported in San Francisco, CA Neighborhoods-SNMC IOI #172 - 21 August 2009

- In this report, SNMC demonstrated that it can quickly report instances when local populations detect aberrations with potential homeland security implications.
- SNMC reported 13 Twitter posts focused on an unidentified foul odor in several San Francisco, CA neighborhoods. Three examples are included below.
  - "We can smell the odor here in North Beach too! Haven't been able to figure it out yet, but we're still getting new reports of the smell"
  - "What's that smell? SFFD checking out reports of a foul odor in several neighborhoods, mostly Richmond and Sunset."
  - "Getting calls from the west side of SF from people who say there is a foul smell in the area, like really foul. Anyone out there smell it?"
- Subsequent media reports indicate that the source of the smell was never determined; it did not appear to cause any serious damage.
- Nevertheless, this report illustrates SNMC's capability for rapidly reporting human-detected aberrations. This could be invaluable for detecting the first signs of a natural disaster, terrorist attack, and other events of importance to DHS.

Monthly Report Example

Social Networking/Media Capability (SNMC)
August 2009 - Monthly Status Report

The SNMC continues to work with DHS Office of General Council, Privacy Office, Civil Rights and Civil Liberties Office and Public Policy Office to work through privacy issues in relation to SNMC Privacy Impact Assessment (PIA) and CONOPs. The SNMC team continues its 24-hour internal Watch operation. Currently, the SNMC creates two products: "Tips" on potential Items of Interest (IOI) that support the MMC and SNMC IOIs meant to demonstrate the operational value of social networks in providing breaking news, granularity, and popular perspective. The team is using the internal watch as a way to refine the Watch process to be ready to send valuable IOIs directly to the NOC once a completed PIA is approved at DHS. The decision to create unique SNMC IOIs was executed in an effort to separate the functions of the SNMC from the MMC and to aid in the evolution of SNMC products. The SNMC team is composed of six analysts including two senior managing analysts, working three 8-hour shifts during the week and two 12-hour shifts on the weekends. The SN team has continued to evolve the social networking tools and processes and is now working on developing requirements for Phase II tasks that include social networking widgets that the public can interact with the information. **<u>NO SNMC REPORTING or STORING of DATA IS UNDERWAY PENDING COORDINATION BY LEGAL, PRIVACY and CIVIL RIGHTS CIVIL LIBERTIES OFFICES and APPROVAL by DHS OPS LEADERSHIP.</u>**

- August 1-31: All six analysts, including senior managing analysts cover 24-hour shift schedule for SNMC Watch
- August 1-31: Project time spent on continued refinement of PIA, CONOPs, SOP, Implementation Plan, Battle Rhythm, Watch related process, tools and procedures
- August 1-31: Project time spent on the creation of weekly reports and weekly reviews of operational value
- August 1-31: SNMC Watch produced 328 "Tips" to the MMC
- August 1-31: Of all the "Tips" to the MMC, 161 resulted in IOIs or Steady-State Updates for the MMC
- August 1-31: SNMC Analyst (b)(6), (b)(7)(C) continued development of a real-time H1N1 monitoring dashboard including some custom programming using the Twitter API
- August 3: Installation of Audio/Video Wall in the Watch Office was completed, including a full software/hardware switching system and four 40" LCD monitors mounted on a brushed aluminum rack
- August 5-13: All MMC and SNMC analysts were provided training notes on the use of the new Audio/Video Wall, and instructed to become proficient in changing video signals and channels and using the audio system
- August 6: A dedicated electrical circuit was installed to properly accommodate the portable AC unit that runs during nights and weekends in the Watch Office

- August 13: SNMC Watch produced its first SNMC IOI

- August 13- 31: SNMC Watch produced 357 SNMC IOIs

- August 13: Senior SNMC Analysts participated in a teleconference with Senior Staff to discuss planning for the upcoming H1N1 Flu season and how social networks/media could be used to better inform DHS in real-time during an outbreak

- August 13: SNMC decided to reorient its efforts in order to separate its functions from the MMC. The SNMC implemented a quota of one SNMC IOI an hour to develop and refine the value of the SNMC

- August 14: Wall placards were hung in the Watch room to reflect visually operational procedures for analysts and in preparation for S1 and other DHS visitors

- August 18: Senior SNMC Analysts met with Senior Staff to discuss planning for the upcoming H1N1 Flu season and how social networks/media could be used to better inform DHS in real-time during an outbreak

- August 18: Senior SNMC Analysts sent out three guiding directives for how to differentiate the SNMC from the MMC. The SNMC decided to focus on three principles: early detection, granularity, and popular perspective. Analysts were encouraged to think outside of the box in order to create products that are valuable from the social networking perspective. In addition to IOIs, analysts are also meant to look for topics that are appropriate for one to two page themed reports called SN Advisories

- August 20: All SNMC analysts began use of the (b) (7)(E) Messenger system while on watch and on project time in the office

- August 21: The SN team met to discuss new directives and the future of SNMC's functions. Analysts are continuing to brainstorm new products that will be valuable to Homeland Security

- August 21: Members of the SN team participated in Department of Homeland Security's New Hire Orientation program

- August 26-27: (b) (6) participated in the Gov 2.0 Leadership, Collaboration, and Public Engagement Symposium at the Ronald Reagan Building

Operational Implementation Outline
Social Networking/Media Capability (SNMC)

1. SNMC Overview and Characteristics

- Key member of the DHS SN Working Group
- 24/7/365 SNMC Watch Desk:
    - One analyst, utilizing an 8 hour weekday and 12 hour weekend shift combination
    - 7 days a week:
        - Weekdays: 0600 to 1400 morning; 1400 to 2200 swing; 2200 to 0600 night
        - Weekends: 0600 to 1800 and 1800 to 0600
- SNMC Project Time:
    - Two staff members, regular hours - Monday through Friday (0800 to 1700)
- Overseen by two senior social media/networking experts

1.1 Operations Timeline

<u>January 2010 to March 2010</u>

- Active 24/7 Watch for Haiti recovery and 2010 Winter Olympic events as defined by their respective PIAs
- On-call support to Media Monitoring and NOC
- Continued development of CONOPs, working with DHS Privacy Office, OPS Legal and other departments
- Continued research and mock 24/7/365 Watch with limited research distribution to Senior Management
- Research and development of tools, software and processes

1.2 Implementation Assumptions

1.2.1 Operational

- Adoption of Privacy Impact Assessment (PIA) without any substantial changes that affect the SNMC CONOPS
    - SNMC will comply with PII restrictions
    - Normal vs. Exceptional Operations (see 4.3 and 4.4 respectively)
- Currently have 6 analysts that have been trained and are standing Watch

1.2.2 Monitoring

- SNMC is currently fully operational 24/7 since January 12th, 2010 and will continue until March 2010 or based on updates made to the current PIAs for the Haiti recovery and 2010 Winter Olympics
- Analysts will follow the PIA and CONOPs to conduct searches for Items of Interest to report to the NOC approved distribution list for Haiti recovery and 2010 Winter Olympics
    - Reports include Guardian Advisory Reports (GARs) and Guardian Information Reports (GIRs)

    - GARs are to alert the NOC to breaking events
    - GIRs provide additional in-depth information to situational awareness
- The SMNC is also generating Guardian Special Reports (GSRs) for both the Haiti recovery and 2010 Winter Olympics. These reports provide a summary of agreed upon items at daily intervals—defined by Don Triner (DHS/OPS Current Ops Branch Chief)
    - SNMC management and senior staff will take shifts to provide on-call review and advising for reports
- SNMC will continue to give tips to the MMC as part of its operations

1.2.3 Public Engagement: OPS to Public

- SNMC will work with an OPS/NOC point of contact to develop content requirements for public widgets, applications or social networking presences
- OPS/NOC point of contact will sign-off on any content before it is published to the public or a basic content requirement process will be agreed to that the SNMC will utilize for content development
- Assumes a PIA for general operations has been approved and further guidance has been approved for Phase II operations

1.2.4 Public Engagement: Public to OPS

- SNMC will work with an OPS/NOC point of contact to develop content requirements for public widgets, applications or social networking presences
- OPS/NOC point of contact will sign-off on any content before it is published to the public or a basic content requirement process will be agreed to that the SNMC will use utilize for content development
- SNMC will have a point of contact within the OPS/NOC to forward relevant public submissions
    - OPS/NOC responses will then be submitted back to the public
- Assumes a PIA for general operations has been approved and further guidance has been approved for Phase II operations

2. Battle Rhythm for Watch Analysts

2.1 Review and Sign-Off on the Turnover Briefing

- This is a synopsis of the previous shift and will aid the oncoming analyst to continue operations without any substantial break in reporting and will include:
    - Guardian Operational Summary (G24)
    - Guardian Special Reports (GSRs)
    - Any active National Situation Summary (NSS)
    - International Situation Summary (ISS)
    - Steady State incidents
    - Current requests for information from the NOC Watch Team, and any additional instructions for the next shift
    - Review on-going Trend Analysis summary
- Review the SNMC checklist and sign off that you understand directions and have performed all relevant checks on office equipment

- Check Outlook - The previous analyst will have sent you the daily log and the SNMC checklist. Download the log and checklist, and review previously distributed SN Items of Interest (IOIs) and Exceptional Items
- Review Management briefings, and any new operations directives

2.2 Check in with MMC Watch Analyst

- Review the MMC's Turnover Briefing
- Participate with MMC watch analyst with the call to the KMO, advise of the watch shift, receive any special instructions and note all in the Daily log
- Ask if there are any incidents they need help researching
    - Media Sources

      Social Networks

2.3 Monitoring

2.3.1 Full Initial Sweep of First Tier Social Network Sites (see First Tier List)

- Begin your search for emerging news stories and/or coverage of active situations. A recommend scan process is as follows:
    - Determine what information has been distributed already (read and analyze prior SN IOI's and Exception Items). Focus on the previous 24 hours but have a working knowledge of the previous 5 days
    - Keep an eye on live social networking streams on Twitter using Search.Twitter.com, Google Search, and RSSOwl Feeds
    - Launch RSSOwl and do a complete scrub of information. (Utilize the cleanup wizard to remove items older than 24hrs). Ensure all watches are read and marked so as when new information arrives it is easier to distinguish
    - Actively utilize search tools available on each site (that are not loaded into SN RSS Tools) in an attempt to locate stories pertaining to items such as Homeland Security, DHS, terrorism, weather, or other items of focus
        - Use the Key Words list (See SNMC SOP)
        - Search terms based on Turnover Briefing, CIRs and OPSUM
        - Repeat this process for Tier 2 and 3 social networking sites
- Monitor and give tips to MMC based on CIRs
- Do follow-up research on Trend Analysis Directives
- Keep notes in MS OneNote

2.3.1.1 Tracking developing events on Social Media: Examples

- Establish which hash-tags and keywords are being used by the public
- Search twitter, YouTube and flickr
- Search blogs via Google Blogsearch, Technorati, etc.
- Watch Wikipedia entries on the topic for changes
- (See Section 8.0 and 8.1 for a complete list)

2.3.2 Research

- Research ongoing trends

    - Add notes to Trend Analysis Summary
- Dig into second and third tier social network sites or specific niche sites
- For additional granularity: dig into third tier social networking sites or specific niche sites

2.3.3 Engagement Tool

- Update OPS/NOC SNMC managed web site (Phase II, TBD)
- Update social network applications and widgets as directed

2.3.4 Reporting

- SN Reporting (Guardian Reports) – (see 4.3)
- "Exception Reporting" (see 4.4)
- SN Daily Summary Reports due to leadership 5 am (see 4.5)

3. Battle Rhythm for Project Time Analysts

- Check-in with SNMC Watch Analyst
- Support the SNMC Watch Analyst
- Research trends
- Update OPS/NOC SNMC managed web sites, social network applications and widgets
- Research and develop SNMC Trend Reports as directed by OPS/NOC
- Research and help manage on-going development efforts to improve monitoring and public engagement and involvement projects

4. OPS Reporting Requirements/Parameters for SNMC Operations

4.1 DHS OPS Critical Information Requirements (CIRs)

- Potential threat to DHS, other federal, and state and local response units, facilities and resources
- Potential impact on DHS capability to accomplish the HSPD-5 mission
- Identifying events with operational value…corroborating critical information
- Identifying media reports that reflect adversely on DHS and response activities
- Standing HSC planning scenarios

4.2 SNMC Trend Analysis Requirement: Compare validity and value of data collected

- Credible Source (media-linked reporter or expert)
- Credible Evidence (photo, video, audio)
- Collection of Corroborating "Hits" Indicating a Trend (posts, observations and opinions from multiple sources)
- Official Alerts (local, state, national, tribal governments, NGOs)

4.3 SN Reporting: During "Normal" Operations:

- **Monitor** - Using Web 2.0 tools to search and observe social networks' communications
- **Collect Hits** – Potential "hits" are deleted of all personally identifiable information and stored for analysis
- **Analyze Hits** - Comparing "hits" to the Critical Information Requirements and Trend Analysis Requirements

- **Produce Results** – Selecting "hits" that contribute to overall situational awareness
- **Report Format** – Decide whether critical information should be communicated as a GAR, GIR, GSR, or TIP to the MMC
- **Report Results** - Reporting possible items of interest to the NOC and an approved distribution list that includes senior MMC OPS advisor and/or on duty MMC analyst
- **Purge** – Non-PII information will be held for trend analysis for a period of one year, then will be deleted from SNMC systems

4.3.1 NSS/ISS reporting: Same process as above, but with different reporting template

4.4 Suspicious "Exceptional" activity reports

4.4.1 This triggers the "Exceptional" Operations: SNMC will collect PII information that relates to the rare situations that have "life or death" implications:

- **Monitor** - Using Web 2.0 tools to search and observe social networks' communications
- **Collect Hits** – Potential "hits" including relevant PII are collected temporarily, but will not be put into a searchable database
- **Analyze Hits** - Comparing "hits" to the Critical Information Requirements and Trend Analysis Requirements
- **Produce Results** – Selecting "hits" that contribute to overall situational awareness, the rest immediately have all PII deleted if not part of the report to the NOC
- **Report Results** - Reporting the data directly to senior management for approval, and then to the NOC
  - Confirm that the NOC received the information
- **Purge** – All PII will be deleted from the data within 24 hours of the initial collection time or upon confirmation the NOC received the information
  - Delete and remove all unused information from SNMC analyst's systems

4.5 Daily Report

4.5.1 SNMC will be submitting a daily report as part of the 0500 MMC report to the NOC

- Summary of SN IOIs, NSS/ISS, Steady States
- Summary of any Exceptional Items
  - Do not include any PII
- PII must be deleted within 24 hours of initial collection or upon confirmation the NOC received the information
- Summary of any social network trends in relation to CIRs or NOC directives
- Daily Report should be finished by 0400 for review
  - Email report to SNMC management for review and sign-off

5. SNMC Operations

5.1 Monitor Social Networks and Media

- There are hundreds of Social Networks and Social Media websites and tens of thousands of active blogs, but a smaller subset receives a high percentage of the overall traffic

- Based on statistics issued by Nielsen, the SNMC has determined a list of social websites, search tools and aggregation tools that cover a large swath of these social communications on a daily basis
- SNMC will focus on a list of **40** websites, which include social networks, social media, search engines and social data aggregators (see Appendices)
- There are **16** unofficial groups for DHS components on Facebook and Myspace, and **16** unofficial DHS related blogs we've identified to be relevant and timely (see Appendices)

The SNMC will monitor public social communications on the internet using:

Social Approach	http://socialapproach.com/gov20
Go.usa.gov	http://go.usa.gov
WikiLeaks	http://wikileaks.org/
Cryptome	http://cryptome.org/
Google Blog Search	http://blogsearch.google.com
Technorati	http://technorati.com/
Foreign Policy Passport	http://blog.foreignpolicy.com/
Danger Room	http://www.wired.com/dangerroom/
Threat Level	http://www.wired.com/threatlevel/
Homeland Security Today	http://www.hstoday.us/
NTARC	http://www.nationalterroralert.com/
LA Now	http://latimesblogs.latimes.com/lanow/
NYTimes Lede Blog	http://thelede.blogs.nytimes.com/
STRATFOR	http://www.stratfor.com/
Drudge Report	http://drudgereport.com/
Huffington Post	http://huffingtonpost.com/
BNOnews	http://www.bnonews.com/
MEMRI	http://www.memri.org/
Informed Comment	http://www.juancole.com/
Homeland Security Watch	http://www.hlswatch.com/
Borderfire Report	http://www.borderfirereport.net/
Homeland Security Watch	http://www.hlswatch.com/
ABCNews Blotter	http://abcnews.go.com/Blotter/
WireUpdate	http://wireupdate.com/
RSSOwl	http://www.rssowl.org/
Twitter	http://twitter.com

5.2 Engage and Inform the Public Using Social Networks – TBD (not operational)

- The public will have an opportunity to agree to a "Terms of Service" (TOS) that will give them the ability to submit comments, tips, photos, audio/video files, hyperlinks and other useful information to the social networking accounts and widgets.

5.2.1 DHS OPS/NOC Webpages (OPS to Public) – TBD (not operational)

- Provide a current public view of the events that the DHS OPS/NOC is tracking and working on

- Inform the public about the role and responsibilities of the OPS/NOC
- Brief the public on ways that they can contribute to help OPS and DHS in the event of a crisis
- Provide a brief description of trending "hot" topics and events that pertain to the daily mission of the OPS/NOC
- Links to the outreach efforts of other DHS components could be provided
- Frequently Asked Questions that give guidance on what types of information the OPS/NOC is interested in rcceiving

5.2.2 Widgets – TBD (not operational)

- The SNMC will develop "widgets" that would be available to the public for placement on various related public websites
- Widgets are small, portable blocks of code that are openly shared with website operators in the hopes that they will help disseminate featured information to the people who view their webpages
- This strategy is currently used by Ready.gov, FEMA and the DHS Leadership Journal
- Widgets direct traffic and information flow back to the OPS/NOC webpage
- Widgets can be deployed to support incident specific activities rapidly

5.2.3 Social Network Accounts – TBD (not operational)

- SNMC will open accounts on popular social networks that will be complementary to the OPS/NOC webpages
- Establish a presence on these social networks for the SNMC to further engage the public on behalf of the OPS/NOC and direct the public to visit the OPS/NOC webpages for further information

5.2.4 Social Network Web Applications – TBD (not operational)

- Applications will be created that will be a complementary extension of the OPS/NOC webpages
- Aiming to reach out to sectors of the public that would otherwise be uninterested in visiting the OPS/NOC webpages

5.2.5 Mobile/Phone Applications – TBD (not operational)

- The ubiquity of cellular telephones provides a vehicle for the dissemination and collection of real-time data during a crisis
- The SNMC proposes to create applications for two leading platforms: Blackberry and Apple's iPhone
- The applications would be provided to the public at no cost through the Blackberry Store and iTunes Store
- Through the use of a mobile applications, the OPS/NOC can send announcements or alerts, push relevant health information, or issue a request for event specific details

5.3 Informing DHS OPS/NOC (Public to Ops) – TBD (not operational)

5.3.1 Web pages on dhs.gov (Public to OPS) – TBD (not operational)

- Website will have a mechanism to receive potentially operationally relevant information from the public to enhance situational awareness for the OPS/NOC
- Contributors will be guided through a decision tree filter that will increase the likelihood of getting actionable and relevant information during an event or crisis

5.3.2 Widgets– TBD (not operational)

- Widgets can also be designed to receive information directly from the public
- A form can be embedded into a widget so that a concerned citizen or event eyewitness can fill out and submit the information
- These widgets are extensions of the OPS/NOC webpage functions

5.3.3 Social Network Accounts– TBD (not operational)

- The public will interact with the OPS/NOC through the accounts created by the SNMC on various social networking websites

5.3.4 Social Network Web Applications– TBD (not operational)

- The public will use social network applications to submit information and ask questions regarding OPS related events and crises

5.3.5 Mobile/Phone Applications– TBD (not operational)

Through the use of a mobile application, the public would be able to submit the following examples:

- A photo of rising flood waters that has been geo-tagged to an exact location
- Video from the scene of an accident on I-95 involving a tanker truck
- A text message giving the number of terrorists who have taken over a high school

6. Security Protocols: SNMC Social Networking Accounts – TBD (not operational)

- Usernames and Passwords
  - Passwords will change monthly to limit the exposure of accounts and fend off hackers
  - SNMC management will change the passwords and keep them in the SNMC SOP for the analysts
- If an account appears to be compromised, it must be reported to SNMC management for further instructions
  - Record and screen capture all changes to the account for record keeping
- Report any other suspicious activity

7. Current DHS Web 2.0

DHS and its agencies utilize several Web 2.0 technologies and tools to engage and inform the public like the DHS Journal maintained by OPA (List of DHS Blog under the Appendix)

- (e.g.) U.S. Coast Guard extended their presence to the major social networks
  - Official pages on Facebook maintained by the Coast Guard for:
    - The Commandant
    - Coast Guard
    - Two ships and two stations

- Several unofficial "groups" within Facebook and MySpace have been created by employees, friends and family

7.1 Current DHS OPS Web Site

DHS OPS does not have any Web 2.0 presences. The only web site is located at: http://www.dhs.gov/xabout/structure/editorial_0797.shtm

8. Appendices

All sites must have the ability to be searched openly and not require registration for accounts or clickable Terms-of Service. List is subject to change at anytime based on changes to registration requirements by the 3rd party owners. Those sites listed below are a sample of the types of sites analysts could search, as long as they continue to not conflict with stated procedures.

8.1 Searched Networks, Blogs, Searches and Aggregator

Social Networks:
Myspace
Facebook

Niche Social Networks:
Stormfront
InfoWar.com

Blogs and Micro-blogs:
Twitter
TweetGrid
Technorati
Blogger.com
LiveJournal
Wordpress.com

Photos:
Flickr
Smugmug
Photobucket
iReport
uReport
Zooomr
Ask.com
Pixsy

Videos:
Youtube
Yahoo Video
Myspace Video
Vimeo
UStream
Justin.tv
Metacafe
Blip.tv
Dailymotion

Social Bookmarking:
Digg
Delicious
Reddit
Stumbleupon
Newsvine

Realtime Twitter Search:
Tweetmeme
OneRiot (twitter + digg)
TwitScoop

Crowdsourcing:
Wikipedia
Google Groups
Ning

Aggregators:
Britekite
SocialMention
BackType
Friendfeed
Spy.appspot.com
Google Blogsearch

DHS-related Blogs:
In Homeland Security
HSDL-NPS On the Homefront
DefenseTech
Homeland Security Affairs Journal
Homeland Security Leader
Open Target
Security Debrief
Michael Brown Today
DangerRoom/Wired
Homeland Security Watch
Immigration Prof Blog
MetaSecurity
Counterterrorism Blog
In Case of Emergency
Privacy and Security Law Blog
Disaster Zone

8.2 Tiered Listing of Social Media Sites the SNMC will Search

(determined by Alexa, Compete, Hitwise and Comscore ratings and experience in SN)

Tier 1:
Facebook
Twitter
Myspace
Flickr
YouTube
Event specific sites (eg. Inauguration, Olympics, etc.)

Tier 2:
Photobucket
Yahoo Video
Myspace Video
Dailymotion
Blogger.com
LiveJournal
Wordpress
Blogs.com
Digg
Delicious
Reddit
Linkedin
Ning
TweetGrid
Technorati
iReport

Tier 3:
MeetUp
Skyrock
Scribd
Stormfront
InfoWar.com
Hatewatch

Others as needed by situation or event

Social Networking/Media Capability (SNMC)
Battle Rhythm

Version 7
18 February 2010

Battle Rhythm for Watch Analysts

1. **Review and Sign-Off of the Change Over Briefing**
   - This is a synopsis of the previous shift and will aid the oncoming analyst to continue operations without any substantial break in reporting. The following will be the search priorities for each analyst for every shift, including but not limited to:
     - All items from the latest NOC Priorities and Monitoring Report including:
       - Any active National Situation Summaries (NSS)
       - International Situation Summaries (ISS)
       - Steady-State incidents
       - Events of high media interest
       - Current requests for information from the NOC Watch Team, DHS Senior Staff Requests and any additional instructions for the next shift (see section___ Change-Over)
     - Selected items from the MMC Operational Summary (OPSUM)
     - TSI Management Notes/Directives/Instructions
     - Watch Analyst's Notes/Questions/Instructions including:
       - Hashtags that are being used for events/incidents that would be helpful to the next analyst
     - Events of high media interest
     - Review on-going Trend Analysis summary (see section _____ Trend Analysis)
   - Review the SNMC Change Over and sign off that you understand directions and have performed all relevant checks on office equipment
   - Check Outlook - The previous analyst will have saved the change over on the T: Drive and the SNMC daily log on Google Docs. Review the daily log and previously distributed SN Guardian Information Reports (GIRs) and Exceptional Items

2. **Check in with MMC Watch Analyst**
   - Review the MMC's Turnover Briefing
   - Participate with MMC watch analyst on the call to the KMO, receive any special instructions and note all in the Daily log
   - Ask if there are any incidents they need help researching
     - Media Sources
     - Social Networks

2. **Login to NOC_Watch on HSIN Over** (b) (7)(E)
   - Need to have HSIN account access
   - Join the NOC_watch channel
   - Do not chat in the channel until SNMC is authorized
     - Any communication with chatroom may be sent via MMC

- An email with registration instructions to both HSIN and(b) (7)(E) will be sent to analyst upon initial training

3. Access SN Tools and enter relevant search terms (OPS Web Site: coming soon…)

- Match the Change Over Briefing, Critical Information Requirements (CIRs) and OPSUM with relevant key words
    - o Access Twitter search tools
        - ▪ Twitter Search: http://search.twitter.com
        - ▪ Twazzup: http://www.twazzup.com
        - ▪ Tweetgrid: http://www.tweetgrid.com
        - ▪ Trendsmap: http://www.trendsmap.com
    - o Access Picture/Video search tools
        - ▪ PicFog: http://www.picfog.com
        - ▪ TwitCaps: http://www.twitcaps.com
        - ▪ Flickr: http://www.flickr.com
        - ▪ PhotoBucket: http://www.photobucket.com
        - ▪ YouTube: http://www.youtube.com
        - ▪ Yahoo Video: http://www.yahoo.com
    - o Open up the 'SNMC Daily Log' Spreadsheet
    - o Open up or continue running SN tools that are on the Mac mini. Login instructions are located on a sticky note attached to the bottom of the Mac
        - ▪ Username: Admin
        - ▪ Password: (b)(6), (b)(7)(E)
    - o Test television video switch settings by logging on to video switch site. 'Output Four' is the designated SNMC screen and should be adjusted so that either the extended desktop on the Mac or laptop is shown while on watch. 'Aux (7)' corresponds with the laptop and 'SNMAC' corresponds with the Mac mini
        - ▪ http://10.1.10.150/content_switch.html
            - Username: Administrator
            - Password: (b)(6), (b)(7)(E)

4. Searching

4.1 Full Initial Sweep of First Tier Social Network Sites (see First Tier List)

- Begin your search for emerging news stories and/or coverage of active situations. A recommend scan process is as follows:
    - o Determine what information was previously distributed (read and analyze prior SN Tips and GIRs). Focus on the previous 24 hours but have a working knowledge of the previous 5 days
    - o Keep an eye on live social networking streams on Twitter using Twazzup, TweetGrid, and Yahoo Pipes RSS Feeds
    - o Utilize search tools available on each site in an attempt to locate stories pertaining to items such as Homeland Security, DHS, terrorism, weather, or other items of focus
        - ▪ Use the Key Words list (See SNMC SOP)
        - ▪ Search terms based on Turnover Briefing, CIRs and OPSUM

        - Repeat this process for Tier 2 and 3 social networking sites
- Review the Change-Over/OPSUM and all other items in section 2.1 of the Battle Rhythm and cycle through and search each of those priorities at least once every couple of hours
- Employ use of Boolean logic, usage of "OR", "AND" and "FROM:" to make searches more efficient. Examples:
    - arrested OR arrests OR arrest
    - "dirty bomb" OR "nuclear bomb" OR nuke FROM:cnn
    - Operators such as "OR", "AND" and "FROM:" must be capitalized for most search tools/engines
- Search and give tips to MMC based on CIRs
- Do follow-up research on Trend Analysis Directives

4.1.1 Tracking developing events on Social Media: Examples

- Establish which hashtags and keywords are being used by the public, note in Daily Log when possible
- Search twitter, youtube and flickr
- Search blogs via Google Blogsearch, Google News
- Watch Wikipedia entries on the topic for changes
- (See Section 8.0 and 8.1 for a complete list)

4.2 Research

- Research ongoing trends
    - Add notes to Trend Analysis Summary
- For additional granularity: dig into second and third tier social networking sites or specific niche sites

5. Engagement (not active)

- Update OPS/NOC SNMC managed web site (Phase II, TBD)
- Update social network applications and widgets as directed

6. Reporting

- Guardian Advisory Reports (GARs)
    - Short alerts regarding a breaking event or incident
- "Exceptional Reporting"
- Guardian Information Reports (GIRs)
    - Detailed information beyond what a GAR provides, often giving sentiment or granularity
- Guardian Special Reports (GSRs)
    - Long form reports usually requested by Senior Staff or the NOC

SN Daily Summary Reports due to leadership 5 am

7. Battle Rhythm for Project Time Analysts

- Check-in with SNMC Watch Analyst
- Support the SNMC Watch Analyst
- Research trends
- Update OPS/NOC SNMC managed web sites, social network applications and widgets
- Develop SNMC Trend Reports as directed by OPS/NOC (See SNMC Trend Reports section)
- Research and help manage ongoing development efforts to improve monitoring and public engagement/involvement projects

8. Appendices

All sites must have the ability to be searched openly and not require registration for accounts or clickable Terms-of Service. List is subject to change at anytime based on changes to registration requirements by the 3rd party owners. Those sites listed below are a sample of the types of sites analysts could search, as long as they continue to not conflict with stated procedures.

8.1 Searched Networks, Blogs, Searches and Aggregator

Social Networks:
Myspace
Facebook

Niche Social Networks:
Stormfront
InfoWar.com

Blogs and Micro-blogs:
Twitter
TweetGrid
Technorati
Blogger.com
LiveJournal
Wordpress.com

Photos:
Flickr
Smugmug
Photobucket
iReport
uReport
Zooomr
Ask.com
Pixsy

Videos:
Youtube
Yahoo Video
Myspace Video
Vimeo
UStream
Justin.tv
Metacafe
Blip.tv
Dailymotion

Social Bookmarking:
Digg
Delicious
Reddit
Stumbleupon
Newsvine

Realtime Twitter Search:
Tweetmeme
OneRiot (twitter + digg)
TwitScoop

Crowdsourcing:
Wikipedia
Google Groups
Ning

Aggregators:
Britekite
SocialMention
BackType
Friendfeed
Spy.appspot.com
Google Blogsearch

DHS-related Blogs:
In Homeland Security
HSDL-NPS On the Homefront
DefenseTech
Homeland Security Affairs Journal
Homeland Security Leader
Open Target
Security Debrief
Michael Brown Today
DangerRoom/Wired
Homeland Security Watch
Immigration Prof Blog
MetaSecurity
Counterterrorism Blog
In Case of Emergency
Privacy and Security Law Blog
Disaster Zone

8.2 Tiered Listing of Social Media Sites the SNMC will Search

(determined by Alexa, Compete, Hitwise and Comscore ratings and experience in SN)

Tier 1:
Facebook
Twitter
Myspace
Flickr
YouTube
Event specific sites (eg. Inauguration, Olympics, etc.)

Tier 2:
Photobucket
Yahoo Video
Myspace Video
Dailymotion
Blogger.com
LiveJournal
Wordpress
Blogs.com
Digg
Delicious
Reddit
Linkedin
Ning
TweetGrid
Technorati
iReport

Tier 3:
MeetUp
Skyrock
Scribd
Stormfront
InfoWar.com
Hatewatch

Others as needed by situation or event

8.3 News agencies/personalities on Twitter

Breaking News:
BreakingNews
CNNbrk
breakingnewsdeu
capitalalert
BN_newsalert

Media Agencies:
LATimes
NYTimes
cnn
wsj
foxnews
CBSNews
ajc
dallas_news
reuters
nprnews

Privacy Impact Assessment
for the

Office of Operations Coordination and Planning

Haiti Social Media

Disaster Monitoring Initiative

January 21, 2010

Contact Point
Donald Triner
Director (Acting), National Operations Center
Office of Operations Coordination and Planning
(202) 282-8611

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), has launched a Haiti Social Media Disaster Monitoring Initiative (Initiative) to assist the Department of Homeland Security (DHS), and its components involved in the response, recovery, and rebuilding effort resulting from the recent earthquake and after-effects in Haiti. The NOC is using this vehicle to fulfill its statutory responsibility to provide situational awareness and establish a common operating picture for the federal Government, and for those state, local, and tribal governments, as appropriate, assisting with the response, recovery, and rebuilding effort in Haiti. OPS may also share information with international partners and the private sector where necessary and appropriate for humanitarian assistance and disaster relief. The NOC is only monitoring publicly available online forums, blogs, public websites, and message boards to collect information used in providing situational awareness and to establish a common operating picture. OPS will not set up user accounts to access any information. While this Initiative is not designed to collect personally identifiable information (PII), OPS is conducting this Privacy Impact Assessment (PIA) because the Initiative could potentially involve information received in an identifiable form. This PIA is effective for 90 days and will be reviewed and updated at that time. Should the requirements for the Initiative change before this expiration date, OPS and the Privacy Office will immediately update this PIA.

Overview

Federal law requires the NOC to provide situational awareness and a common operating picture for the entire federal Government, and for state, local, and tribal governments as appropriate, and to ensure that critical disaster-related information reaches government decision-makers. *See* Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)). The law defines the term "situational awareness" as "information gathered from a variety of sources that, when communicated to emergency managers and decision-makers, can form the basis for incident management decision-making." OPS is launching this Initiative to fulfill the NOC's legal mandate—in this case, to provide situational awareness directly related to the response, recovery, and rebuilding effort in Haiti.

The NOC is using Internet-based platforms that provide a variety of ways to follow activity in the earthquake stricken country of Haiti by monitoring publicly available online forums, blogs, public websites, and message boards. Through the use of publicly available search engines and content aggregators,[1] the NOC continuously monitors activities on social media sites (e.g., a variety of major/niche social networking sites, blog networks) for information directly relevant to the disaster in Haiti. The NOC gathers, stores, analyzes, and disseminates relevant and appropriate information to federal, state, local, and foreign governments, and private sector partners requiring and authorized to receive situational awareness and a common operating picture.

The NOC is identifying and monitoring only information directly related to the response, recovery, and rebuilding arising from the earthquake in Haiti. The NOC will use this information only to fulfill the statutory mandate set forth above to include the sharing of information with foreign governments and the private sector as otherwise authorized by law. The NOC will not:

[1] Content aggregators generally provide a consolidated view of web content in a single browser display or desktop application.

- seek, collect, or retain any PII;
- conduct any social networking where individuals are required to establish a username and password to gain access to information;
- seek to establish or establish individual identities or connect with other individuals' identities.

Should PII come into the NOC's possession, the NOC shall delete and destroy it prior to further dissemination of any collected information.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The NOC is reviewing information posted by individual account users on third party social media providers, of activities and events necessary to provide situational awareness regarding the response, recovery, and rebuilding efforts arising from the earthquake in Haiti. Third party service providers provide an array of applications that provide social media services along with publicly available online forums, blogs, public websites, and message boards, such as Twitter. See Appendix I for a list of the types of sites that may be viewed for information related to the Haiti earthquake. The NOC is accessing these web-based platforms to identify content posted by public users for the purpose of providing situational awareness and establishing a common operating picture on the disaster in Haiti. The NOC is assessing information identified to assist decision-makers in the response, recovery and rebuilding effort in Haiti. The NOC shall not collect data on the individuals posting information to third party service providers, about individual users, or any PII. The NOC will immediately destroy any PII that it discovers at any time in its possession as a result of this Initiative.

1.2 What are the sources of the information in the system?

Members of the public as well as first responders, press, humanitarian organizations, and others provide publically available information on social media sites including online forums, blogs, public websites, and message boards.

1.3 Why is the information being collected, used, disseminated, or maintained?

The NOC is identifying, using, disseminating, and maintaining this information to comply with its statutory mandate to provide situational awareness and a common operating picture for the entire federal Government, and for state, local, and tribal governments as appropriate, and to ensure that critical disaster-related information reaches government decision-makers. In this case, the NOC is monitoring information directly related to the response, recovery, and rebuilding arising from the earthquake in Haiti. The aggregation of data published via social media sites will likely make it possible for the NOC to provide more accurate situational awareness, a more complete common operating picture, and more timely disaster-related information for decision-makers.

1.4 How is the information collected?

The NOC identifies information directly from the third-party hosting social media services. The NOC is accessing and collecting information from various informational streams (e.g., "tweets") and postings that the NOC, as well as the broader public, view and monitor. For example, information can normally be read in "news feeds," which are data streams of account activity from other account holders.

1.5 How will the information be checked for accuracy?

The NOC identifies information from third party hosts submitted voluntarily by members of the public and compares that information with information available in open source reporting and through a variety of public and Government sources. By bringing together and comparing many different sources of information, the NOC will attempt to generate a more accurate picture of activities occurring in Haiti.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Congress requires the NOC "to provide situational awareness and establish a common operating picture for the entire federal Government, and for state, local, and tribal governments as appropriate, in the event of a natural disaster... and ensure that critical . . . disaster-related information reaches government decision-makers." Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)).

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

There is a risk that the NOC will receive PII that is not relevant to this Initiative. The NOC has a clear policy in place that any PII incidentally received will be destroyed immediately. Information collected to provide situational awareness and establish a common operating picture originates from publically available social media sites and is available to the public.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The NOC is using Internet-based platforms that provide a variety of ways to follow activity in the earthquake stricken country of Haiti by monitoring publicly available online forums, blogs, public websites, and message boards. Through the use of publicly available search engines and content aggregators, the NOC will continuously monitor activities on social media sites (e.g., a variety of major/niche social networking sites, blog networks such as those listed in Appendix I) for information directly relevant to the disaster in Haiti. The NOC will gather, store, analyze, and disseminate relevant and appropriate information to federal, state, local, and foreign governments, and private sector partners requiring and authorized to receive situational awareness and a common operating picture.

2.2 What types of tools are used to analyze data and what type of data may be produced?

NOC analysts are responsible for monitoring and evaluating information provided on social media sites. The overall analysis will be used to provide situational awareness and establish a common operating picture.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Publicly available, user-generated data can be useful to decision makers as it provides "on-the-ground" information to help corroborate information received through official sources.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

As the NOC does not plan to collect or use any PII, the risk to privacy is that PII will be brought into the NOC unintentionally. This has been mitigated by the clear policy that any PII inadvertently collected shall be destroyed immediately. As noted in section 1, any PII related to the posting will be redacted.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

The NOC will retain only user-generated information posted to publicly available online social media sites. The NOC will not retain information related to individuals posting the information.

3.2 How long is information retained?

The NOC will retain information only long enough to provide situational awareness and establish a common operating picture.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

The DHS Records Officer is working with NARA to establish an approved retention and disposal policy.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The risk associated with retention of information is that PII will be retained when it is not necessary and that the information will be kept longer than is necessary. The NOC has mitigated this risk by not collecting any PII.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Information related to the Haiti disaster is shared within the NOC, with Departmental leadership, and with those components within the Department involved in the response, recovery, and rebuilding effort in Haiti. The NOC is sharing this information for the statutorily mandated purpose of providing situational awareness and establishing a common operating picture

4.2 How is the information transmitted or disclosed?

Information is transmitted via email and telephone within the NOC and to the Department's components where necessary and appropriate. PII is not collected, but if pushed to the NOC, it will be deleted by the NOC before information is shared. The remaining data is analyzed and prepared for reporting.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The risk associated with sharing this information is that PII will be inadvertently collected and shared. The NOC has mitigated this risk by establishing effective policies to avoid collection of PII and for its immediate destruction if collected inadvertently. Additionally, the NOC will not conduct any social networking where individuals are required to establish a user name and password to gain access to information. Instead, the NOC is only monitoring publicly accessible sites where users post information voluntarily; hence there is no reasonable expectation of privacy in such information thereby mitigating any potential privacy risks associated with sharing.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

The NOC is using this Initiative to fulfill its statutory responsibility to provide situational awareness and establish a common operating picture for the entire federal government, and for state, local, and tribal governments as appropriate, and to ensure that critical disaster-related information reaches government decision-makers. Information may also be shared with private sector and international partners where necessary, appropriate, and authorized by law.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

PII is not collected, retrieved, shared or retained. Information is only collected to provide situational awareness and to establish a common operating picture.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information is shared by phone and email. No PII is collected, retrieved, shared, or retained.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

External sharing risks are minimal as the Initiative does not share PII; only information collected to provide situational awareness and to establish a common operating picture is shared.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

The Department may publicize its use of social media. The NOC does not, however, provide notice to specific public users who voluntarily provide user-generated information on publicly accessible social media sites where individuals are *not* required to establish a user name and password to gain access to information. The NOC may retrieve public information from the social media sites, but will not respond to individual users as no accounts will be created.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Information posted to social media is publicly accessible and voluntarily generated. Thus, the opportunity not to provide information exists prior to the informational post by the user.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Individuals voluntarily post information on social media sites and have the ability to restrict access to their posts as they see fit. Any information posted publicly can be used by the NOC in providing situational awareness and establishing a common operating picture.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

There is no legal requirement to provide notice to individuals under the framework applied under this Initiative. Information posted to social media approved for monitoring under this Initiative is publicly accessible without a password and voluntarily generated. There is no reasonably expectation of privacy with such information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Social media are public websites. All users have access to their information through their user accounts. Individuals should consult the privacy policies of the services to which they subscribe for more information.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Users may accidentally or purposefully generate inaccurate or erroneous information. There is no mechanism for correcting this. However, the community is largely self-governing and erroneous information is normally expunged or debated rather quickly by others within the community with more accurate and/or truthful information.

7.3 How are individuals notified of the procedures for correcting their information?

There is no specified procedure for correcting information; if there was, it relates to a social media-provided process and not a DHS process. Individuals may change their PII on the sites as well as the accessibility of their content posts at any time they wish through their user account management tools on social media sites.

7.4 If no formal redress is provided, what alternatives are available to the individual?

There is no specified procedure for correcting information; if there was, it relates to a social media-provided process and not a DHS process. Individuals may change their PII as well as the accessibility of their content posts at any time they wish through their user account management tools on the social media sites. Individuals should consult the privacy policies of the services they subscribe to for more information.

7.5 <u>Privacy Impact Analysis</u>: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

The information available on social networking websites is largely user-generated, which means that the individual chooses the amount of information available about himself/herself as well as the ease with which it can be accessed by other users. Thus, the primary account holder should be able to redress any concerns through the third party host of the service. Individuals should consult the privacy policies of the services they subscribe to for more information.

.Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

No procedures are in place. Social media sites are publicly available, third-party services

8.2 Will Department contractors have access to the system?

Yes, as it is required in the performance of their duties at DHS.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All DHS employees and contractors are required to take annual privacy training.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

No, it is not necessary.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

OPS will review after 90 days all the information collected for this project to ensure that no PII has accidentally been collected and to determine whether the Initiative should continue.

8.6 <u>Privacy Impact Analysis</u>: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

These social media sites are publicly available, third-party services. Information is collected by the service itself to establish an account. Thereafter, users determine their level of involvement and decide how "visible" they wish their presence on any given service to be. The ability to choose how much information to disclose, as well as the short period of retention for any PII collected by the NOC, serve to mitigate any privacy risk.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

Third parties control and operate these services. Users should consult with representatives of the service provider in order to make themselves aware of technologies utilized by the sites or services.

9.2 What stage of development is the system in and what project development lifecycle was used?

The Initiative is operational. The social media sites are third-party owned and operated

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

Individuals should consult the privacy policies of the social media services to which they subscribe for more information.

Responsible Officials

Donald Triner
Director (Acting), National Operations Center
Office of Operations Coordination and Planning
Department of Homeland Security

Approval Signature

Original signed copy on file at the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX I

Examples of Social Media Web Sites Monitored by the NOC

This list is not comprehensive, but provides a list of the types of sites that the NOC is reviewing in order to improve its situational awareness and common operating picture related to Haiti earthquake.

Social Approach	http://socialapproach.com/gov20
Go.usa.gov	http://go.usa.gov
WikiLeaks	http://wikileaks.org/
Cryptome	http://cryptome.org/
Google Blog Search	http://blogsearch.google.com
Technorati	http://technorati.com/
Foreign Policy Passport	http://blog.foreignpolicy.com/
Danger Room	http://www.wired.com/dangerroom/
Threat Level	http://www.wired.com/threatlevel/
NEFA Foundation	http://www.nefafoundation.org/
Counter-Terrorism Blog	http://www.counterterrorismblog.com/
Homeland Security Today	http://www.hstoday.us/
NTARC	http://www.nationalterroralert.com/
LA Now	http://latimesblogs.latimes.com/lanow/
NYTimes Lede Blog	http://thelede.blogs.nytimes.com/
STRATFOR	http://www.stratfor.com/
Drudge Report	http://drudgereport.com/
Huffington Post	http://huffingtonpost.com/
BNOnews	http://www.bnonews.com/
MEMRI	http://www.memri.org/
Informed Comment	http://www.juancole.com/
LA Wildfires Blog	http://latimesblogs.latimes.com/lanow/wildfires/
Homeland Security Watch	http://www.hlswatch.com/
Joe Cirincione's nuclear issues blog	http://www.ploughshares.org/news-analysis/blog
Borderfire Report	http://www.borderfirereport.net/
Homeland Security Watch	http://www.hlswatch.com/
ABCNews Blotter	http://abcnews.go.com/Blotter/
WireUpdate	http://wireupdate.com/
MexiData.info	http://mexidata.info/
RSSOwl	http://www.rssowl.org/
Twitter	http://twitter.com

Privacy Impact Assessment
for the

Office of Operations Coordination and Planning

2010 Winter Olympics Social Media

Event Monitoring Initiative

February 10, 2010

Contact Point
Donald Triner
Director (Acting), National Operations Center
Office of Operations Coordination and Planning
(202) 282-8611

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), has launched a 2010 Winter Olympics Social Media Event Monitoring Initiative (Initiative) to assist the Department of Homeland Security (DHS) and its components involved in the security, safety, and border control associated with the 2010 Winter Olympics in Vancouver, British Columbia (BC). The NOC is using this vehicle to fulfill its statutory responsibility to provide situational awareness and establish a common operating picture for the federal government, and for those state, local, and tribal governments, as appropriate, assisting with the security, safety, and border control associated with the Olympics. OPS may also share information with international partners and the private sector where necessary and appropriate for security, safety, and border control coordination. The NOC is only monitoring publicly available online forums, blogs, public websites, and message boards to collect information used in providing situational awareness and to establish a common operating picture. OPS will not set up user accounts to access any information. While this Initiative is not designed to collect personally identifiable information (PII), OPS is conducting this Privacy Impact Assessment (PIA) because the Initiative could potentially involve information received in an identifiable form. This PIA is effective for 30 days and will expire at that time. Should the requirements for the Initiative change before this expiration date, OPS and the Privacy Office will immediately update this PIA.

Overview

Federal law requires the NOC to provide situational awareness and a common operating picture for the entire federal Government, and for state, local, and tribal governments as appropriate, and to ensure that critical disaster-related information reaches government decision makers. *See* Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)). The law defines the term "situational awareness" as "information gathered from a variety of sources that, when communicated to emergency managers and decision makers, can form the basis for incident management decision-making." OPS is launching this Initiative to fulfill its legal mandate to provide situational awareness and establish a common operation picture directly related to the security, safety, and border control associated with the 2010 Winter Olympics in Vancouver, BC.

The NOC is using Internet-based platforms that provide a variety of ways to follow activity related to the 2010 Winter Olympics by monitoring publicly available online forums, blogs, public websites, and message boards. Through the use of publicly available search engines and content aggregators,[1] the NOC continuously monitors activities on social media sites, such as those listed in Appendix A, for information directly relevant to the 2010 Winter Olympics so the NOC can provide situational awareness and establish a common operating picture. The NOC gathers, stores, analyzes, and disseminates relevant and appropriate de-identified information to federal, state, local, and foreign governments, and private sector partners authorized to receive situational awareness and a common operating picture.

The NOC is identifying and monitoring only information directly related to the security, safety, and border control associated with the 2010 Winter Olympics in Vancouver, BC. The NOC will use this

[1] Content aggregators generally provide a consolidated view of web content in a single browser display or desktop application.

information to fulfill the statutory mandate set forth above to include the sharing of information with foreign governments and the private sector as otherwise authorized by law. The NOC will not:

- Seek, collect, or retain any PII or other information in an identifiable form;
- Conduct any social networking where the Department's employees are required to establish a username and password to gain access to information; and
- Seek to establish or establish individual identities or connect with other individuals' identities.

Should PII come into the NOC's possession, the NOC shall delete and destroy it prior to further dissemination of any collected information.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The NOC is reviewing information posted by individual account users on third party social media providers of activities and events necessary to provide situational awareness and establish a common operating picture regarding the security, safety, and border control associated with the 2010 Winter Olympics in Vancouver, BC. Third party service providers provide an array of applications that provide social media services along with publicly available online forums, blogs, public websites, and message boards. See Appendix A for a list of the types of sites that may be viewed for information related to the 2010 Winter Olympics. The NOC is accessing these web based platforms to identify content posted by public users for the purpose of providing situational awareness and establishing a common operating picture on the 2010 Winter Olympics. The NOC is assessing information identified to assist decision-makers in the security, safety, and border control associated with the 2010 Winter Olympics. The NOC shall not collect data on the individuals posting information to third party service providers, about individual users, or any PII. The NOC will immediately destroy any PII that it discovers at any time in its possession as a result of this Initiative.

1.2 What are the sources of the information in the system?

Members of the public as well as first responders, press, volunteers, and others provide publicly available information on social medial sites including online forums, blogs, public websites, and message boards.

1.3 Why is the information being collected, used, disseminated, or maintained?

The NOC is identifying, using, disseminating, and maintaining this information to comply with its statutory mandate to provide situational awareness and establish a common operating picture for the entire federal government, and for state, local, and tribal governments as appropriate and to ensure that this information reaches government decision makers. In this case, the NOC is monitoring information directly related to the security, safety, and border control associated with the 2010 Winter Olympics in Vancouver, BC. The aggregation of data published via social media sites will likely make it possible for the NOC to provide more accurate situational awareness, a more complete common operating picture, and more timely 2010 Winter Olympics-related information for decision makers.

1.4 How is the information collected?

The NOC identifies information directly from third-party social media services. The NOC is accessing and collecting information from various informational streams and postings that the NOC, as well as the broader public, view and monitor.

1.5 How will the information be checked for accuracy?

The NOC identifies information from third party hosts submitted voluntarily by members of the public and compares that information with information available in open source reporting and through a variety of public and government sources. By bringing together and comparing many different sources of information, the NOC will attempt to generate a more accurate picture of activities occurring at the 2010 Winter Olympics.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Congress requires the NOC "to provide situational awareness and establish a common operating picture for the entire federal government and for state, local, and tribal governments as appropriate, in the event of a natural disaster, act of terrorism, or other manmade disaster; and ensure that critical terrorism and disaster-related information reaches government decision-makers." Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)). The Olympics are a potential target for such events.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

There is a risk that the NOC will receive PII or other identifiable information that is not relevant to this Initiative. The NOC has a clear policy in place that any PII incidentally received will be destroyed immediately. Information collected to provide situational awareness and establish a common operating picture originates from publicly available social media sites and is available to the public.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The NOC is using Internet-based platforms that provide a variety of ways to follow activity at the 2010 Winter Olympics in Vancouver, BC, by monitoring publicly available online forums, blogs, public websites, and message boards. Through the use of publicly available search engines and content aggregators, the NOC will continuously monitor activities on social media sites, such as those listed in Appendix A, for information directly relevant to the 2010 Winter Olympics. The NOC will gather, store, analyze, and disseminate relevant and appropriate information to federal, state, local, and foreign governments, and private sector partners requiring and authorized to receive situational awareness and a common operating picture.

2.2 What types of tools are used to analyze data and what type of data may be produced?

NOC analysts are responsible for monitoring and evaluating information provided on social media sites. The overall analysis will be used to provide situational awareness and establish a common operating picture.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Publicly available, user-generated data can be useful to decision-makers as it provides "on-the-ground" information to help corroborate information received through official sources.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

As the NOC does not collect or use any PII, the risk to privacy is that PII will be brought into the NOC unintentionally. This has been mitigated by the clear policy that any PII inadvertently collected shall be destroyed immediately. As noted in section 1, all PII will be redacted.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

The NOC will retain only user-generated infonnation posted to publicly available online social media sites. The NOC will not retain information related to individuals posting the information.

3.2 How long is information retained?

The NOC will retain information only long enough to provide situational awareness and establish a common operating picture.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

The DHS Records Officer is working with NARA to establish an approved retention and disposal policy.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The risk associated with retention of information is that PII will be retained when it is not necessary and that the information will be kept longer than is necessary. The NOC has mitigated this risk by not collecting any PII, and immediately destroying any PII it inadvertently collects.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Information related to the 2010 Winter Olympics is shared within the NOC, with Departmental leadership, and with those components within the Department involved in the security, safety, and border control associated with the 2010 Winter Olympics. The NOC is sharing this information for the statutorily mandated purpose of providing situational awareness and establishing a common operating picture.

4.2 How is the information transmitted or disclosed?

Information is transmitted via email and telephone within the NOC and to the Department's components where necessary and appropriate. PII is not collected, but if pushed to the NOC, it will be deleted by the NOC before information is shared. The remaining data is analyzed and prepared for reporting.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The risk associated with sharing this information is that PII will be inadvertently collected and shared. The NOC has mitigated this risk by establishing effective policies to avoid collection of PII and for its immediate destruction if collected inadvertently. Additionally, the NOC will not conduct any social networking where individuals are required to establish a user name and password to gain access to information. Instead, the NOC is only monitoring publicly accessible sites where users post information voluntarily; hence there is no reasonable expectation of privacy in such information thereby mitigating any potential privacy risks associated with sharing.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

The NOC is using this Initiative to fulfill its statutory responsibility to provide situational awareness and establish a common operating picture for the entire federal government, and for state, local, and tribal governments as appropriate, and to ensure that critical disaster-related information reaches government decision makers. Information may also be shared with private sector and international partners where necessary, appropriate, and authorized by law.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

PII is not collected, retrieved, shared, or retained. Information is only collected to provide situational awareness and to establish a common operating picture.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information is shared by phone and email. No PII is collected, retrieved, shared, or retained.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

External sharing risks are minimal as the Initiative does not share PII; only information collected to provide situational awareness and to establish a common operating picture is shared.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

The Department may publicize its use of social media. The NOC does not, however, provide notice to specific public users who voluntarily provide user-generated information on publicly accessible social media sites where individuals are ***not*** required to establish a user name and password to gain access to information. The NOC may retrieve public information from the social media sites, but will not respond to individual users as no accounts will be created.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Information posted to social media websites is publicly accessible and voluntarily generated. Thus, the opportunity not to provide information exists prior to the informational post by the user.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Individuals voluntarily post information on social media sites and have the ability to restrict access to their posts as they see fit. Any information posted publicly can be used by the NOC in providing situational awareness and establishing a common operating picture.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

There is no legal requirement to provide notice to individuals under the framework applied under this Initiative. Information posted to social media approved for monitoring under this Initiative is publicly accessible without a password and voluntarily generated. There is no reasonable expectation of privacy for such information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Social media are public websites. All users have access to their information through their user accounts. Individuals should consult the privacy policies of the services they subscribe to for more information.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Users may accidentally or purposefully generate inaccurate or erroneous information. There is no mechanism for correcting this. However, the community is largely self-governing and erroneous information is normally expunged or debated rather quickly by others within the community with more accurate and/or truthful information.

7.3 How are individuals notified of the procedures for correcting their information?

There is no specified procedure for correcting information; if there was, it relates to a social media provided process and not a DHS process. Individuals may change their PII on the sites as well as the accessibility of their content posts at any time they wish through their user account management tools on social media sites.

7.4 If no formal redress is provided, what alternatives are available to the individual?

There is no specified procedure for correcting information; if there was, it relates to a social media-provided process and not a DHS process. Individuals may change their PII as well as the accessibility of their content posts at any time they wish through their user account management tools on the social media sites. Individuals should consult the privacy policies of the services to which they subscribe for more information.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

The information available on social networking websites is largely user-generated, which means that the individual chooses the amount of information available about himself/herself as well as the ease with which it can be accessed by other users. Thus, the primary account holder should be able to redress any concerns through the third party host of the service. Individuals should consult the privacy policies of the services they subscribe to for more information.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

No procedures are in place. Social media sites are publicly available, third-party services.

8.2 Will Department contractors have access to the system?

Yes, as it is required in the performance of their duties at DHS.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All DHS employees and contractors are required to take annual privacy training.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

No.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

This PIA is effective for 30 days and will expire at that time. Should the requirements for the Initiative change before this expiration date, OPS and the Privacy Office will immediately update this PIA.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

These social media sites are publicly available, third-party services. Information is collected by the service itself to establish an account. Thereafter, users determine their level of involvement and decide how "visible" they wish their presence on any given service to be. The ability to choose how much information to disclose, as well as the short period of retention for any PII collected by the NOC, serve to mitigate any privacy risk.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology

9.1 What type of project is the program or system?

Third parties control and operate these services. Users should consult with representatives of the service provider in order to make themselves aware of technologies utilized by the system.

9.2 What stage of development is the system in and what project development lifecycle was used?

The Initiative is operational. Social media is third-party owned and operated.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

Individuals should consult the privacy policies of the services they subscribe to for more information.

Responsible Officials

Donald Triner
Director (Acting), National Operations Center
Office of Operations Coordination and Planning
Department of Homeland Security

Approval Signature

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX A

Examples of Social Media Web Sites Monitored by the NOC

This list is not comprehensive, but provides a list of the types of sites that the NOC is reviewing in order to improve its situational awareness and establish a common operating picture related to 2010 Winter Olympics in Vancouver, BC.

Social Approach	http://socialapproach.com/gov20
Go.usa.gov	http://go.usa.gov
WikiLeaks	http://wikileaks.org/
Cryptome	http://cryptome.org/
Google Blog Search	http://blogsearch.google.com
Technorati	http://technorati.com/
Foreign Policy Passport	http://blog.foreignpolicy.com/
Danger Room	http://www.wired.com/dangerroom/
Threat Level	http://www.wired.com/threatlevel/
Homeland Security Today	http://www.hstoday.us/
NTARC	http://www.nationalterroralert.com/
LA Now	http://latimesblogs.latimes.com/lanow/
NYTimes Lede Blog	http://thelede.blogs.nytimes.com/
STRATFOR	http://www.stratfor.com/
Drudge Report	http://drudgereport.com/
Huffington Post	http://huffingtonpost.com/
BNOnews	http://www.bnonews.com/
MEMRI	http://www.memri.org/
Informed Comment	http://www.juancole.com/
Homeland Security Watch	http://www.hlswatch.com/
Borderfire Report	http://www.borderfirereport.net/
Homeland Security Watch	http://www.hlswatch.com/
ABCNews Blotter	http://abcnews.go.com/Blotter/
WireUpdate	http://wireupdate.com/
RSSOwl	http://www.rssowl.org/
Twitter	http://twitter.com
NYTimes Rings Blog Vancouver Olympics 2010	http://vancouver2010.blogs.nytimes.com/
Vancouver City Blog	http://vancitybuzz.blogspot.com/
BBC Sports Olympics Blog	http://www.bbc.co.uk/blogs/olympics/
AOL News	http://www.aolnews.com/
Yahoo Fourth Place Medal Blog	http://sports.yahoo.com/olympics/vancouver/blog/fourth_place_medal
ESPN Winter Olympics Blog	http://espn.go.com/olympics/blog/_/name/winter olympics

Social Networking/Media Capability Privacy FAQ
Reference Document – 20 February 2010

What is PII?

Personally identifiable information is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. PII includes, but is not limited to full name, email address, mailing address, telephone numbers, credit card number, IP addresses, specific locations or other information that could identify a specific person. (analysts ref the chart on the wall)

What are you looking for?

- **Items of Interest (IOIs)** to fulfill NOC requirements: NOC Priorities, CIR (Critical Information Requirements), as well as identify potentially hazardous situations in order to alert operations center personnel

- **NOC Priorities:** (updated nightly)

- **NOC CIR's** include information and/or events that:
    - threaten DHS, other federal, state and local response units, facilities, and resources
    - impact on DHS capability to accomplish the HSPD-5 mission
    - have operational value...corroborating critical information
    - reflect adversely on DHS and response activities
    - involve standing HSC planning scenarios

- **NOC Interest Categories** that include 14 subjects, used as guidance for analysts to search for operationally relevant information in reporting

What do the analysts do when they encounter PII?

Under Normal Operations:

If relevant data is identified for further analysis, the PII is immediately deleted during the gathering process. To the extent that collected information contains PII, it will normally be in the form of user names of people who blog, or post, comments and messages on social networking sites. This PII, however, will not be saved, maintained or stored in any fashion by the SNMC. During Normal Operations, all PII, including but not limited to usernames, IDs, addresses or other information that could be linked back to a particular person, will be deleted from all reports before they are forwarded to the NOC. (analysts ref the chart on the wall)

Exceptional Operations

The following are examples of situations that trigger "exceptional operations" for the SNMC and include the collection of PII. (analysts ref the chart on the wall)

- "I'm John Doe, I'm trapped in my house at 4200 Wisconsin Ave and the flood water is rising. I need help!"

The example could be picked-up via searching,

If the SNMC receives a report from the public or observes messages posted publicly to the social networks containing PII that must be reported to the NOC, due to exceptional circumstances, it will not be stored in a searchable database where records can be retrieved by a person's name or other PII. The analyst will:

1. Report the event to a Senior Management and/or the NOC including PII,

2. Wait for confirmation that the NOC has received the information, then

3. Immediately delete the PII from all maintained records in the SNMC

The PII will be deleted within 24 hours of the time that the information was initially transmitted to the NOC even if confirmation from the NOC has not occurred. The remaining non-PII information will be stored for future reference. Once again, the stored information will not contain PII and therefore, could not be retrieved by reference to any PII. By design, SNMC reports will be searchable by reference to the date, type of incident and key words (e.g. Attack on federal building on 19 May 2009—key word: terrorism) and not by PII.

What sources do you use?

- The SNMC uses information provided by members of the public, first responders, the press, humanitarian organizations, and others on social media sites including online forums, blogs, public websites and message boards.
- The SNMC monitors mainstream social media sites such as Twitter, Flickr, and YouTube. The SNMC looks at a number of topical blog sites, and message boards.
- The SNMC only uses sources that are open to all public viewers, and where users voluntarily generate information.
- We do not search any sites that require us to have a user acct

Many media sources are using social networks to promote their stories and to get ahead of competitors. In some cases, reporters will post information to social networks as it occurs before they are able to write an article. Analysts will use sources such as Twitter to find that information.

Have the analysts implemented the SM/N CONOPs in a real world situation?

Yes, the analysts use the relevant guidance from the CONOPS daily as part of their work on the Watch supporting Haiti recovery and the 2010 Winter Olympics. Search operations and PII procedures are consistently followed.

What is a PIA?

A Privacy Impact Assessment (PIA) is an analysis of how personally identifiable information is collected, used, disseminated, and maintained. It examines how the Department has incorporated privacy concerns throughout the development, design, and deployment of a technology or rulemaking. "Personally identifiable information" is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

The PIA is one of the most important instruments through which the Department establishes public trust in its operations. Section 208 of the E-Government Act of 2002 requires all federal government agencies to conduct PIAs for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information.

How do the SM/N analysts structure their searches to fulfill the NOC information requirements?

- Structured Searches targeted at:
  - NOC CIRs and NOC Priorities
  - 14 Item of Interest Categorizations
- IOI Categorizations:
  - Terrorism
  - Weather/Natural Disaster/Emergency Management
  - Fire
  - Trafficking/Border Control Issues
  - Immigration
  - HAZMAT
  - Nuclear

        - Transportation Security
        - Infrastructure
        - National/International Security
        - Health Concerns, National/International
        - Public Safety
        - Reports on DHS, Components, and other federal agencies
        - Cyber Security

    - Methodology:
        - **Utilize multiple means of gathering information for distribution**

        - **During normal operations** – scan media websites for items of interest, searching for information on a current NOC Priorities or National Operations Center's Critical Information Requirement and fulfill one the 14 categories.

            - Utilize tools such as Meltwater and RSS Owl which search thousands of media sources for articles that match a predetermined set of Keywords or phrases. These programs sort individual articles into organized watch folders making it easy for analysts to scan hundreds of articles in a particularly short timeframe.

            - Monitor at least two live television broadcasts for breaking news stories

        - **When the NOC is actively tracking a situation or specifically seeking information on a specific topic** – key words or terms associated with that Issue are used In conjunctlon wlth Internet news browsers llke Google News, Yahoo News, Netscape, and AOL News to locate syndicated new items across a wide range of news sources. This method is extremely useful when information on a specific issue or incident is required.

What Type of Coverage does the SNMC Provide?

- 24 hour/7 coverage
- Surge capacity during incidents, significant events, and crisis

How do you communicate with the NOC?

- HSIN (b) (7)(E)
- Telephone
- Email distribution list

Who controls the distribution list?
Don Triner (DHS/OPS Current Ops Branch Chief)

NOC Media Monitoring Capability (MMC)
Social Networking/Media Analysts

Initial Training Completion Matrix

NAME	Date Stated	Completed	Status
[redacted]	[redacted]	[redacted]	[redacted]

(b) (6)

SNMC
Training Plan

DHS OPS Social Networking and Media Capability

TechOp Solutions International, Inc.

Version 10
31 December, 2009
2200 hours

TRAINING PARAMETERS	
Item	**Parameter**
Type of Staff to be Trained	New SNMC Staff
Type of Training	SNMC 101
Amount of Time Allotted	10 days **(Jan.4-8, 11-15 with option to extend to 18-22)**
Number of Training Sites	one
Number of Classrooms	one
Number of Trainees	1
Number of Trainers	Two
Length of Each Session	8 hours
Recommended Classroom Size	10
Amount of Equipment	1 laptop, projector, printer
Travel Time and Holidays	None
Special Circumstances	Training must be completed before Jan 25, 2009

1. INTRODUCTION

1.1 Assumptions

The training strategies, activities, and methods are predicated upon the following assumptions:

- A laptop will be provided to each analyst for training and shift work
- New staff will have a working knowledge of XP-based PCs, Microsoft Office and web browsers
- The only stupid questions are the ones not asked

1.2 Goals of the Training Plan

The goals of the training plan are to:

- Provide new staff with an understanding of the role of the SNMC, and provide continual refinement and training for current staff.
- Educate new staff about the issues regarding monitoring and engagement on behalf of DHS and the policies of the SNMC
- How the SNMC works with the Media Monitoring Center (MMC)
- Train new staff in the processes and procedures of monitoring social networks and media
- Train new staff to properly handle personally identifiable information

1.3 Overview of the Training Plan

This document defines the Training Plan for the Department of Homeland Security's OPS/NOC Social Networking / Media Capability. The Training Plan is a working document. It is revised on a continuous basis as decisions are made and issues are resolved. The document is organized as follows:

· Training Scope: Clearly states a list of the objectives and goals of the training, as well as a list of assumptions.

· Training Offerings: Describes the offerings that define the training, including the training groups, types of training, training approach, training curricula, training schedule, and logistical information.

· Roles and Responsibilities: Presents the roles and responsibilities of the staff responsible for preparing, conducting, and evaluating the training, and includes a clear definition of the resources and a work plan.

· Contingency Plan: Identifies anticipated contingencies and details a plan for each contingency.

· Training Material Design, Standards, and Guidelines: A copy of the Training Material Design, Standards, and Guidelines that will be used to prepare the training materials.

2. TRAINING SCOPE

2.1 Training Goals and Objectives

The objectives of the training are:

- Completion of an 8 day training period
- Introduction to the SNMC and its relationship with the MMC and DHS OPS/NOC
- Familiarization with the Department of Homeland Security components and leadership
- Familiarization with the 24/7 schedule and shift Battle Rhythm
- Familiarization with software and technologies utilized by the SNMC
- Knowledge of processes and software tools involved in monitoring social networks
- Awareness of the issues surrounding Personally Identifiable Information (PII)
- Efficient use of the Critical Information Requirements (CIRs) and Trend Analysis Requirements
- Creation of the Items of Interest (IOIs), Daily Summary, Logs and the Operational Summary
- Develop an understanding of "exceptional" circumstances and the handling of PII in those cases
- Understanding the SNMC policies regarding personal vs. company accounts/identities
  - o Safeguarding SNMC social networking presences, applications and widgets
- Team operation, coordination and innovation from the same understandings and directives

To achieve these objectives, the following goals are established:

- Describe the mission of the SNMC
- Present the trainees with information on DHS structure and personnel
    - Have trainees do research on DHS organizational structure
- Explain and give examples and practice with Personally Identifiable Information and the SNMC's PII policies
- Learn the Director's Criterion, Critical Information Requirements, and Trend Analysis Requirements
- Instruct the staff on the daily Battle Rhythm and 24/7 shift schedule
- Describe the coordination of the team
- Educate new staff on the processes and sensitivities of monitoring social networks
- Demonstrate the components of the SNMC watch desk
- Train new staff in the use of technologies and software to aid in the mission of the SNMC
- Familiarize and train the analysts on the Apple Mac Mini and Dell laptops
- Exercise the use of tools and processes to produce and log Items of Interest
- Explain the differences and between Regular and Exceptional events
- Outline policy on use of personal and company accounts and identities
- Development, refinement and improvement of processes over time

3. TRAINING

3.1 Training Logistics

This section identifies logistical information based on the requirements for the defined training offerings. The logistical information includes a list of the equipment and supplies required.

3.1.1 Analyst Trainee

- Laptop for each analyst
- Documents
    - CONOPS (draft)
    - PIA (draft)
    - Implementation Plan (draft)
    - Standard Operating Procedures (draft)

3.1.2 Trainer Needs

- Computer with internet access
- Whiteboard
    - Markers
- Handouts
    - Critique/Comment Forms (and other ref materials given to the participants, e.g., Binders.

4. ROLES AND RESPONSIBILITIES

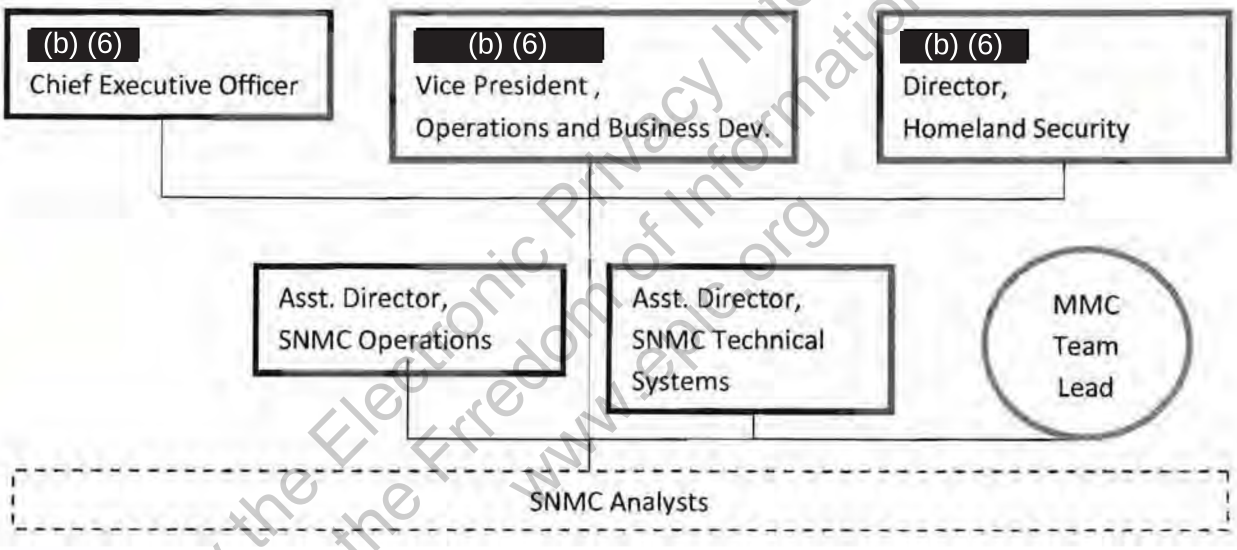
This section details the roles and responsibilities of the personnel responsible for preparing, conducting, and evaluating the training for *** *System Name* ***.

4.1 Resources

SNMC Team Leads will be leading the training for the new analysts. One will lead a section, but will work in tandem together to address all the training materials and objectives. Senior Staff will make introductions and get us started, in addition to providing ongoing input and perspective during training.

This section describes the roles of those involved, the individuals who will fulfill the roles, and their area of responsibility.

Training Team Structure



5. TRAINING CURRICULUM and SCHEDULE

TRAINING CURRICULUM 2009						
Type of Training: System Overview						
Date	**Topic**	**Description**	**Objectives**	**Time**	**Method/Medium**	**Instructor**
1/4	**HR Orientation**	VP of HR and Dir. Homeland Security will give new hire briefing	To ensure trainees are acquainted with employee benefits and procedures	1000-1130	Meeting in Director's office	VP, Human Resources
1/4	**Office Orientation**	Tours of office facility, bathrooms, kitchen, watch office and project offices				
1/5	**Training Process**	Introduce instructors, general information, (e.g., location of rest rooms), define training roles and responsibilities, and review the agenda.	To ensure trainees are familiar with training logistics, their role and the instructor's role, and the material that will be covered.	1300-1315	classroom training / in-person lecture	Asst. Dir., SNMC Operations or Dir. Homeland Security for TSI
1/5	**Training Objectives**	Review the objectives of the system overview training.	To ensure trainees understand the desired effect of the training.	1315-1345	classroom training / in-person lecture, (transparencies)	Asst. Dir., SNMC Operations or Dir. Homeland Security for TSI

1/5	**Introduction to the SNMC and its relationship with the MMC and DHS OPS/NOC**	Why does the SNMC exist, where did the idea come from and how does this fit within DHS OPS/NOC?	Help new analysts become familiar with the mission and goals of the SNMC within then broader picture of MMC and DHS OPS/NOC.	1345-1445	classroom training / in-person lecture	Asst. Dir., SNMC Operations or Dir. Homeland Security for TSI
1/5	**Watch Desk – Computers and Software**	Where is the SNMC and what equipment and software does it use?	To familiarize the analysts with the equipment and software they will be using during their shifts.	1500-1600	On site view	Asst. Dir., SNMC Technical Systems
1/5	**Basic Tool Set-up on Analyst Computers**	Instruction to download and install some of the basic SN tools for monitoring and analysis.	To ensure that each analyst has the approved basic tools on their laptop for work.	1600-1700	On site instruction and classroom training	Asst. Dir., SNMC Technical Systems
1/6	**Daily Objectives Brief**	Review of previous day's topics and briefing of the topics to be covered today.	Opportunity for analysts to ask questions and be refreshed on previous topics.	0800-0815	Classroom training	Asst. Dir., SNMC Operations and Asst. Dir., SNMC Technical Systems
1/6	**The Battle Rhythm and You**	How will each shift work and what tasks and objectives will need to be completed?	To ensure what is expected of the analysts while on shift.	0815-1015	classroom training / in-person lecture, with examples	Asst. Dir., SNMC Operations and Asst. Dir., SNMC Technical Systems

1/6	**Privacy Impact Assessments and How They Drive What We Do**	In-depth discussion of Privacy Impact Assessments	Describe the importance of privacy in our operations. Provide valuable background for operations with the OPS/NOC.	1015-1215	classroom training / in-person lecture reading and understanding materials	Asst. Dir., SNMC Operations or Dir. Homeland Security for TSI
1/6	**Lunch**			1215-1330		
1/6	**CIRs and TARs: What do they mean?**	What will an analyst be using as criteria for doing their job?	To ensure analysts know what the requirements are for monitoring, collecting information and reporting to the NOC.	1330-1600	classroom training / on-line exercises	MMC Team Lead and Asst. Dir., SNMC Operations
1/7	**Daily Objectives Brief**	Review of previous day's topics and briefing of the topics to be covered today.	Opportunity for analysts to ask questions and be refreshed on previous topics.	0800-0815	Classroom training	Asst. Dir., SNMC Operations and Asst. Dir., SNMC Technical Systems
1/7	**Personally Identifiable Information (PII)**	What is PII and why should SNMC analysts care? How do we protect privacy while doing our job?	To ensure analysts know the process and procedures for deleting PII during the collection process during "normal operations."	0815-1015	classroom training / in-person lecture, with examples	Asst. Dir., SNMC Operations and Asst. Dir., SNMC Technical Systems

1/7	**Exceptional Circumstances and Handling of PII**	What are the exceptions to when SNMC is allowed to report PII to the NOC?	To ensure the analysts know the process, procedures and rules for collecting and reporting items that contain PII and how to properly dispose of it when the NOC no longer needs it.	1100-1200	classroom training/ in-person lecture,	Asst. Dir., SNMC Operations and Asst. Dir., SNMC Technical Systems
1/7	**SNMC Vision**	TSI CEO and DHS Senior Advisor to present SNMC vision and take questions.	Opportunity for analysts to hear the vision of the SNMC's purpose from senior leadership.	1245-1315	Classroom lecture	TSI CEO and DHS Senior Advisor
1/7	**DHS and OPS NOC Leadership**	Analysts research biographical information, including photos to develop organizational placards for office. Prepare to present information to TSI senior staff.	To familiarize analysts with our client's leadership and their positions within the DHS organizational structure.	1315-1500	Classroom research and development	Asst. Dir., SNMC Operations
1/7	**SNMC Binders**	Analysts construct office binders as a resource and opportunity to learn the following: 1. Privacy Binder	To familiarize analysts through research and activities the important information and resources	1500-1700	Classroom research and development	Asst. Dir., SNMC Operations

		2. DHS Org/leadership 3. SNMC Operations 4. TSI Contacts	needed to stand watch.			
1/8	**Daily Objectives Brief**	Review of previous day's topics and briefing of the topics to be covered today.	Opportunity for analysts to ask questions and be refreshed on previous topics.	0800-0815	Classroom training	Asst. Dir., SNMC Operations and Asst. Dir., SNMC Technical Systems
1/8	**Continuation of previous days research projects**			0815-0930	Classroom research and development	Asst. Dir., SNMC Operations and Asst. Dir., SNMC Technical Systems
1/8	**PART 1: Building Items of Interest, Logs and the Operational Summary**	How does an analyst report what they find to the NOC?	Familiarize and ensure how to fill-out a reporting template.	0930-1230	classroom training/ in-person lecture,	Asst. Dir., SNMC Operations and Asst. Dir., SNMC Technical Systems
1/8	**Lunch**			1230-1315		
1/8	**Use of Personal vs. Company Equipment**	What are the protocols for using personal vs. company equipment	To ensure the analyst knows the rules for using personal and company equipment and how to protect them.	1315-1415	classroom training/ in-person lecture,	Asst. Dir., SNMC Technical Systems
1/8	**Additional setting-up and Logging-in to company tools**	Inform the SN analysts which tools to be used. ie. Firefox, MS Office	To ensure all the SN analysts have the same tools	1415-1530	Classroom instruction and help from the instructors	Asst. Dir., SNMC Technical Systems

		accounts and preferences.				
1/8	**The Sensitive Nature of Monitoring and Engaging with the Public**	Why must SNMC analysts protect what we do? And what that could mean in a climate that is skeptical of government? How do we protect the accounts from hackers?	To ensure the analyst has an understanding of the risks and procedures involved in operating a social networking monitoring program for DHS.	1530-1600	classroom training/ in-person lecture,	Asst. Dir., SNMC Operations and Asst. Dir., SNMC Technical Systems
1/8	**PART 2: Refining the building Items of Interest, NSS/ISS, Logs, Operational Summary – Plus Turnover Summary**	Further refining and developing how an analyst reports what they find to the NOC.	Familiarize and ensure how to fill-out a reporting template.	1600-1630	classroom training/ in-person lecture,	Asst. Dir., SNMC Operations and Asst. Dir., SNMC Technical Systems
1/11	**Daily Objectives Brief**	Review of previous day's topics and briefing of the topics to be covered today.	Opportunity for analysts to ask questions and be refreshed on previous topics.	0800-0815	Classroom training	Asst. Dir., SNMC Operations and Asst. Dir., SNMC Technical Systems

1/11	**Part 2: Media Monitoring Center (MMC) Overview -**	Presentation of what and how the MMC operates: NOC Notes, Blast Calls, Steady States, OPSUMs plus tricks and tips for working with the NOC.	To help analysts understand the role of the MMC and how the SNMC will compliment their mission, plus learning from their experiences.	0815-0915	in-person lecture	MMC Team Lead
1/11	**NOC Concept of Operations and Standard Operating Procedures**			0915-1045		DHS NOC Operations Officer
1/11	**Crisis Operations...CAT Process, CAT Teams, CAT reporting (SITREPs and Senior Leadership Briefs), SLG Calls**			1045-1215		DHS Deputy Dir., Future Operations
1/11	**Lunch**			1215-1330		
1/11	**DHS mission, organization, offices, operating components, and key authorities**			1330-1430	in-person lecture	Director of Information Sharing

1/11	**DHS Operations (OPS) mission, organization and key elements – HSIN and COP**			1430-1530	in-person lecture	Director of Information Sharing/Dir. of Continuity
1/11	**Hurricanes, H1N1, IND/RDD, white powder events, terrorist acts**			1530-1615		Dir. of Continuity
1/12	**Daily Objectives Brief**	Review of previous day's topics and briefing of the topics to be covered today.	Opportunity for analysts to ask questions and be refreshed on previous topics.	0800-0815	Classroom training	Asst. Dir., SNMC Operations and Asst. Dir., SNMC Technical Systems

1/12	**Part 3: Exercise – Monitor, Create IOIs, Logs and OPSUMs**	Final Drafts.	To ensure all analysts are comfortable with the battle rhythm process and reporting templates.	0815-1200	In class project	Asst. Dir., SNMC Operations and Asst. Dir., SNMC Technical Systems
1/12	**Left-overs: Finish up any outstanding projects – Org Charts, Binders, etc…**	Finish projects for review.	Learning by doing and possibly presenting the information to senior leadership.	1300-1600	In class project	Asst. Dir., SNMC Operations and Asst. Dir., SNMC Technical Systems
1/13-1/15	**Mock Watch Sessions**	Utilizing tools for real-time monitoring of the Social Networks, running through the shift battle rhythm.	To ensure all SN analysts are comfortable with developing IOIs, OPSUMs, Exceptional Items, Change Over Summaries and working through the shift requirements, before being signed off for shift duty.	2 days	classroom training and online exercises	TSI Senior Staff and Asst. Dir., SNMC Operations and Asst. Dir., SNMC Technical Systems

Social Networking/Media Capability Mission Statement

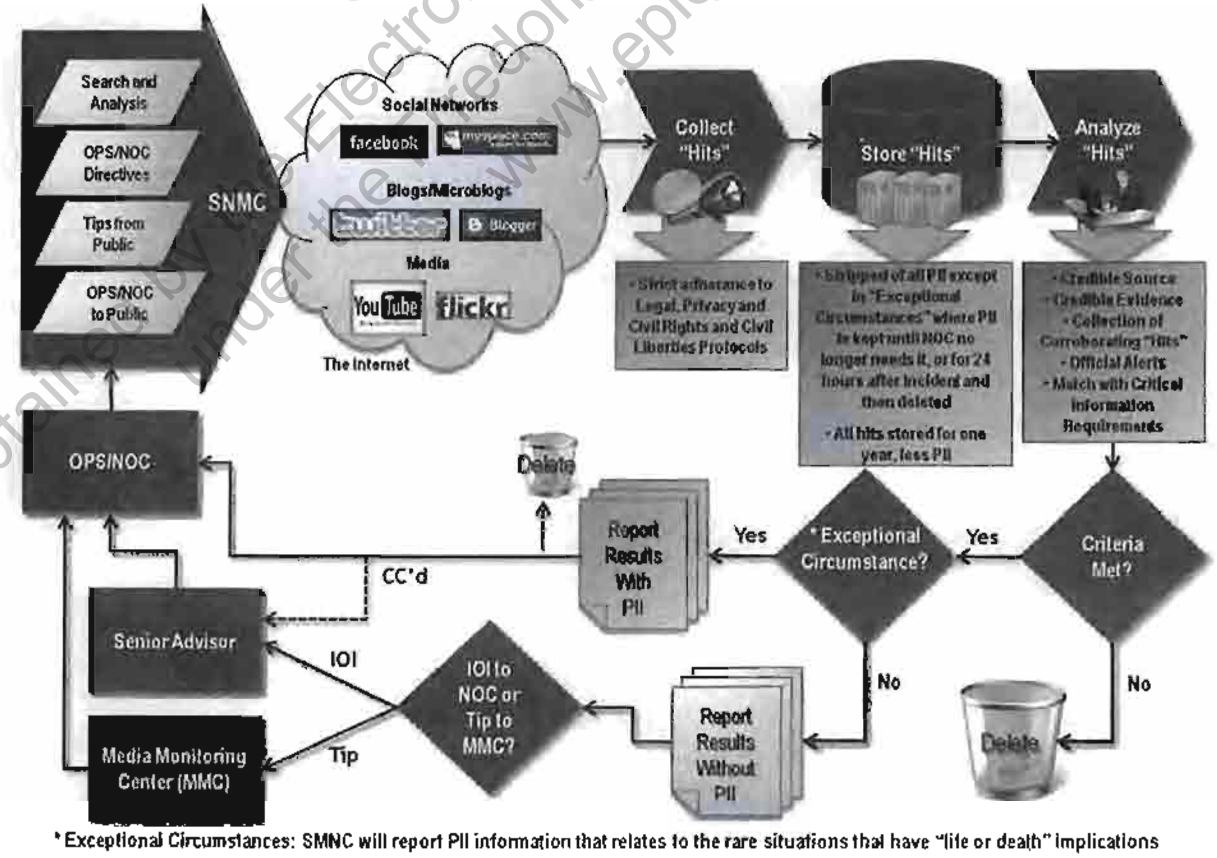
The SNMC has three primary missions:

Enhance situational awareness by continuously searching social networking sites for NOC Critical Information Requirements (CIRs).

Establish a presence on social networking sites to provide important information to the public regarding DHS NOC operations and alerts in order to assist the public in preparing for and mitigating the effects of natural and man-made disasters.

Facilitate the public's desire to knowingly submit operationally relevant information and interact with DHS Operations and the NOC.

Social Networking / Media Capability Process


Search and Analysis
OPS/NOC Directives
Tips from Public
OPS/NOC to Public
SNMC
Social Networks
facebook
myspace.com
Blogs/Microblogs
twitter
Blogger
Media
YouTube
flickr
The Internet
Collect "Hits"
Store "Hits"
Analyze "Hits"
• Strict adherance to Legal, Privacy and Civil Rights and Civil Liberties Protocols
• Stripped of all PII except in "Exceptional Circumstances" where PII is kept until NOC no longer needs it, or for 24 hours after incident and then deleted
• All hits stored for one year, less PII
• Credible Source
• Credible Evidence
• Collection of Corroborating "Hits"
• Official Alerts
• Match with Critical Information Requirements
Criteria Met?
Yes
No
* Exceptional Circumstance?
Yes
No
Report Results With PII
Delete
CC'd
Report Results Without PII
Delete
IOI to NOC or Tip to MMC?
IOI
Tip
OPS/NOC
Senior Advisor
Media Monitoring Center (MMC)

* Exceptional Circumstances: SMNC will report PII information that relates to the rare situations that have "life or death" implications

Critical Information Requirements

Critical Information Requirements (CIR) below are utilized as the mechanism for MMC/SNMC collection, processing, and distributions efforts.

1. **Potential threat to DHS, other federal, state and local response units, facilities, and resources**
   - A. Learning that something has occurred
   - B. Collecting operational data, information, and imagery

2. **Potential impact on DHS capability to accomplish the HSPD-5 mission**
   - A. Corroborating/reconciling reports
   - B. Threatens DHS and other response units, facilities, or supporting activities
   - C. Present unique demands on low density – high demand assets

3. **Identifying events with operational value…corroborating critical information**
   - A. Collecting imagery not otherwise available
   - B. Identifying operational factors that may impact DHS capabilities
   - C. Analyzing the effectiveness of response activities

4. **Identifying media reports that reflect adversely on DHS and response activities**
   - A. Identifying gaps in the response
   - B. Identifying inaccurate and/or incomplete media reports

5. **Standing HSC planning scenarios**

DO NOT STORE
PERSONALLY IDENTIFIABLE INFORMATION (PII)!

What is PII?

- Names
- Email Addresses
- Mailing Addresses
- Telephone Numbers
- Usernames
- Photos
- Specific Locations
- Credit Card Number
- IP Addresses and URL's
- Other PII

CNNReporter: Joe Smith, a student at GW has guns, has taken hostages, and is making demands *about 3 minutes ago from web*

- **No PII issue because the info was obtained from a media news report.**

Jazz42: Bob Doe and I saw a plane crash into an appt bldg at 9 Downing St, in Baltimore *about 3 minutes ago from web*

- **Bob Doe would be stripped as PII, before the data is stored or shared**

Exceptional Operations – Examples of "life or death" incidents picked up via searches or because it was posted to a DHS widget or link for the public to provide information:

JohnDoe: I'm trapped in my house at 4200 Wisconsin Ave and the flood water is rising. I need help!! *about 3 minutes ago from web*

or

JaneDoe: just watched 10 guys in masks with guns and backpacks run into the Marriott Hotel in St Louis *about 3 minutes ago from web*

Exceptional PII Handling:

Only essential PII is included in report to NOC, then deleted immediately upon NOC confirmation of receipt; or deleted within 24 hours if no confirmation is received. Either way, PII is never entered into a database.

Item of Interest Categorization

1. Terrorism: Media reports on the activities of terrorist organizations both in the United States as well as abroad. This category will also cover media articles that report on the threats, media releases by al Qaeda and other organizations, killing, capture, and identification of terror leaders and/or cells.

2. Weather/Natural Disasters/Emergency Management: Media reports on emergency and disaster management related issues. Reports include hurricanes, tornadoes, flooding, earthquakes, winter weather, etc. (all hazards). Reports will outline the tracking of weather systems, reports on response and recovery operations, as well as the damage, costs, and effects associated with emergencies and disasters by area.

3. Fire: Reports on the ignition, spread, response, and containment of wildfires/industrial fires/explosions regardless of source.

4. Trafficking/Border Control Issues: Reports on the trafficking of narcotics, people, weapons, and goods into and out of the United States of an exceptional level. Reports will also include articles outlining the strategy changes by Agencies involved in the interdiction of the items outlined above.

5. Immigration: Reports on the apprehension of illegal immigrants, policy changes with regard to immigration in the United States, and border control issues.

6. HAZMAT: Reports on the discharge of chemical, biological, and radiological hazardous materials as well as security and procedural incidents at nuclear facilities around the world, and potential threats toward nuclear facilities in the United States. Also included under this category will be reports and response to suspicious powder and chemical or biological agents.

7. Nuclear: Reports on international nuclear developments, attempts to obtain nuclear materials by terrorist organizations, and stateside occurrences such as melt downs, the mismanagement of nuclear weapons, releases of radioactive materials, illegal transport of nuclear materials, obtaining of weapons by terrorist organizations, and breaches in nuclear security protocol.

8. Transportation Security: Reports on security breaches, airport procedures, and other transportation related issues, and any of the above issues that affect transportation. Reports will include threats toward and incidents involving rail, air, road, and water transit in the United States.

9. Infrastructure: Reports on national infrastructure including key assets and technical structures. Reports will include articles related to failures or attacks on transportation networks, telecommunications/ internet networks, energy grids, utilities, finance, domestic food and agriculture, government facilities, and public health, as well as those listed above.

10. National/International Security: Reports on threats or actions taken against United States national interests both at home and abroad.

11. Health Concerns, National/International: Articles on national and international outbreaks of infectious diseases and recalls of food or other items deemed dangerous to the public health.

12. Public Safety: Reports on public safety incidents, building lockdowns, bomb threats, mass shootings, and building evacuations.

13. Reports on DHS, Components, and other Federal Agencies: Positive and negative reports on FEMA, CIA, CBP, ICE, etc. as well as organizations outside of DHS.

14. Cyber Security: Reports on cyber security matters that could have a national impact on other CIR Categories; internet trends affecting DHS missions such as cyber attacks, computer viruses; computer tools and techniques that could thwart local, state and federal law enforcement; use of IT and the internet for terrorism, crime or drug-trafficking; and Emergency Management use of social media strategies and tools that aid or affect communications and management of crises.

Trend Analysis Requirements

1. Credible Source (media-linked reporter or expert)

2. Credible Evidence (photo, video, audio)

3. Collection of corroborating “hits” indicating a trend (posts, observations and opinions from multiple sources)

4. Official Alerts (local, state, national, NGO)

Must meet at least one of the requirements to be a candidate for match with DHS Critical Information Requirements (CIRs). If matched the SN “Hit” becomes a potential “Item of Interest” (IOI) or a “Tip” that runs through MMC to DHS OPS/NOC.

Social Networking/Media Capability

Resources for Privacy Issues

(Refer to Separate Binder)

February 2010

Table of Contents

Social Networking/Media Capability
Resources for Privacy Issues
February 2010

Table of Contents

Social Networking/Media Capability (SNMC)
Battle Rhythm

Version 11
23March 2011

Battle Rhythm for Watch Analysts

1. Review and Sign-Off of the Changeover Briefing

- This is a synopsis of the previous shift and will aid the oncoming analyst to continue operations without any substantial break in reporting. The following will be the search priorities for each analyst for every shift, including but not limited to:
    - All items from the latest NOC Priorities and Monitoring Report including: (sent via email – make sure you are receiving them)
        - Any active National Situation Summaries (NSS)
        - International Situation Summaries (ISS)
        - Steady-State incidents
        - Events of high media interest
        - Current requests for information from the NOC Watch Team, DHS Senior Staff Requests and any additional instructions for the next shift
    - Selected items from the MMC Operational Summary (OPSUM)
    - TSI Management Notes/Directives/Instructions
    - Watch Analyst's Notes/Questions/Instructions including:
        - Hashtags, links and keywords (No PII) that are being used for events/incidents that would be helpful to the next analyst
- Review the SNMC Changeover with the analyst going off-duty and then signoff that you understand what occurred in the previous shift, any new directives and directions
- Perform all relevant checks on office equipment to ensure things are working properly
    - If a problem is detected, then do the following:
        - Work with the MMC analyst to find a solution
        - If you need call technical support, call (b) (6)
        - Send email to (b) (6) summarizing the problem
- Check Outlook - The previous analyst will have saved the Changeover on the T: Drive and the SNMC daily log on Google Docs. Review the daily log and previously distributed SN Guardian Information Reports (GIRs) and Exceptional Items

2. Check in with MMC Watch Analyst

- Review the MMC's Changeover Briefing
- Participate with MMC watch analyst on the call to the KMO, receive any special instructions and note all in the Daily log

- Participate in all Blast Calls from the NOC
- Ask if there are any incidents they need help researching
    - Media Sources
    - Social Networks

3. Login to NOC Watch room on HSIN over Jabber

- Need to have HSIN account access, which will be arranged by your team lead
    - An email with registration instructions to both HSIN and Jabber will be sent to analyst upon initial training
- Start the Jabber program and join the NOC Watch channel
- Communication with other watch standers
    - Provide only information that contributes to the situational awareness of the NOC
    - No chit – chat, obscene language or jokes
    - Respond immediately to requests from the NOC
    - If a request is beyond normal watch duties, contact Brad Duty or a team lead for guidance immediately
- Remain logged in during your shift

4. Login into the combined MMC/SN Daily Log, the Clip Board and the IOI App

- Combined Daily Log – Lists all the IOIs and any notes made by the analysts during shift
    - Read any notes left from the last shift, highlighted in Yellow
    - Use the log as another way to check to see if the IOI you are writing has already been done or could be used as an update to a previous IOI
- Clip Board – Used to build IOI drafts for peer review before being sent to the NOC distribution list(s)
    - Clear the Clip Board of any leftover IOI drafts
    - Use the Clip Board to build new IOI drafts to be reviewed by your MMC counterpart
    - Check for spelling, grammar, content and PII; including the links
- IOI App – Used for sending IOIs to the distribution list(s)

5. Access SN Tools and enter relevant search terms

- Using relevant keywords from current incidents and trends, the 14 NOC Critical Information Requirement (CIR) categories and the most recent "Approved Key Words - Based on General PIA", the SNMC will search for Items of Interest that provide situational awareness to the NOC
- Access TweetDeck:
    - Under the granted PIA, one of our primary tools is TweetDeck. TweetDeck is loaded on the Apple Mac Mini on the SN watch desk, and on analysts' laptops
        - TweetDeck on the Mac Mini and analyst's laptops will be configured with only SNMC approved social networking accounts

        - No personal accounts will be configured for use on TSI-owned computers. Likewise, no general SNMC accounts will be configured or used on personal laptops
        - TweetDeck **will not** be used to post ANY information to social networks, unless it is directed by senior leaders. **You will not engage the public or respond to any requests from the public.** ***Doing so without authorization is grounds for termination.***
    - TweetDeck should be scanned regularly to identify breaking news/incidents relating to our mission

- Use the keywords and Twitter Search tabs on the Firefox browser on the Apple Mac Mini to scan for current reportable incidents
    - Make sure all the key words searches are there for your shift
        - Work your way across all the search tabs
    - Access other Twitter search tools for deeper dives on topics:
        - Twitter Search: http://search.twitter.com
        - Twazzup: http://www.twazzup.com
        - Tweetgrid: http://www.tweetgrid.com
        - Trendsmap: http://www.trendsmap.com
- Access Picture/Video search tools
    - PicFog: http://www.picfog.com
    - TwitCaps: http://www.twitcaps.com
    - Flickr: http://www.flickr.com
    - PhotoBucket: http://www.photobucket.com
    - YouTube: http://www.youtube.com
    - Yahoo Video: http://www.yahoo.com
- Open up or continue running SN tools that are on the Mac mini. Login instructions are located on a sticky note attached to the bottom of the Mac
    - Username: Admin
    - Password: (b) (7)(E)
    - Clear the cache on the Mac's web browser both before and after your shift; current settings automatically do most of this for you
- Login to Shrook/RSS Owl or one of the other RSS readers and scan RSS feeds
    - Scan through all the different folders to check for any leads for IOIs
    - Click the Read function under Tools to mark items as you go to better keep track of new information
- Test television video switch settings by logging on to video switch site. 'Output Four' is the designated SNMC screen and should be adjusted so that either the extended desktop on the Mac or laptop is shown while on watch. 'SNEXT' corresponds with the extended desktop monitor for the laptop and 'SNMAC' corresponds with the Apple Mac Mini

- http://192.168.1.195/ content_switch.html
  - Username: Administrator
  - Password: (b) (7)(E)

6. Searching

6.1 Full Initial Sweep of First Tier Social Network Sites (see First Tier List)

- Begin your search for emerging news stories and/or coverage of active situations. A recommended scan process is as follows:
  - Determine what information was previously distributed (read and analyze prior SN Tips and IOIs). Focus on the previous 24 hours but have a working knowledge of the previous 5 days
  - Keep an eye on live social networking streams on Twitter using TweetDeck, Twazzup, TweetGrid, or one of the other tools on the Mac
  - Run through the RSS reader list of sites
  - Utilize search tools available on each site in an attempt to locate stories pertaining to items such as Homeland Security, DHS, terrorism, weather, or other items of focus
    - Use the Key Words list (See "Approved Key Words - Based on General PIA" in Training folder)
    - Search terms based on current events/incidents, Changeover Briefing, CIRs and OPSUM
    - Repeat this process for Tier 2 and 3 social networking sites
- Review the Change-Over/OPSUM and all other items in sections 1 and 2 of the Battle Rhythm and cycle through and search each of those priorities at least once every couple of hours
- Employ use of Boolean logic, usage of "OR", "AND" and "FROM:" to make searches more efficient. Examples:
  - arrested OR arrests OR arrest
  - "dirty bomb" OR "nuclear bomb" OR nuke FROM:cnn
  - Operators such as "OR", "AND" and "FROM:" must be capitalized for most search tools/engines
- Search and give tips to MMC based on CIRs
- Do follow-up research on Trend Analysis Directives

6.1.1 Tracking developing events on Social Media: Examples

- Establish which Hashtags and keywords are being used by the public, note in Change Over and emails to teammates when possible
- Search Twitter, Youtube and Flickr
- Search blogs via Google Blogsearch, Google News

- Watch Wikipedia entries on the topic for changes
- (See Section 8.0 and 8.1 for a complete list)

- For additional granularity: dig into second and third tier social networking sites or specific niche sites

7. Battle Rhythm for Project Time Analysts

- Check-in with SNMC Watch Analyst
- Support the SNMC Watch Analyst
- Research trends
- Update OPS/NOC SNMC managed web sites, social network applications and widgets
- Develop SNMC Trend Reports as directed by OPS/NOC (See SNMC Trend Reports section)
- Research and help manage ongoing development efforts to improve monitoring and public engagement/involvement projects

8. Appendices

8.1 Social Media Web Sites Monitored by the NOC's MMC-SN Desk

This is a representative list of sites that the NOC's MMC-SN Desk will start to monitor in order to provide situational awareness and establish a common operating picture under this Initiative. Initial sites listed may link to other sites not listed. The NOC's MMC-SN Desk may also monitor those sites if they are within the scope of this Initiative.

This list is based on Appendix A of the "Publicly Available Social Media Monitoring and Situational Awareness Initiative" PIA, dated June 22, 2010.

Tool	**Link**	**User/Password Required**
General Search		
Collecta	http://collecta.com	No
RSSOwl	http://www.rssowl.org/	No
Social Mention	http://socialmention.com/	No
Spy	http://www.spy.appspot.com	No
Who's Talkin	http://www.whostalkin.com/	No
Shrook RSS reader	http://www.utsire.com/shrook/	No
Video		
Hulu	http://www.hulu.com	No
iReport.com	http://www.ireport.com/	No
Live Leak	http://www.liveleak.com/	No
Magma	http://mag.ma/	No
Time Tube	http://www.dipity.com/mashups/timetube	No

Vimeo	http://www.vimeo.com	No
Youtube	http://www.youtube.com	No
MySpace Video	http://vids.myspace.com/	No
Maps		
Global Incident Map	http://globalincidentmap.com/	No
Google Flu Trends	http://www.google.org/flutrends/	No
Health Map	http://www.healthmap.org/en	No
IBISEYE	http://www.ibiseye.com/	No
Stormpulse	http://www.stormpulse.com/	No
Trends Map	http://www.trendsmap.com	No
Photos		
Flickr	http://www.flickr.com/	No
Picfog	http://picfog.com/	No
Twicsy	http://www.twicsy.com	No
Twitcaps	http://www.twitcaps.com	No
Twitter/API		
Twitter/API	http://www.twitter.com	Yes
Twitter Search		
Monitter	http://www.monitter.com/	No
Twazzup	http://www.twazzup.com	No
Tweefind	http://www.tweefind.com/	No
Tweetgrid	http://tweetgrid.com/	No
Tweetzi	http://tweetzi.com/	No
Twitter Search	http://search.twitter.com/advanced	No
Twitter Trends		
Newspapers on Twitter	http://www.newspapersontwitter.com/	No
Radio on Twitter	http://www.radioontwitter.com/	No
Trendistic	http://trendistic.com/	No
Trendrr	http://www.trendrr.com/	No
TV on Twitter	http://www.tvontwitter.com/	No
Tweet Meme	http://tweetmeme.com/	No
TweetStats	http://tweetstats.com/	No
Twellow	http://www.twellow.com/	No
Twendz	http://twendz.waggeneredstrom.com/	No
Twitoaster	http://twitoaster.com/	No
Twitscoop	http://www.twitscoop.com/	No
Twitturly	http://twitturly.com/	No
We Follow	http://wefollow.com/	No
Facebook		
It's Trending	http://www.itstrending.com/news/	No
Facebook	http://www.facebook.com	Yes
	http://www.myspace.com	Yes
MySpace		
MySpace (limited search)	http://www.myspace.com	No
Blogs Aggs		
ABCNews Blotter	http://abcnews.go.com/Blotter/	No

al Sahwa	http://al-sahwa.blogspot.com/	No
AllAfrica	http://allafrica.com/	No
Avian Flu Diary	http://afludiary.blogspot.com/	No
BNOnews	http://www.bnonews.com/	No
Borderfire Report	http://www.borderfirereport.net/	No
Borderland Beat	http://www.borderlandbeat.com/	No
Brickhouse Security	http://blog.brickhousesecurity.com/	No
Chem.Info	http://www.chem.info/default.aspx	No
Chemical Facility Security News	http://chemical-facility-security-news.blogspot.com/	No
ComputerWorld Cybercrime Topic Center	http://www.computerworld.com/s/topic/82/Cybercrime+and+Hacking	No
Counter-Terrorism Blog	http://www.counterterrorismblog.com/	No
Crisisblogger	http://crisisblogger.wordpress.com/	No
Cryptome	http://cryptome.org/	No
Danger Room	http://www.wired.com/dangerroom/	No
Drudge Report	http://drudgereport.com/	No
El Blog Del Narco	http://elblogdelnarco.blogspot.com/	No
Emergency Management Magazine	http://www.emergencymgmt.com	No
Foreign Policy Passport	http://blog.foreignpolicy.com/	No
Global Security Newswire	http://gsn.nti.org/gsn/	No
Global Terror Alert	http://www.globalterroralert.com/	No
Global Voices Network	http://globalvoicesonline.org/-/world/americas/haiti/	No
Google Blog Search	http://blogsearch.google.com	No
Guerra Contra El Narco	http://guerracontraelnarco.blogspot.com/	No
H5N1 Blog	http://crofsblogs.typepad.com/h5n1/	No
Homeland Security Today	http://www.hstoday.us/	No
Homeland Security Watch	http://www.hlswatch.com/	No
Huffington Post	http://huffingtonpost.com/	No
Hurricane Information Center	http://gustav08.ning.com/	No
HurricaneTrack	http://www.hurricanetrack.com/	No
InciWeb	http://www.inciweb.org/	No
Informed Comment	http://www.juancole.com/	No
Jihad Watch	http://www.jihadwatch.org/	No
Krebs on Security	http://krebsonsecurity.com/	No
LA Now	http://latimesblogs.latimes.com/lanow/	No
LA Wildfires Blog	http://latimesblogs.latimes.com/lanow/wildfires/	No
Livesay Haiti Blog	http://livesayhaiti.blogspot.com/	No
LongWarJournal	http://www.longwarjournal.org/	No
Malware Intelligence Blog	http://malwareint.blogspot.com/	No
MEMRI	http://www.memri.org/	No
MexiData.info	http://mexidata.info/	No
MS-13 News and Analysis	http://msthirteen.com/	No
Narcotrafico en Mexico	http://narcotraficoenmexico.blogspot.com/	No
National Defense Magazine	http://www.nationaldefensemagazine.org	No

National Terror Alert	http://www.nationalterroralert.com/	No
NEFA Foundation	http://www.nefafoundation.org/	No
Newsweek Blogs	http://blog.newsweek.com/	No
Nuclear Street	http://nuclearstreet.com/blogs/	No
NYTimes Lede Blog	http://thelede.blogs.nytimes.com/	No
Plowshares Fund	http://www.ploughshares.org/news-analysis/blog	No
Popular Science Blogs	http://www.popsci.com/	No
Port Strategy	http://www.portstrategy.com/	No
Public Intelligence	http://publicintelligence.net/	No
ReliefWeb	http://www.reliefweb.int	No
RigZone	http://www.rigzone.com/	No
Science Daily	http://www.sciencedaily.com/	No
STRATFOR	http://www.stratfor.com/	No
Technorati	http://technorati.com/	No
Terror Finance Blog	http://www.terrorfinance.org/the_terror_finance_blog/	No
The Latin Americanist	http://ourlatinamerica.blogspot.com/	No
Threat Level	http://www.wired.com/threatlevel/	No
Threat Matrix	http://www.longwarjournal.org/threat-matrix/	No
Tickle the Wire	http://www.ticklethewire.com/	No
Tribuna Regional	http://latribunaregional.blogspot.com	No
TruckingInfo.com	http://www.truckinginfo.com/news/index.asp	No
United Nations IRIN	http://www.irinnews.org/	No
Ushahidi Haiti	http://haiti.ushahidi.org/	No
War on Terrorism	http://terrorism-online.blogspot.com/	No
WireUpdate	http://wireupdate.com/	No

Critical Information Requirements:

Critical Information Requirements (CIR) are utilized as the mechanism for MMC/SNMC collection, processing and distributions efforts – and used to categorize items of interest according to the following:

1. Potential threat to DHS, other federal, and state and local response units, facilities, and resources

- Learning that something has occurred
- Collecting operational data, information, and imagery

2. Potential impact on DHS capability to accomplish the HSPD-5 mission

- Corroborating/reconciling reports
- Threatens DHS and other response units, facilities, or supporting activities
- Present unique demands on low density – high demand

3. Identifying events with operational value…corroborating critical information

- Collecting imagery not otherwise available
- Identifying operational factors that may impact DHS capabilities
- Analyzing the effectiveness of response activities

4. Identifying media reports that reflect adversely on DHS and response activities

- Identifying gaps in the response
- Identifying inaccurate and/or incomplete media reports

5. Standing HSC planning scenarios (see next page)

Homeland Security Council Scenarios:

The Homeland Security Council (HSC) national planning scenarios are used by DHS to guide the development/elicitation of critical data requirements and to organize information. MMC should the use the HSC scenarios as additional guidance in reporting parameters.

1. **Nuclear Detonation** – Nuclear Detonation
2. **Biological Attack** – Aerosol Anthrax
3. **Biological Disease Outbreak** – Pandemic Influenza
4. **Biological Attack** – Plague (e.g. Pneumonic Plague)
5. **Chemical Attack** – Blister Agent
6. **Chemical Attack** – Arsine
7. **Chemical Attack** – Nerve Agent
8. **Chemical Attack** – Chlorine
9. **Natural Disaster** – Earthquake
10. **Natural Disaster** – Hurricane
11. **Radiological Attack** – RDD (Radiological Dispersal Devices)
12. **Explosives Attack** – IED (Improvised Explosive Devices)
13. **Biological Attack** – Food Contamination
14. **Biological Attack** – FMD (Foreign Animal Disease)
15. **Cyber Attack** – Cyber Critical Infrastructure

IOI Categorization

(Last updated - 13 Jan 10)

These IOI categories complement the more formal, broad CIRs and help in the establishment of search criteria. They also facilitate specially requested look-back research efforts. The categories include:

1. **Terrorism**: Includes media reports on the activities of terrorist organizations both in the United States as well as abroad. This category will also cover media articles that report on the threats, media releases by al Qaeda and other organizations, killing, capture, and identification of terror leaders and/or cells.

2. **Weather/Natural Disasters/Emergency Management**: Includes media reports on emergency and disaster management related issues. Reports include hurricanes, tornadoes, flooding, earthquakes, winter weather, etc. (all hazards). Reports will outline the tracking of weather systems, reports on response and recovery operations, as well as the damage, costs, and effects associated with emergencies and disasters by area. Will also include articles regarding requests for resources, disaster proclamations, and requests for assistance at the local, state, and federal levels.

3. **Fire:** Includes reports on the ignition, spread, response, and containment of wildfires/industrial fires/explosions regardless of source.

4. **Trafficking/Border Control Issues**: Includes reports on the trafficking of narcotics, people, weapons, and goods into and out of the United States of an exceptional level. Reports will also include articles outlining the strategy changes by Agencies involved in the interdiction of the items outlined above.

5. **Immigration**: Includes reports on the apprehension of illegal immigrants, policy changes with regard to immigration in the United States, and border control issues.

6. **HAZMAT**: Includes reports on the discharge of chemical, biological, and radiological hazardous materials as well as security and procedural incidents at nuclear facilities around the world, and potential threats toward nuclear facilities in the United States. Also included under this category will be reports and response to suspicious powder and chemical or biological agents.

7. **Nuclear**: To include reports on international nuclear developments, attempts to obtain nuclear materials by terrorist organizations, and stateside occurrences

such as melt downs, the mismanagement of nuclear weapons, releases of radioactive materials, illegal transport of nuclear materials, obtaining of weapons by terrorist organizations, and breaches in nuclear security protocol.

8. **Transportation Security**: To include reports on security breaches, airport procedures, and other transportation related issues, and any of the above issues that affect transportation. Reports will include threats toward and incidents involving rail, air, road, and water transit in the United States.
9. **Infrastructure**: Includes reports on national infrastructure including key assets and technical structures. Reports will include articles related to failures or attacks on transportation networks, telecommunications/ internet networks, energy grids, utilities, finance, domestic food and agriculture, government facilities, and public health, as well as those listed above.

10. **National/International Security**: Includes reports on threats or actions taken against United States national interests both at home and abroad. Reports would include articles related to threats against American citizens, political figures, military installations, embassies, consulates, as well as efforts taken by local, state, and federal agencies to secure the homeland. Articles involving intelligence will also be included in this category.

11. **Health Concerns, National/International**: Includes articles on national and international outbreaks of infectious diseases and recalls of food or other items deemed dangerous to the public health.

12. **Public Safety**: Includes reports on public safety incidents, building lockdowns, bomb threats, mass shootings, and building evacuations.

13. **Reports on DHS, Components, and other Federal Agencies**: Includes both positive and negative reports on FEMA, CIA, CBP, ICE, etc. as well as organizations outside of DHS.

14. **Cyber Security**: Reports on cyber security matters that could have a national impact on other CIR Categories; internet trends affecting DHS or government security such as cyber attacks, computer viruses; computer tools and techniques that could thwart local, state and federal law enforcement; and Emergency Management use of social media strategies and tools that aid or affect communications and management of crises.

Trend Analysis Requirements

1. **Credible Source** (media-linked reporter or expert)

2. **Credible Evidence** (photo, audio or video)

3. **Collection of corroborating "hits" indicating a trend** (posts, observations and opinions from multiple sources)

4. **Official Alerts** (local, state, national, NGO)

Must meet at least one of the above requirements to be a candidate for a match with DHS Critical Information Requirements (CIRs). If matched, the SN "Hit" becomes a potential "Item of Interest" (IOI) or a "Tip" that is passed through the MMC to DHS OPS/NOC.

Sourcing Items of Interest:

1. **Official Alert:** The item of interest was distributed by governmental and NGOs.

2. **Alert:** The item of interest was initiated because of a "real time" alert via email, RSS or other instant communication format.

3. **Passive Scan:** The item of interest was produced following the finding of an article as the analyst searched websites (Twitters, Flickr, YouTube, Facebook, etc.) without any prior alert by a SNMC tool.

4. **Active Search:** The item of interest was distributed after the analyst found an article by seeking out certain topics in search engines (Google, Twitter, Bing, etc.).

Privacy Compliance Review
Office of Operations Coordination
Olympics Social Media Monitoring Initiative

Below is a preliminary list of questions to help guide the discussion. The demonstration and walk through of the Olympics Social Media Monitoring Initiative may answer many of these questions.

We'll plan to talk through this list during the round table discussion.

1. What written guidance have you provided to your analysts on what is acceptable or not acceptable information to review and then include in situational reports and the common operating picture?
   Analyst Handbook: PIAs, CONOPs, PII Reference Chart (also on the wall), Privacy Reference Documents,

2. Do you maintain copies of what is reviewed? We don't keep copies of all the things we review; we only keep copies of we actually send

3. How do you maintain the source of the information?
   The sent email has it, and the daily log has a primary source link, unless the links had to be redacted for PII.

4. What is your process from initial review to creation of the product?
   See CONOPS sect 5 and 6.3
   a. Who signs off on final products?
   GARs and GIRs are created and sent by the watch analyst. GSRs are built by analysts and reviewed by a senior reviewer. In training the analysts get guidance and review by a senior reviewer prior to sending.

5. How are you defining success? - Positive feedback that the reports are useful i.e. from NOC, State
   a. Provide examples of success stories. – State Dept., Joint Task Force Haiti, Blast call ref to an Olympic GSR
   b. How many reports have you distributed? – Appx. 281 reports as of 23 Feb (Olympic = 62 Haiti = 219)
   c. Have you received any feedback from the distribution on the utility of the reports? – Yes, State Dept. Joint Task Force Haiti, FBI

6. How are you sharing the situation reports and the common operating picture?
   - Just by email, and occasionally phone
   a. How are recipients using the information?
   b. Is it used to do further, more targeted, monitoring/and or searches?
   c. Do you maintain copies of what is disseminated? - Yes

7. Have you discovered PII or other information in an identifiable form? Yes

   a. If so, when and what were the circumstances? – Daily, but the information is not collected under normal operations and is ignored while searching and deleted while generating reports
   b. What did you do with it to ensure it did not enter agency files? – We do not collect it, we delete it and we run scan systems to ensure we delete files and cookies.

8. Have you had to engage in social networking where OPS employees were required to establish a username and password to gain access to information? No, it was never allowed
   a. If so, explain the circumstances. – N/A

9. How did you train OPS employees on what was permitted under social media monitoring vs full social networking? – CONOPs, PIAs, Reference Materials and in-class training
   a. Please provide a copy of the training. (Analyst book will be provided)

10. Has your records officer established a NARA approved retention and disposal policy for this Initiative? – No, the process is still ongoing with Privacy as we understand it

NOTES

Don,

Thanks for sharing your thoughts with the MMC Team last week. The more insights they get from you, the better we'll be able to tailor MMC's involvement, coordination, and report products to assist the NOC, and the DHS senior leadership situational awareness and decision support processes. ***I wanted, for our collective benefit, to capture the key areas from our discussions, particularly where you agreed to follow up or provide additional direction, and approved specific MMC recommendations that were presented to you.***

1. ***You agreed***:
   - ***a.*** with our ***assessment of the "new Overarching PIA" in terms of what it allows and what it does not allow***
   - ***b.*** to ***reach out to OPA in order to obtain a copy of the Facebook Terms of Service (TOS) Agreement*** that was referenced a week or so ago, and to determine whether other impending TOS Agreements were soon to be signed. (These are important to us for a number of reasons, but specifically regarding any direction for "Username" naming conventions and account opening related items.)
   - ***c.*** to confirm the ***situation regarding*** (b)(6), (b)(7)(C) who informed us by email that he was no longer with OPA
   - ***d.*** to ***provide direction regarding who should be on Distribution List B*** (limited distribution) and, when required Distribution List C (special distribution)

2. ***You approved MMC Recommendations to:***
   - ***a. Use DHSNOCMMC-1 through DHSNOCMMC-n as the naming convention*** the MMC and management staff would use to ensure full disclosure regarding the MMC being an element of the DHS National Operation Center (absent any conflicting OPA direction)
   - ***b. Adopt MMC "Overarching PIA" Implementation concept***
     - ***1.*** Relate social networking/media (SN) report to a standing or incident CIR

     - ***2.*** Corroborate SN report with other SN posts, MMC reports, or other sources

     - ***3.*** Determine SN report has DHS incident or strategic value

     - ***4.*** Provide senior level review of draft SN report

     - ***5.*** Distribute SN report to the appropriate distribution list
       - a) Distribution List A – full distribution (FULLDIS)
       - b) Distribution List B – limited distribution (LIMDIS)
       - c) Distribution List C – special distribution (SPECDIS)

     - ***6.*** Complete a daily post processing review of all SN reports

     - ***7.*** Provide structured daily feedback to SN watch standers

   - ***c. Reduce the number of MMC and SN report formats from nine to five total***

   - ***d. Adopt the new MMC report formats that will be standard to media monitoring and social media reports***

e. *Implement the new MMC application in accordance with the schedule below:*

1. *July 26-30:*
   a) Individual Training on MMC application via emailed instructions
   b) Analysts will post test reports with a non-live version of the MMC application prior to formal training
   c) Provides testing feedback prior to formal training

2. *August* 2-*6:*
   d) Analysts will attend one of two scheduled formal training days, based on their preference and schedule
   e) Formal training will reinforce the individual training
   f) Two training days will allow for each analyst to attend at least one session
   g) Analyst will have ample time to post multiple reports into the system prior to beginning concurrent operations

3. *August 7-15:*
   h) Concurrent reporting via both Outlook (live) and the MMC application (archive only)
   i) Concurrent reporting will allow the syncing of report numbers to the beginning of the month
   j) Reports will be added into the database, building an operational archive
   k) Analysts will continue to learn and train in live-fire conditions
   l) “Live” testing will expose any possible programming or formatting issues

4. *August 16:* Switch to MMC application for full live operations at 1200 EDT

V/r, (b)(6), (b)(7)(C)

DRAFT

22 Nov 2010

To: Media Monitoring Capability (MMC) Watch Analysts

CC: (b) (6)

Subject: Draft Inadvertent PII Inclusion Procedure (External)

From: (b) (6) Senior Ops Advisor, NOC Media Monitoring

In the event of an inadvertent PII inclusion in MMC reports (IOI, Steady State, NSS/ISS, OPSUM, Weekly Data Reports, etc.), the following procedure must be implemented to fully comply with Personally Identifiable Information (PII) guidance and rules.

As soon as unauthorized PII has been identified, the analyst must notify (b) (6) (or his backup if (b) (6) is unavailable) (b) (6) will notify the DHS/OPS Current Branch Chief and NOC Director (CC to (b) (6) (b) (6) that an IOI with inadvertent PII included been sent (template 1 below) and request authorization for the watch to send an email deletion advisory (template 2 below) to the full distro list. The latter email will advise readers that unauthorized, but unclassified information was accidentally included in the IOI (identified by subject line and DTG) and therefore must be permanently deleted. A general description of how to permanently delete the IOI in MS Outlook will be provided along with a notice to contact the recipients' system administrator with questions for programs other than Outlook.

Template 1: Initial notification to NOC Leadership of inadvertent PII:

> Sir,
> MMC has sent out an IOI containing inadvertent PII to the (full or LIMDIS) distro list. The IOI was:
>
> > (*example) Germany Tightens Airport and Rail Security Over Possible Late November Terror Attack--MMC IOI #2627-10;* (sent 11/16/10 at 5:17 pm) PII was included in the 3rd bullet. With your approval we will send an IOI deletion advisory to the affected distro list.

Template 2: IOI deletion advisory for inadvertent PII:

> You received a NOC Media Monitoring email report (IOI) that inadvertently included unauthorized but unclassified information. Therefore, please permanently delete the following report:
>
> > *(Example) Germany Tightens Airport and Rail Security Over Possible Late November Terror Attack--MMC IOI #2627-10;* (sent 11/16/10 at 5:17 pm)
>
> *NOTE:* for MS Outlook users, an email can be permanently deleted by either holding the shift key when deleting it from the inbox or folder or deleting it and then deleting again from the Deleted Items folder.
>
> For programs other than MS Outlook, please contact your System Administrator if you have questions.

DRAFT

John Doe
Operations Analyst
DHS NOC Media Monitoring
Phone: (b) (6)
Cell: 7 (b) (6)

This procedure has been coordinated with (b) (6) Acting Director, Operations Coordination Division, DHS/OPS.

(b) (6)

22 Nov 2010

To: Media Monitoring Capability (MMC) Watch Analysts

CC: (b) (6)

Subject: Inadvertent PII Inclusion Procedures (Internal)

From: (b) (6) Senior Ops Advisor, NOC Media Monitoring

In the event of an inadvertent PII inclusion in MMC reports (IOI, Steady State, NSS/ISS, OPSUM, Weekly Data Reports, etc.), the following procedure must be implemented to fully comply with Personally Identifiable Information (PII) guidance and rules.

As soon as unauthorized PII has been identified, the analyst must notify (b) (6) (or his backup if (b) (6) s unavailable). Please provide enough details with report ID#, dates, and PII items in your message. (b) (6) and Jae will confer, after which (b) (6) will notify all MMC and SNMC team members and provide direction.

Direction to TechOp readers other than analysts will be to permanently delete the offending IOI for Outlook by either holding the shift key when deleting or deleting it from the *Deleted Items* folder. For MMC analysts and within the MMC application, the offending PII will be manually deleted and overwritten based on where in the IOI the PII is.

The manual deletion procedure will be included in each email directing such action. The following steps must be used:

1. Open the email message
2. Select "Other Actions" in the "Actions" section of the toolbar at the top of the page
3. Select "Edit Message" from the Other Actions pull down menu
4. Replace the offending PII with "xxxx," "NO Link due to PII," whichever is directed in the email communication
5. Close the edited email, and click yes when asked if you want to save changes

In all cases, analyst or senior reviewer, confirmation of completion of the action must be sent to (b) (6) within 24 hours of receipt.

(b) (6)

New PIA Revisions

Effective immediately (1715, 7 Jan11)

All analysts will read and initial before they may accept a shift

OPS is conducting this update to the Privacy Impact Assessment (PIA) because this initiative may now collect and disseminate PII for certain narrowly tailored categories. *(Abstract p.2)*

Furthermore, PII on the following categories of individuals may be collected when it lends credibility to the report or facilitates coordination with federal, state, local, tribal, territorial, foreign, or international government partners: *(Overview p.3)* *See NOTE below*

1) U.S. and foreign individuals *in extremis* situations involving potential life or death circumstances; *(this is no change)*

2) **Senior U.S. and foreign government officials** who make public statements or provide public updates;

3) **U.S. and foreign government spokespersons** who make public statements or provide public updates;

4) **U.S. and foreign private sector officials and spokespersons** who make public statements or provide public updates;

5) **Names of anchors, newscasters, or on-scene reporters who are known or identified as reporters in their post or article or who use traditional and/or social media in real time to keep their audience situationally aware and informed**;

6) **Current and former public officials who are victims of incidents or activities related to Homeland Security; and**

7) **Terrorists, drug cartel leaders or other persons known to have been involved in major crimes of Homeland Security interest**, (e.g., mass shooters such as those at Virginia Tech or Ft. Hood) **who are killed or found dead**.

NOTE: PII on these individuals may include: 1) full name; 2) affiliation; 3) position or title; and 3) publicly-available user ID. Analysts are trained to use only approved PII that is easily identifiable and to ignore and exclude any non-authorized PII. *Practical implementation: the PII must add value, i.e. we can now say Sheriff or Fire Chief, but if the name is not important (and it usually isn't) don't include the name, just the title, esp for lower level officials.* Should PII come into the NOC's possession, apart from these categories, the NOC shall redact it prior to further dissemination of any collected information. (Section 1.1, p.4) (Current PII retraction procedures do not change)

What was NOT approved:

- We **will not report** on Individuals suspected or accused of committing crimes of National or Homeland Security interest, if captured, (see # 7 above for the exception if they are killed or found dead)

- We **will not report** on Private Citizens no matter if they are witnesses, victims, observers or some other way connected to an event

- We **will not report** on high profile people such as celebrities, sports figures or media members who are victims. (see # 6 above for the exception if they are current or former public officials)

(b) (6)

(b) (6)

From the current PIA:
Furthermore, PII on the following categories of individuals may be collected when it lends credibility to the report or facilitates coordination with federal, state, local, tribal, territorial, foreign, or international government partners:
1) U.S. and foreign individuals *in extremis* situations involving potential life or death circumstances; (no change from what has always been in force)

2) senior U.S. and foreign government officials who make public statements or provide public updates;

3) U.S. and foreign government spokespersons who make public statements or provide public updates; (removes "senior" req't from condition #2)

4) U.S. and foreign private sector officials and spokespersons who make public statements or provide public updates; (includes private sectors" req't from condition #2)

5) Names of anchors, newscasters, or on-scene reporters who are known or identified as reporters in their post or article or who use traditional and/or social media in real time to keep their audience situationally aware and informed;

6) Current and former public officials who are victims of incidents or activities related to Homeland Security; and

7) Terrorists, drug cartel leaders or other persons known to have been involved in major crimes of Homeland Security interest, (e.g., mass shooters such as those at Virginia Tech or Ft. Hood) who are killed or found dead.

****ANSWER KEY****

NOC MEDIA MONITORING CAPABILITY

Privacy Proficiency Exam (Answer Key)

I. Multiple Choice

1) What does PII stand for?

a) Privacy Issue Incident

b) Personal Information Identified

c) Personally Identifiable Information

d) Private Information Intelligence

ANSWER: *C*

2) What is an example of PII?

a) License plate numbers (always, sometimes, never)

b) A person's name (always, sometimes, never)

c) Job titles or elected office (always, sometimes, never)

d) Street addresses (always, sometimes, never)

e) Medical information (always, sometimes, never)

f) Email addresses (always, sometimes, never)

g) Usernames (always, sometimes, never)

h) Social Security numbers (always, sometimes, never)

i) Phone numbers (always, sometimes, never)

ANSWERS:

a) Always

b) Always

c) Sometimes

- *As long as the title or office is broad and vague enough to prevent a reader from identifying any one specific person.*

d) Sometimes

- *While it is permissible to report the location of an incident (e.g., "crews are responding to a pileup at Mile Marker 50.9, between Exits 16 and 17, on the Interstate 405 …"), it's not okay to divulge the precise location where a person lives (i.e., their home address). Business and government building addresses, on the other hand, can appear in an IOI because businesses and government agencies are entities, not specific people or peoples.*

e) ***Sometimes***

- *As long as the medical condition addressed in the IOI is not ascribed to any one particular person.*

f) Sometimes

- *As long as the email address is not a personal email address. A general company or government agency email address is acceptable; it should be noted, however, that email addresses are rarely included in IOIs.*

g) Always

- *Even if a particular username is an obvious alias (e.g. PrinceOfDarkness007), you should redact it. You should always be careful not to include any information that in any way points to a specific individual.*

h) Always (!!)

i) Sometimes

- *Same rule applies here as with email address – personal phone numbers should never be reported in an IOI!*

3) What does PIA stand for?

a) Private Information Alert

b) Private Information Act

c) Preventative Incident Assessment

d) Privacy Impact Assessment

ANSWER: *D*

4) For the following, mark all that apply. The PIA is important to MMC and SN watch operations because,

a) It provides guidance on how the MMC will address privacy concerns

b) It essentially serves an operating "license" granting us permission to perform our job

c) It explains to the public what types of information we collect and how we address privacy concerns

d) All of the above

ANSWER: D

5) You are building an IOI report. One of your sources includes a quote from President Obama. What do you do? (Mark all that apply)

a) Ignore the quote altogether and do not include it in the report

b) Use the quote if its substance is "operationally relevant" and helps improve "situational awareness"

c) Use the quote, but attribute it using a euphemism, such as "a high-ranking U.S. official said…"

d) Use the quote and don’t hesitate to attribute it to “President Obama” because he’s a well-known public official

e) Use the quote and attribute it to “the President,” making sure not to use “Obama”

ANSWER: *B; C*

- *With respect to Choice A, you may very well choose not to include a quote if you believe its content adds nothing substantive to your report. However, there will be instances when a quote might elegantly capture and illustrate a concept or fact you’re trying to convey.*
  - *THE TAKEAWAY – Ignoring a quote should never be your default option. If you chose to use a quote, just make sure you avoid identifying who said it.*
- *With respect to Choice D, we are not allowed to include ANY identifying information in our reports, no matter who is being discussed – even the President of the United States. If, for example, you’re reporting on a federal action on which the President has commented, you would not write “the President said…”, because that would be identifying a specific person – there’s only one American President.*

6) For the following, mark all that apply. You come across a story about the mayor of Ciudad Juarez, which is in the northern Mexican state of Chihuahua, who was gunned down in the street, apparently at the hands of a drug cartel assassin. Should you,

a) Ignore the story altogether because it presents too many PII issues

b) Report the story and don’t worry about identifying the mayor by name because he’s not a U.S. citizen

c) Report the story, but use a euphemism like “a government official” instead of identifying the mayor by name

d) Report the story, identify the victim as the mayor of Ciudad Juarez, but make sure not to use his name

e) Report the story, identify the victim as a mayor in the Mexican state of Chihuahua, but make sure not to use his name

ANSWER: *C; E*

- *Choice C is acceptable because it is vague enough to avoid the risk of a reader matching a title to a specific name. At the same time, you're still conveying the salient point that the assassinated person is an important public figure, which is what makes the story IOI-worthy in the first place.*

- *Choice E is permissible because it is vague enough – the mayor in question could be the mayor of ANY town in the state of Chihuahua. At the same time, you're giving the reader a general sense of geography, which, in this case, is important because Chihuahua is a border state, and we are especially interested in cross-border violence (more so than violence in Mexican states further to the south). To avoid any confusion or PII mistakes, you should not mention the town anywhere in your report.*

7) In the interest of providing our clients with operationally relevant information, the Media Monitoring Capability (MMC) has been granted permission to use different types of traditional and social media Internet resources to gather information that enhances "situational awareness." What sources are most usually always acceptable to use in our reports? (Mark all that apply)

a) Blogs

b) Corporate press releases

c) Chatrooms

d) Editorials/Op-eds

e) Emails

f) Facebook (including restricted access pages, just as long as you don't identify the source by name

g) Reports issued by GAO or CBO

h) Inspector General audits or investigations

i) Message Boards/Forums

j) Traditional media websites

k) Twitter

l) University Studies/Reports

ANSWER: *A; B; C; I; J; K*

- *PLEASE NOTE:*
    - *Choice F above would apply if the Facebook page is publicly accessible.*
    - *In limited circumstances, it may be permissible to reference information from Choices G and L. In such circumstances, your source should not be the GAO, CBO, IG or academic report itself.*

8) If you inadvertently publish an IOI that includes PII, what should you do? (Mark all that apply)

a) Recall the IOI via Outlook's "Recall Email" feature

b) Send a "Correction IOI" acknowledging the mistake

c) Send a Jabber message to NOC acknowledging the mistake

d) Call the SWO to inform them of the mistake

e) Call TSI management to inform them of the mistake

f) Follow the "Inadvertent PII Inclusion Procedure" instructions posted at each Watch Desk

ANSWER: E; F

- Read it and head it

II. TRUE OR FALSE?

1) PII only applies to private citizens of the United States; PII rules do not apply to government officials or individuals in the public eye.
True / [✓ **False**]

EXPLANATION: *Self explanatory*

2) PII not only applies to U.S. citizens; it applies to the citizens of other nations as well.
[✓ **True**] / **False**

EXPLANATION: *Self explanatory*

3) The following representation is acceptable for use in IOIs: "Mexico's marines commander …".

True / [✓ False]

EXPLANATION: *Mexico has only one marines commander.*

4) Because source citations are such an integral component in our reports, it's okay if a listed source link in a report happens to include a name (for example, www.foxnews.com/2010/12/06/**hillary-clinton**-international-stage-war-time); the most important consideration is to ensure that PII does not appear in the report's Subject line or in its body.

True / [✓ False]

EXPLANATION: *Any name appearing anywhere in an IOI is never acceptable***.**

5) While it is certainly important to be on the lookout for PII when reviewing/editing pre-published reports, it is not as important as other considerations, such a content and grammar

True / [✓ False]

EXPLANATION: *PII is among the most important of considerations and should never be subservient to other concerns.*

6) If any PII-related questions arise as you build an IOI, you should err on the side of caution, stop working on the IOI, and NOT send it out.

True / [✓ False]

EXPLANATION: *Consult, consult, consult. If you ever have any questions about PII, query the Watch Desk analyst on the other side of the divider and/or contact Brad.*

7) There is never a condition under which sending out PII is authorized.

True / [✓ False]

EXPLANATION: *In extremis. As always, CONSULT WITH OTHERS FIRST.*

MMC-SN Overarching PIA

Implementation CONOPs

1. Relate social networking/media (SN) report to a standing or incident CIR

2. Corroborate SN report with other SN posts, MMC reports, or other sources

3. Determine SN report has DHS incident or strategic value

4. Provide senior level review of draft SN report

5. Distribute SN report to appropriate distribution list

    a. Distribution List A – full distribution list
    b. Distribution List B – limited distribution group
    c. Distribution List C – special distribution group

6. Complete a daily post processing review of all SN reports

7. Provide structured daily feedback to SN watch standers

<u>Challenges with SN Going Fully Engaged</u>

1. Overwhelming readers with double the MMC distributions
2. Ensuring MMC-T and SN are complementary and not overlapping or redundant
3. Avoiding false positives
4. Figuring out how to fully exploit early warning for the NOC without releasing too much "fluff," i.e. inundation with suspicious packages or school closings due to bomb threats reports
5. Integrating and standardizing with MMC-T IOIs (IOI numbering and follow-ups) while ensuring readers area able to tell whether a report is based on new or traditional media
6. Keeping a tight feedback loop, e.g. for QC, NOC and leadership feedback, adapting and tailoring both search terms and IOIs
7. Getting all SN analysts on the same page with regard to what warrants an IOI when the PIA is wide open instead of narrowly focused on one topic

<u>Meeting the Challenges</u>

1. Overwhelming Readers
    - Refocus both teams on emphasizing "substance"
        - Determine DHS relevance at incident, operational or strategic level
    - Change output standard from 1 per hour per team, to 3 per 2 hours from both teams
    - Use (b) (7)(E) or limited distro (incl. (b) (7)(E)) to let NOC know about potential items, e.g. initial reports of suspicious package at Lincoln Memorial …notifies NOC/SWO know so they can pulse their net without flooding full distro list

2. Ensuring No Overlap
   - Minor format changes to IOIs, (allows (b) (6) app to work) makes IOIs standard for readers
     - SN or MMC boldly obvious in first line
     - Adds NOC number to Steady State and NSS/ISS updates (per NOC request to help them with tracking)
     - Allows both SN and MMC-T to use sequential one system numbering; follow ups can refer to the same IOI regardless of originator

3. False Positives
   - Same ROE as for topic-specific PIAs, don't release without corroboration, for truly urgent breaking news, notify SWO of unconfirmed incident and advise that search is underway for more corroboration (like MMC-T does now with SWO)
     - If in doubt, analyst will always call (b) (6) a Senior Reviewer.

4. Exploit Early Warning
   - Use (b) (7)(E) or limited distro (incl. (b) (7)(E) Restricted email box) to give heads up on potential items, allow NOC/SWO to pulse their net for official corroboration
   - **This does not mean flooding SWO with every suspicious package or bomb threat**, but there are plenty of cases (i.e. Metro or a DC Monument) that the SWO needs to know about but do not warrant an IOI to full distro.

5. Integrating and Standardizing
   - Separate briefing to address IOI format changes, enhancements and standardization
   - Readers will still be able to quickly and easily tell if traditional or new media, but headers/subj lines will be standard

6. Keeping Tight Feedback Loop
   - Initially Senior Level Review before SN report release
   - Very close monitoring by (b) (6) daily presence in the Watch,
   - Daily (M-F) review of and feedback on the previous 24 hours'/weekend 's reports (Reviews by senior reviewers, team leads and QC)
   - Incorporate feedback into frequent training and team-wide feedback
   - React quickly and adapt to NOC leadership feedback and requests
   - Recognize this will evolve (as MMC-T did) as the NOC, SWO, and leadership get used to SN full output and recommend changes which MMC will be ready to rapidly implement

7. Getting Analysts on Same Page
   - Mtg set for Mon 19 Jul (b) (6) to:
     - Get guidance
     - Inform leadership of proposed changes and the rationale
     - Get approval for format changes
   - Conduct skull session with as many analysts as possible to re-emphasize priorities, CIRs, and standards
     - After that, each analyst not at session will be backbriefed before their first shift

umbers

GW has
ng demands

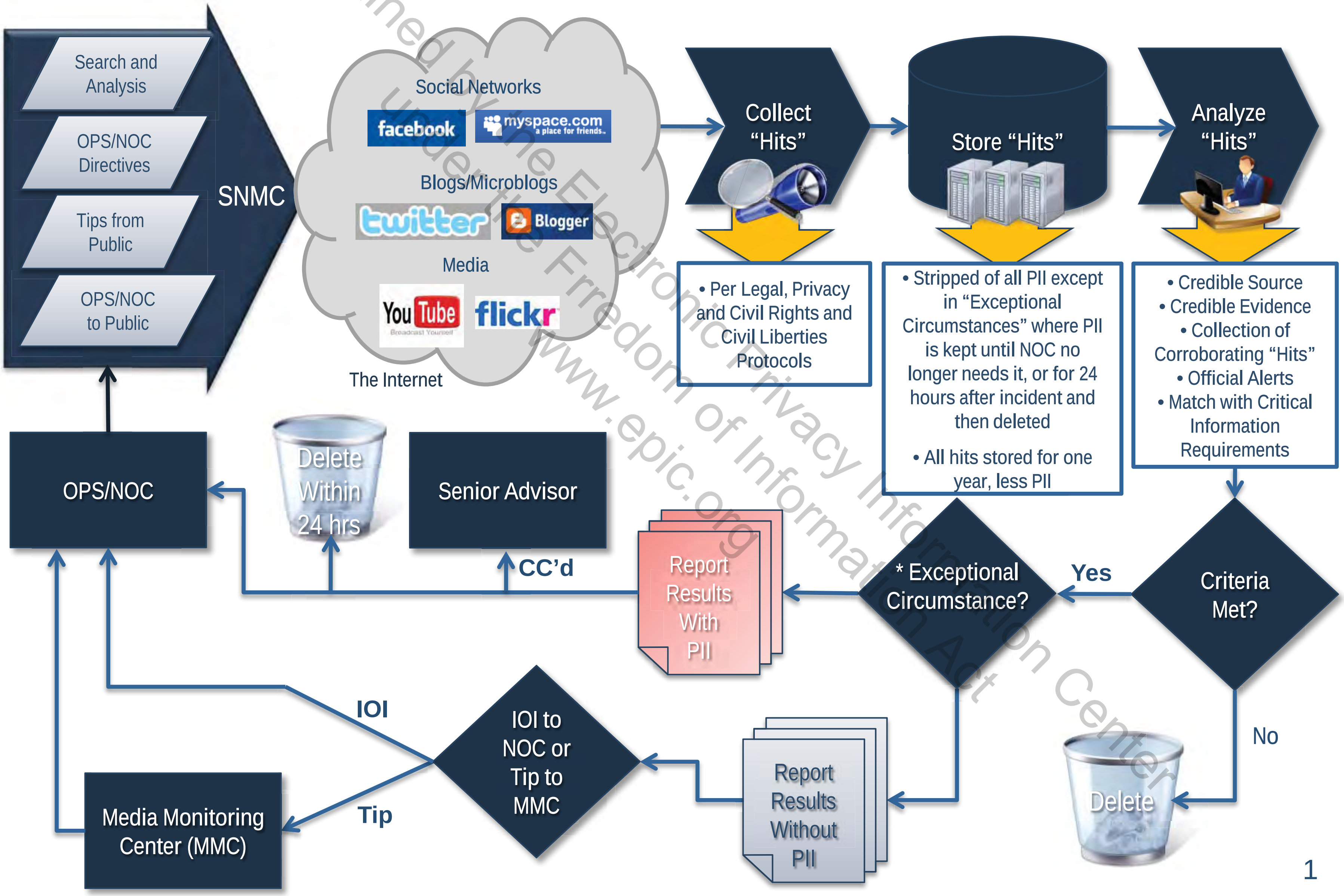
s obtained

Jazz42: Bob Doe
appt bldg at 9 D
minutes ago fro

- **Bob Doe w**
  the data is

nples of "life or death" incider

Social Networking / Media Capability Process



Search and Analysis

OPS/NOC Directives

Tips from Public

OPS/NOC to Public

SNMC

Social Networks

facebook

myspace.com a place for friends.

Blogs/Microblogs

twitter

Blogger

Media

You Tube Broadcast Yourself

flickr

The Internet

Collect "Hits"

- Per Legal, Privacy and Civil Rights and Civil Liberties Protocols

Store "Hits"

- Stripped of all PII except in "Exceptional Circumstances" where PII is kept until NOC no longer needs it, or for 24 hours after incident and then deleted
- All hits stored for one year, less PII

Analyze "Hits"

- Credible Source
- Credible Evidence
- Collection of Corroborating "Hits"
- Official Alerts
- Match with Critical Information Requirements

Criteria Met?

No

Delete

Yes

* Exceptional Circumstance?

Report Results With PII

CC'd

Senior Advisor

Delete Within 24 hrs

OPS/NOC

Report Results Without PII

IOI to NOC or Tip to MMC

IOI

Tip

Media Monitoring Center (MMC)

* Exceptional Circumstances: SMNC will report PII information that relates to the rare situations that have "life or death" implications

Training Plan for
SN Crossing Training

DHS NOC/OPS
MMC - New Media Capability

**TechOp Solutions
International, Inc.**

Version 1
March, 2011

TRAINING PARAMETERS – Crossing Training from MMC to SN	
Item	**Parameter**
Type of Staff to be Trained	New Analysts – MMC New Media Capability
Type of Training	MMC – New Media 101
Amount of Time Allotted	3 days **(specific days unknown at this time)**
Number of Training Sites	One
Number of Classrooms	Three (Conf. Room, PT Office, Watch Room)
Number of Trainees	1
Number of Trainers	2 to 5
Length of Each Session	8 hours
Recommended Classroom Size	1 - 3
Amount of Equipment (for Trainee)	1 laptop, 1 mouse, access to printer
Travel Time and Holidays	None
Special Circumstances	Training must be completed before TBA

1. INTRODUCTION

1.1 Assumptions

The training strategies, activities, and methods are predicated upon the following assumptions:

- A laptop will be provided to each analyst for training and shift work
- New staff will have a working knowledge of XP-based PCs, Microsoft Office and web browsers
- The only stupid questions are the ones not asked

1.2 Goals of the Training Plan

The goals of the training plan are to:

- Provide new staff with an understanding of the role of the MMC's New Media Capability (also referred to as SNMC or SN), and provide continual refinement and training for current staff
- Educate and train new staff about the issues, processes and procedures regarding monitoring social networks/media and engagement on behalf of DHS and the policies of the MMC
- Explain how the New Media Capability works with the Media Monitoring Center (MMC)
- Train new staff in the creation of SN products and quality controls and assessments

- Train new staff to properly handle personally identifiable information (PII)

1.3 Overview of the Training Plan

This document defines the Training Plan for the Department of Homeland Security's OPS/NOC MMC New Media Capability. The Training Plan is a working document. It is revised on a continuous basis as decisions are made and issues are resolved. The document is organized as follows:

- **Training Scope**: Clearly states a list of the objectives and goals of the training, as well as a list of assumptions
- **Training Offerings**: Describes the offerings that define the training, including the training groups, types of training, training approach, training curricula, training schedule, and logistical information
- **Roles and Responsibilities**: Presents the roles and responsibilities of the staff responsible for preparing, conducting, and evaluating the training, and includes a clear definition of the resources and a work plan
- **Contingency Plan**: Identifies anticipated contingencies and details a plan for each contingency
- **Training Material Design, Standards, and Guidelines**: A copy of the Training Material Design, Standards, and Guidelines that will be used to prepare the training materials

2. TRAINING SCOPE

2.1 Training Goals and Objectives

The objectives of the training are:

- Completion of a 13 day training period
- Introduction to the MMC New Media Capability and its relationship with the MMC and DHS OPS/NOC
- Familiarization with the Department of Homeland Security components and leadership
- Familiarization with NOC operations, procedures, communications, and priorities
- Familiarization with the 24/7 schedule and shift Battle Rhythm
- Familiarization with software and technologies utilized by the MMC New Media Capability
- Knowledge of processes and software tools involved in monitoring social networks
- Awareness of the issues surrounding Personally Identifiable Information (PII) and the directives and guidelines set by the MMC New Media Capability's Privacy Impact Assessments, as well as DHS and TSI senior leaders
- Efficient use of the Critical Information Requirements (CIRs) and Trend Analysis Requirements

- Creation of Items of Interest (IOIs), TIPs to the MMC, Combined MMC Operational Summary (OPSUM), Daily Log and Change Over Briefing
- Understand and learn to use the MMC reporting application
- Develop an understanding of "exceptional" circumstances and the handling of PII in those cases
- Understanding the New Media Capability policies regarding personal vs. company accounts/identities
  - Understanding issues and guidance regarding terms of service agreements and usernames/passwords
- Safeguarding DHS NOC MMC social networking presences and applications
- Understanding New Media Capability weekly and monthly data reports, quality control reporting and grading, in addition to other project time directives
- Team operation, coordination and innovation from the same understandings and directives

To achieve these objectives, the following goals are established:

- Describe the mission of the MMC New Media Capability
- Present the trainees with information on DHS structure and personnel
  - Have trainees do research on DHS organizational structure
- Explain and give examples and practice with Personally Identifiable Information (PII) and the MMC New Media Capability's PII policies
- Learn the Director's Criterion, Critical Information Requirements (CIRs), and Trend Analysis Requirements (TARs)
- Instruct the staff on the daily Battle Rhythm and 24/7 shift schedule
- Describe the coordination of the team
- Educate new staff on the processes and sensitivities of monitoring social networks
- Demonstrate the components of the New Media Capability watch desk and MMC watch desk and the NOC Watch Room in Jabber
- Train new staff in the use of technologies and software to aid in the mission of the New Media Capability
- Familiarize and train the analysts on the Apple Mac Mini, Dell laptops, Cradle Point, and server rack cabinet
- Exercise the use of tools and processes to produce and log New Media Capability reports
- Explain the differences and between Regular and Exceptional events
- Outline policy on use of personal and company accounts and identities
- Development, refinement and improvement of processes over time

3. TRAINING

3.1 Training Logistics

This section identifies logistical information based on the requirements for the defined training offerings. The logistical information includes a list of the equipment and supplies required.

3.1.1 Analyst Trainee

- Laptop for each analyst
- Internet access
  - TSI email account
  - Gmail account
  - Access to New Media Capability Google Docs
  - Access to TSI SharePoint Portal
- Training space
- Documents
  - CONOPS (current draft)
  - Standard Operating Procedures (current draft)
  - Training Plan
  - Privacy Impact Assessment(s)
    - Haiti Social Media Disaster Monitoring Initiative
    - 2010 Winter Olympics Social Media Event Monitoring Initiative
    - April 2010 BP Oil Spill Response Social Media Event Monitoring Initiative
    - Publicly Available Social Media Monitoring and Situational Awareness Initiative
    - Social Networking Interactions and Applications (Future Vision)
      - (Communications/Outreach/Public Dialogue)

3.1.2 Trainer Needs

- Computer with internet access
- Whiteboard
  - Markers
- Updated Training Plan
- Handouts
  - Analyst Notebook

4. ROLES AND RESPONSIBILITIES

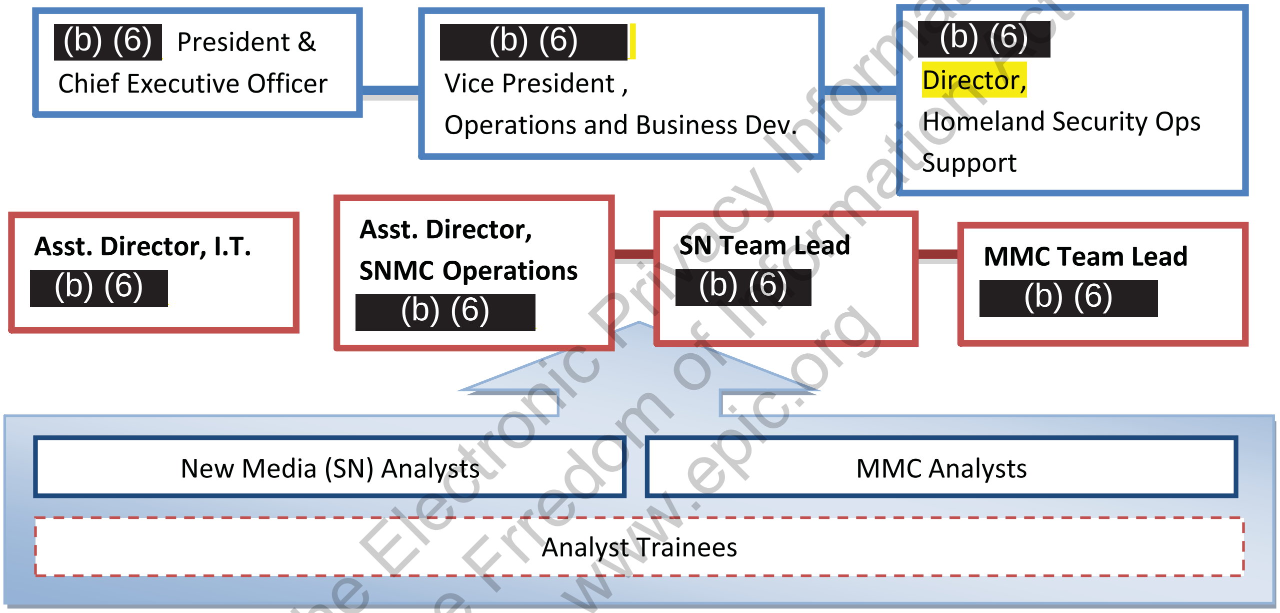
This section details the roles and responsibilities of the personnel responsible for preparing, conducting, and evaluating the training for the MMC New Media Capability.

4.1 Resources

MMC directors and team leads will be leading the training for the new analysts. One will lead a section, but will work together to address all the training materials and objectives. Senior Staff will make introductions and get us started, in addition to providing ongoing input and perspective during training.

This section describes the roles of those involved, the individuals who will fulfill the roles, and their area of responsibility.

TechOp Solutions International, Media Monitoring Capability Team Structure


(b) (6) President & Chief Executive Officer
(b) (6) Vice President , Operations and Business Dev.
(b) (6) Director, Homeland Security Ops Support
Asst. Director, I.T. (b) (6)
Asst. Director, SNMC Operations (b) (6)
SN Team Lead (b) (6)
MMC Team Lead (b) (6)
New Media (SN) Analysts
MMC Analysts
Analyst Trainees

5. TRAINING CURRICULUM and SCHEDULE

DAY 1

DAY:1	**SESSION:**1	**TIME:** 0930-1030	**LOCATION:** PT Office / in-person lecture
TOPIC: Trend Analysis Requirements/New Media Sources			
INSTRUCTOR/S: (b) (6)			
DESCRIPTION: Review of the sources that the MMC New Media Capability uses (ie. Twitter, blogs, etc.), source classifications and methods/requirements to ensure the credibility of information.			
OBJECTIVES: To ensure analysts know what the requirements are for monitoring, collecting information and reporting to the NOC, including the difference between MMC sources and New Media sources and how they are used.			
RESOURCES: • MMC New Media Training Binder			

• General PIA Appendix • Battle Rhythm • CONOPS

DAY:1	**SESSION:**2	**TIME:** 1030-1200	**LOCATION:** PT Office / in-person lecture
TOPIC: The Battle Rhythm and You			
INSTRUCTOR/S: [redacted] (b) (6)			
DESCRIPTION: How will each shift work and what tasks and objectives will need to be completed?			
OBJECTIVES: Review the Battle Rhythm document. Opportunity for the trainee to ask questions about process, searching, sources, etc.			
RESOURCES: • MMC New Media Training Binder • Battle Rhythm			

1200-1300 - LUNCH BREAK (followed by 30 mins of review/Q&A time)

DAY:1	**SESSION:**3	**TIME:** 1300-1530	**LOCATION:** PT Office and MMC Watch Office
TOPIC: Battle Rhythm, Part 2: Tools, Search Engines and Social Networks			
INSTRUCTOR/ [redacted] (b) (6)			
DESCRIPTION: What search tools/sites are analysts allowed to use? What are the protocols for TOS agreements and usernames?			
OBJECTIVES: Ensure the analyst has knowledge of the approved basic search tools. Give time to analyst to familiarize themselves with search tools. Trainee will visit the analyst on duty and observe their ongoing Battle Rhythm.			
RESOURCES: • MMC New Media Training Binder			

DAY 2

DAY:2	**SESSION:**1	**TIME:** 0800-0830	**LOCATION:** PT Office
TOPIC: Daily Objectives Brief			
INSTRUCTOR/S: (b) (6)			
DESCRIPTION: Review of previous day's topics and briefing of the topics to be covered today. Check emails, visit the Watch office to check in and make sure you are aware of any ongoing hot issues/incidents.			
OBJECTIVES: Opportunity for analysts to ask questions and be refreshed on previous topics.			
RESOURCES: • N/A			

DAY:2	**SESSION:**2	**TIME:** 0830-1030	**LOCATION:** PT Office
TOPIC: Privacy Impact Assessments (PIAs)			
INSTRUCTOR/ (b) (6)			
DESCRIPTION: Explanation and review of the overall directives for MMC New Media Operations. What is a Privacy Impact Assessment (PIA)? Review of the PIA that provides our main guidelines for operations.			
OBJECTIVES: Trainee will be provided with background and context on past and present directives for MMC New Media Capability operations. Trainee will become versed in the requirements set forth by the "Publicly Available Social Media Monitoring and Situational Awareness Initiative"			
RESOURCES: • MMC New Media Training Binder			

DAY:2	**SESSION:**3	**TIME:** 1030-1200	**LOCATION:** PT Office
TOPIC: Personally Identifiable Information (PII)			
INSTRUCTOR/S: (b) (6)			
DESCRIPTION: What is PII and why do MMC New Media analysts care? How do we protect privacy while doing our job? How does the Privacy Impact Assessment (PIA) require us to handle PII? Is PII stored?			
OBJECTIVES: To ensure analysts know the background, process and procedures for handling PII during normal operations.			
RESOURCES: • MMC New Media Training Binder • MMC New Media Watch Privacy Resources Handbook • Privacy Resource Documents Binder			

1200-1300 - LUNCH BREAK 1200-1300 (followed by 30 mins of review/Q&A time)

DAY:2	**SESSION:**4	**TIME:** 1300-1430	**LOCATION:** PT Office
TOPIC: Exceptional Circumstances and Handling of PII			
INSTRUCTOR/S: (b) (6)			
DESCRIPTION: What are the exceptions to when MMC New Media is allowed to report PII to the NOC?			
OBJECTIVES: To ensure the analysts know the process, procedures and rules for collecting and reporting items that contain PII and how to properly dispose of it when the NOC no longer needs it.			
RESOURCES: • MMC New Media Training Binder • MMC New Media Watch Privacy Resources Handbook • Privacy Resource Documents Binder			

DAY:2	**SESSION:**5	**TIME:** 1430-1500	**LOCATION:** PT Office
TOPIC: The Sensitive Nature of Searching and Monitoring the Public			
INSTRUCTOR/S: (b) (6)			
DESCRIPTION: Discussion regarding the role of the MMC New Media Capability in the public eye. Background on the evolution of New Media			
OBJECTIVES: Provide an understanding of the risks and procedures involved in operating a social networking monitoring program for DHS.			
RESOURCES: • MMC New Media Training Binder			

DAY:2	**SESSION:**6	**TIME:** 1500-1600	**LOCATION:** PT Office
TOPIC: Review and Set Up of New Media Applications/Tools			
INSTRUCTOR/S: (b) (6)			
DESCRIPTION: Trainees will install and configure applications and tools used by the New Media Capability on their laptops, including TweetDeck, RSS Owl and Notepad++. Trainee will call HSIN help desk to set up a HSIN account, and will instal (b) (7)(E) and ensure access to the (b) (7)(E)			
OBJECTIVES: New Media analysts will have appropriate applications and tools installed on their laptops, which will enable them to communicate and work remotely in a surge operation.			
RESOURCES: • Laptop • T: Drive – (b) (7)(E) read documents and presentations			

DAY:2	**SESSION:**7	**TIME:** 1600-1730	**LOCATION:** MMC Watch Office
TOPIC: Watch Desk Shotgun			
INSTRUCTOR/S: (b) (6)			
DESCRIPTION: Observe the operation of the watch desk			
OBJECTIVES: Analyst will show the trainee the battle rhythm they use on shift. Opportunity for trainee to see the watch operations and ask questions.			
RESOURCES: • N/A			

DAY 3

DAY:3	**SESSION:**1	**TIME:** 0800-0830	**LOCATION:** PT Office
TOPIC: Daily Objectives Brief			
INSTRUCTOR/S: (b) (6)			
DESCRIPTION: Review of previous day's topics and briefing of the topics to be covered today. Check emails, visit the Watch office to check in and make sure you are aware of any ongoing hot issues/incidents.			
OBJECTIVES: Opportunity for analysts to ask questions and be refreshed on previous topics.			
RESOURCES: • N/A			

DAY:3	**SESSION:**2	**TIME:** 0830-1200	**LOCATION:** PT Office
TOPIC: Building IOI, Change Over and OPSUM Reports			
INSTRUCTOR/S: (b) (6)			
DESCRIPTION: What are the components of IOI and OPSUM reports? Trainee will study recent IOI reports and ask questions regarding IOI production. Trainee will scan and search for incidents/news that can be drafted into IOI format for practice (not using the MMC APP at this time), and sent to a reviewer. Trainee will learn how to set up MMC and New Media distribution lists.			
OBJECTIVES: Trainee will familiarize themselves with the IOI and OPSUM reporting formats and learn how to manually build each report type. Trainee will learn to set up distribution lists.			
RESOURCES: • Recent IOI and OPSUM reports			

1200-1300 - LUNCH BREAK 1200-1300 (followed by 30 mins of review/Q&A time)

DAY:3	**SESSION:**3	**TIME:** 1330-1430	**LOCATION:** PT Office
TOPIC: Using the MMC Application to Send IOI Reports			
INSTRUCTOR/[redacted] (b) (6)			
DESCRIPTION: Trainee will be instructed on the use of the MMC Application and given the ability to use the MMC Application Testing Environment. Trainee will use the MMC Application Testing Environment to build and publish IOI reports that include varied sources and images. Trainee will publish at least 15 IOIs to be reviewed by instructors, over the course of the next few training days.			
OBJECTIVES: Opportunity for analysts to ask questions and be refreshed on previous topics.			
RESOURCES: • MMC APP Training Handout (T: Drive)			

DAY: 3	**SESSION:**4	**TIME:** 1430-1600	**LOCATION:** PT Office
TOPIC: Practice – Monitor Sources and Create Reports			
INSTRUCTOR/[redacted] (b) (6)			
DESCRIPTION: Monitoring of SN sources, writing mock reports to be sent to a New Media analyst or senior reviewer. Use of the MMC Application Testing Environment to send TEST IOIs to reviewers.			
OBJECTIVES: To help analysts understand the role of the MMC and how the SNMC will compliment their mission, plus learning from their experiences.			
RESOURCES: • MMC New Media Training Binder • MMC New Media Watch Privacy Resources Handbook • Privacy Resource Documents Binder			

DAY:3	**SESSION:**5	**TIME:** 1600-1800	**LOCATION:** MMC Watch Office
TOPIC: Watch Desk Shotgun			
INSTRUCTOR/S:[redacted] (b) (6)			
DESCRIPTION: Observe the operation of the watch desk			
OBJECTIVES: Analyst will show the trainee the battle rhythm they use on shift. Opportunity for trainee to see the watch operations and ask questions.			
RESOURCES: • N/A			

DAY 4

DAY:4	**SESSION:**1	**TIME:** 0900-1030	**LOCATION:** PT Office
TOPIC: Review of SNMC Project Time Work			
INSTRUCTOR/ (b) (6)			
DESCRIPTION: Review recently produced combined (MMC and New Media) weekly data reports and monthly reports. Learn how to construct weekly and monthly reports. Learn Q/C assessments and reporting.			
OBJECTIVES: Learn how to support the SNMC during project time hours.			
RESOURCES: • Previous combined Weekly Data reports and Monthly reports • Combined Daily Log • Recently produced IOI reports			

DAYS:4	**TIME:** 1030-1800	**LOCATION:** PT Office and Watch Desk
TOPIC: Mock Watch Sessions		
INSTRUCTOR/S: Watch Analyst		
DESCRIPTION: Analyst in training will simulate a watch shift through a mixture of sitting at either the watch desk, or in the PT office. Trainee will use the tools and methods described in MMC New Media training to draft IOI reports. Trainee will use the MMC Application Testing Environment to produce IOIs that will be sent to the designated trainer and (b) (6)		
OBJECTIVES: Produced IOIs will be critiqued by trainers and (b) (6) and if relevant and timely – will be sent by the New Media analyst on watch to the distribution list. Trainee will gain experience and knowledge by training in the same environment that analysts use on a daily basis. When trainee has sufficiently proven their progress, (b) (6) will approve them to send reports via the MMC Application to the DHS distribution list. No IOIs will be sent without his approval.		
RESOURCES: • NA		

Interim Guidance Regarding PII and Reference to Government Spokespersons and Non-U.S. Citizen Terrorist or DTO Leaders
Mon 8/30/2010 10:46 PM

Teammates,
I discussed the ***Privacy Office PII concerns regarding MMC IOIs and the reference to government spokespersons and non-U.S. citizen terrorists and DTO leaders*** with (b) (6) late this afternoon. (b) (6) and I have a teleconference discussion scheduled for Wednesday at 1600 with the Privacy Office. ***Until we conclude that discussion and develop an understanding, adhere to the following*** regarding social networking reports and referencing government spokespersons and non-U.S. citizen/U.S. citizen terrorists and DTO leaders:

1. ***Refer to the government spokesperson by position, the L.A. County spokesperson or a Jefferson City fire chief. Do not include the individual's name***.

2. Where the subject of the report is the killing, capture, or some other significant occurrence of ***a non-U.S. citizen terrorist or DTO leader, include the individual's name.***

3. Where the subject of the report is the killing, capture, or some other significant occurrence of ***a U.S. citizen terrorist or DTO leader, tip the report to the Traditional Media watch stander to locate an article and publish an IOI.***

If you have an questions, ***please cal***(b) (6) ***or me at anytime***. V/r, (b) (6)
[redacted]

Interim MMC Personal Identifiable Information (PII) Guidance/Direction Effective 090110 at 1800 Local
Thu 9/2/2010 2:15 PM

Teammates,
The Office of Operations Coordination and Planning (OPS) is in discussion with the DHS Privacy Office ***to integrate additional operational scenario related guidance and direction in the PIA. These changes will enable MMC watch standers to include in certain cases, PII that may be important to DHS situational awareness and decision making.*** The current Publicly Available Social Media Monitoring and Situational Awareness Initiative PIA dtd 22 Jun 2010 accommodates the inclusion of Personal Identifiable Information (PII) only in "***in extremis situations***".

While the additional operational scenario related guidance and direction is being developed for inclusion in a revised PIA, *ALL MMC watch standers – effective 090110 at 1800 – must strictly observe the below guidelines for BOTH TRADITIONAL AND NEW MEDIA MMC reporting:*

1. ***NO PII is authorized to be included in any MMC reports unless approved by the appropriate DHS OPS authority or it is determined to be an in extremis situation***.

2. *The appropriate DHS OPS authority includes the OPS Senior Executive leadership and the SWO.*

3. *An in extremis situation exists when there is an imminent threat of loss of life, serious bodily harm, or damage/destruction to critical facilities or equipment.*

4. *MMC reports reflecting a senior government official, spokesperson, or law enforcement officer's comments provided to the public or the media, must not include the individual's name, position, or any other information when the inclusion of that information would enable someone to determine the individual's name. Instead, the individual must be referenced, for instance, as a "Maryland State Spokesperson or Senior Maryland State Official". Similarly, MMC watch standers may not refer to the Governor of Maryland or the President, as they indicate a specific individual.*

5. *MMC reports that address known or suspected terrorists, DTO leaders, or other individuals who are a threat to homeland security, regardless of whether a U.S. citizen or non-U.S. citizen, must not include PII.*

6. *MMC reports that address a private sector spokesperson or private citizen statement or information provided to the public or the media, regardless of whether a U.S. citizen or non-U.S. citizen, must not include PII.*

7. *The MMC watch stander may provide the name, position, or other information considered to be PII to the NOC over the telephone when approved by the appropriate DHS OPS authority. That information must not be provided in a venue that would be stored in a database and could be subsequently searched by an individual's PII.*

Follow the above guidelines explicitly, but also *understand and adhere to the spirit and intent expressed therein*.

V/r, (b) (6)

VERSION 2 - Interim MMC Personal Identifiable Information (PII) Guidance/Direction Effective 090110 at 1800 Local
Fri 9/3/2010 10:17 PM

Teammates,
VERSION 2 (Changes are in Blue)

The Office of Operations Coordination and Planning (OPS) is in discussion with the DHS Privacy Office ***to integrate additional operational scenario related guidance and direction in the PIA. These changes will enable MMC watch standers to include in certain cases, PII that may be important to DHS situational awareness and decision making.*** The current Publicly Available Social Media Monitoring and Situational Awareness Initiative PIA dtd 22 Jun 2010 accommodates the inclusion of Personal Identifiable Information (PII) only in "***in extremis situations***".

While the additional operational scenario related guidance and direction is being developed for inclusion in a revised PIA, ***ALL MMC watch standers – effective 090110 at 1800 – must strictly observe the below guidelines for BOTH TRADITIONAL AND NEW MEDIA MMC reporting:***

8. ***NO PII is authorized to be included in any MMC reports unless approved by the appropriate DHS OPS authority or it is determined to be an in extremis situation***.

9. ***The appropriate DHS OPS authority includes the OPS Senior Executive leadership and the SWO.***

10. ***An in extremis situation exists when there is an imminent threat of loss of life, serious bodily harm, or damage/destruction to critical facilities or equipment.***

11. ***MMC reports reflecting a senior government official, spokesperson, or law enforcement officer's comments provided to the public or the media, must not include the individual's name, position, or any other information when the inclusion of that information would enable someone to determine the individual's name. Instead, the individual must be referenced, for instance, as a "Maryland State Spokesperson or Senior Maryland State Official". Similarly, MMC watch standers may not refer to the Governor of Maryland or the President, as they indicate a specific individual.***

12. ***MMC reports that address known or suspected terrorists, DTO leaders, or other individuals who are a threat to homeland security,***

regardless of whether a U.S. citizen or non-U.S. citizen, must not include PII.

13. *MMC reports that address a private sector spokesperson or private citizen statement or information provided to the public or the media, regardless of whether a U.S. citizen or non-U.S. citizen, must not include PII.*

14. *MMC reports will continue to include the links to the actual articles or postings referenced provided the links themselves do not contain PII.*

15. *The MMC watch stander may provide the name, position, or other information considered to be PII to the NOC over the telephone when approved by the appropriate DHS OPS authority. That information must not be provided in a venue that would be stored in a database and could be subsequently searched by an individual's PII.*

Follow the above guidelines explicitly, but also *understand and adhere to the spirit and intent expressed therein*.

V/r, (b) (6)

COP Update change due to PII rules
Thu 9/30/2010 12:19 PM

Team

We have a potential PII problem. As you know, when the NOC goes to Phase 1, we are supposed to post updates to the COP via HSIN. Those updates include an abstract as well as the full text of the article. There is also a place for an analyst note. In the abstract it is easy to keep PII out—just don't enter any. For the full text, you can no longer just cut and paste the entire article. If not edited, it would obviously contain any PII in the article. This is not permitted under our current ROE.

Our solution to this issue is for the analysts to edit out the PII before posting the full text, and then posting the advisory: "*Full text has been edited to redact PII*" in the analyst note section.

This course of action (COA) is what we will do until we get a change in guidance on the PIA. This needs to be an interim change to the COP update procedures. Please add it to changeover as well.

New twist on acknowledging: Vote yes to acknowledge receipt and understanding, but please add your first to the subject line before voting OR vote and then when it asks if you want to edit before sending your vote, check edit response and then add your first name to the subject line. (This helps me keep track of who has responded since you all show up as NOC Media Monitoring)

Thanks
(b) (6)

MMC Application Training and Implementation Timeline

Wednesday, July 28: MMC Application Training for (b) (6)
Time: 1300 tentative – Instructed by (b) (6)
Friday, July 30: MMC Application Training for (b) (6)
Time: 1745 tentative – Instructed by (b) (6)
Saturday, July 31: Basic MMC Application Training for (b) (6) Time: 1745 tentative – Instructed by (b) (6)

Starting at 0000, Sunday, August 1:

> **WATCH:** Analysts will continue to work within Outlook to draft and send IOI/GIR/GAR reports, but once they have received the report they just sent out, they will rebuild the IOI by logging in to the MMC App at (b) (7)(E). The time that the report is added is not as important as the order that the reports are added, which is VERY important and should mirror the order of reports sent via Outlook. Current Steady-State and Phase reports will be preloaded so that new reports can be generated within the system. Updates (follow-ups) to previous reports that are not already in the MMC app will not need to be added, because they will not be preloaded (we have no way to know what reports may need follow-ups). Analysts will continue the cooperative coordination that has been achieved during reporting for Deepwater Horizon, across all topic areas.
>
> **PROJECT TIME:** Analysts on project time will log in to a special TEST version of the MMC App at (b) (7)(E) They will do their best to approximate live conditions of building an IOI within the MMC App. Analysts are encouraged to use a wide range of sources, including typical news sources, and SN sources (blogs, tweets, Facebook) and to cut and paste from those sources into the MMC App. Both PT analysts should send reports together, as to mimic two analysts working on the app at the same time. Analysts will be trained to document any bugs/problems they encounter in an email and send them directly (b) (6)

Wednesday, August 4: MMC App Training for (b) (6), Time: 1300 tentative – Instructed by (b) (6)

On Friday, Aug 16:
> **WATCH:** Analysts will begin drafting and sending IOI reports directly from MMC App at Noon.

Training will consist of these topics:

- MMC App Implementation Timeline

- Concurrent Operations for Watch

- Using Outlook as primary send application, MMC App as secondary

    - MMC continues using current IOI format
    - SN continues using current GIR/GAR formats
- Coordinating reporting across MMC and SN watch desks
- Using MMC App
    - Viewing and creating main Reports (IOI/Steady State/NSS/ISS)
    - Viewing and creating other Reports (Tips/Other log entries)
    - Using Search
    - Using log/dashboard
    - Stats page
    - Admin section
- Priorities in a breaking news/incident situation

- Concurrent Operations for Project Time

- Live Conditions Testing
- Sources
- What we're looking for during testing
- Documenting Bugs/Errors

- Review of Backup Procedures in event MMC App is ever non-functional (After Aug.16)

- Who to contact immediately
- Manual Operations Checklist (b) (6) will create)
- Use of new IOI format within Outlook
- Continuing manual IOI numbering
- MMC Distribution List (Automatically sent to analysts once per week via email)
- What needs to be done when MMC App is back online

(b) (6)
Operations Analyst
DHS NOC Media Monitoring
(b) (6)

Teammates,

VERSION 2 Updated Guidance to: MMC Watch Standers and Senior Reviewers to Increase the Focus on Operationally Valuable Media Reporting

WHERE WE SEEM TO BE

It seems to me that ***we tend to drift away from the OPS NOC Priorities and Monitoring Report***, and ***particularly away from information/media reporting that we know the Secretary and her senior most staff must learn about right away***. MMC's ***central focus must always be to "provide timely and accurate reports on relevant media coverage in order to enrich OPS situational awareness, support executive decision making, and reduce the likelihood of surprise"***.

In this effort, we are aided by what we will call "standing critical information requirements (CIRs) and, the NOC Priorities and Monitoring Report which are generally issued multiple times daily". The CIRs are fairly broad, seldom change, and you can accommodate a wide variety of topics. The NOC Priorities and Monitoring Report are fairly straight forward, address anticipated or ongoing events, change modestly a few times daily, and are easily followed. I have discussed various potential IOIs with many of you and the ***questions and discussion always seems to revolve around "what is operationally valuable to the DHS Sec and OPS, and what is not"***.

Stay Away From IOI Reporting that:

- ***Addresses a policy issue, debate, or discussion***
- ***Characterizes a study, review, or assessment***
- ***Overviews proposed legislation or potential appeals on signed legislation***
- ***Has an obvious political bias or agenda***
- ***Criticizes the DHS or its leadership***
- ***Is predictive or futuristic***

As a matter then of routine, the ***MMC watch standers typically produce IOIs on events that are imminent, reported to have happened, or have already occurred:***

1. Manmade and natural domestic incidents, significant events, disasters – We have been publishing IOIs on these stories. We will continue publishing these IOIs to the full distribution list (FULLDIS). Pay particular attention to the geo-spatial location of the event.

2. Deepwater Horizon issues, progress, operations, and activities – We have been publishing IOIs on these stories. We will continue reporting these IOIs to the full distribution list (FULLDIS) as long as they relate to the Deepwater Horizon operations.

3. California wildfires, floods, and mudslides – We have been publishing IOIs on these stories. We will continue publishing these IOIs to the full distribution list (FULLDIS).

4. US/Mexico Border violence – We have been publishing IOIs on these stories. We will continue publishing these IOIs to the full distribution list (FULLDIS) as long the situation relates in some specific way to the United States and/or DHS. Such reports could include extraordinary brutality; unseen before use of technology; effects on U.S. border communities; and/or involve U.S. citizens being killed, injured, or kidnapped.

5. Counter drug stories in the western hemisphere – We have been publishing IOIs on these stories. We will continue publishing these IOIs to the full distribution list (FULLDIS) as long the situation relates in some specific way to the United States/or DHS; involves U.S. citizens being killed, injured, and/or kidnapped; or involves interagency/DHS component operations and/or publicity.

6. Mass/multiple killings or deaths – We have been publishing IOIs on these stories. These generally involve a mass/multiple killing at a public places such as malls, universities, and mass transit venues/locations. We have also covered mass/multiple killings that have occurred at public and private workplaces. We will continue publishing these IOIs to the full distribution list (FULLDIS) as long the situation relates in some specific way to the United States/or DHS; involves U.S. citizens being killed, injured, and/or kidnapped; or involves interagency/DHS component operations and/or publicity.

7. Domestic oil spills - We have been publishing IOIs on these stories. We will continue publishing these IOIs to the full distribution list (FULLDIS).

8. Afghanistan stories related to Taliban leaders being killed – We have been publishing IOIs on these stories. ***WE DON'T NEED TO ANY LONGER***...unless the Taliban leader has been connected recently in some

way to the United States. We will continue publishing these IOIs to the full distribution list (FULLDIS).

9. Terrorism stories to include – We have been publishing IOIs on these stories. We have seemed to publish IOIs whenever the "terrorism" word is present in the article, even when the terrorist or activity is reported to be in Chechnya. ***WE DON'T NEED TO ANY LONGER***...unless the terrorist, terrorist group, or terrorist activity has been connected recently in some way to the United States, or the event in another country (outside Iraq and Afghanistan) is exceptionally violent, i.e. a major attack on mass transit, or public infrastructure, or use unique means or technology.

10. Al Qaida leadership, activities, and threats – We have been publishing IOIs on these stories. We have seemed to publish IOIs whenever "Al Qaida" is referenced in an article. ***WE DON'T NEED TO ANY LONGER***...unless the Al Qaida reference is connected recently in some way to the United States, then we will publish the IOI to the full distribution list (FULLDIS).

11. Suspicious packages, white powder reports, HAZMAT report – We will generally publish these reports to the limited distribution list (LIMDIS). This unless the suspicious packages, white powder reports, HAZMAT situation is reported within the National Capitol Region or in proximity to national leaders or critical infrastructure in which case, we will publish the IOI to the full distribution list (FULLDIS).

12. School, public building, commercial building, mall, and sporting event lockdowns – We will generally publish these reports to the limited distribution list (LIMDIS). This unless the school, public building, and commercial building lock down is the result of a situation presenting a real and substantive threat to the children and/or occupants of the building; or the facility is located within the National Capitol Region or in proximity to national leaders or critical infrastructure in which case, we will publish the IOI to the full distribution list (FULLDIS).

13. Major disruption in the transportation system - We have been publishing IOIs on these stories. We will publish these IOIs to the limited distribution list (LIMDIS) if the incident involves a traffic accident that disrupts a major United States traffic artery. We will publish

these IOIs to the full distribution list (FULLDIS) when the situation relates in some specific way to DHS; involves suspicious circumstances; involves U.S. citizens being injured or killed; or involves interagency/DHS component operations and/or publicity.

14. Explosions – We will generally publish these reports to the limited distribution list (LIMDIS). This unless the explosion is reported within the National Capitol Region or in proximity to nation leaders or critical infrastructure in which case, we will publish the IOI to the full distribution list (FULLDIS).

I understand your ***frustrations that we're "damned if you do, damned if you don't"***. This played out again recently when the NOC was ***caught short for not alerting the distribution list when an explosion occurred at the Farragut West Metro Station***. The MMC watch checked all the normal sources and found only a Daily Caller report which indicated clearly that there didn't appear to be any malicious causes; a transformer had exploded; Metro service was not interrupted; there were no injuries; and MPD was on hand. No other coverage on line, radio, or TV occurred until 5-6 hours later which only repeated the early report. It ***seemed unreasonable that anyone would be upset that this hadn't been reported***. ***The point many missed, or did not think about, was that the proximity to certain Washington D.C. vital areas made it important for some on the distribution list to be assured that the explosion was not the result of a terrorist explosion or in any way endangered the vital areas.***

<u>SCORING POTENTIAL IOIs</u>

Scale	Description
5	Extremely time Sensitive; DHS Sec & senior staff need to know immediately; addresses DHS OPS CIRs/NOC Priorities and Monitoring Report directly; geospatially sensitive; adds significant operational value
4	Time sensitive; DHS senior staff need to know at the first opportunity; relates to a homeland security matter of interest; not currently a top priority; may be geospatially significant to other ongoing events; adds operational value
3	Uncertain time sensitivity; not currently a priority to federal officials; senior staff will be interested; addresses a storyline/situation that may become a matter of interest; additional information is required
2	Not time sensitive; indirectly relates to homeland security matter of interest, may be political, academic, or deliberative; GAO or other report about DHS organization/operation/etc
1	Not time sensitive; does not relate to DHS OPS CIRs or NOC Priorities and Monitoring Report; generally relates to a homeland security matter of interest; provides a political perspective, does not add operational value

As you approach your responsibilities as MMC watch standers***, use the below IOI Assessment Scoring Construct to assist you in assessing whether an IOI should be published for a particular story or a breaking event***. A ***"breaking event"*** will typically mean that the MMC watch stander will jabber the NOC SWO; MMC watch stander will also call the Senior Reviewer and/or MMC Project Manager; and a NOC blast call will occur. I recommend using the matrix provided below:

IOI ASSESSMENT SCORING CONSTRUCT

5 – If you score a story as a 5, you know an IOI absolutely must be published right away.

4 – If you score a story as a 4, you are saying it is important, and that you need to publish an IOI as soon as you can.

3 – If you score a story as a 3, you need to do further research and/or analysis, and score the story as either a 4 or a 2. If you change the score to a 4, you need to publish an IOI as soon as you can. If you change the score to a 2, you need to follow the rules below for scoring a story as a 2.

2 – If you score a story as a 2, you should not publish an IOI unless it is a follow-up to an earlier IOI. In that case, you may publish an IOI to the LIMDIS.

1 – If on the other hand, you score a story as a 1, you should conclude that an IOI absolutely should not be sent.

COORDINATING W/EACH OTHER & SENIOR REVIEWERS

We are rolling out the full-PIA authorized social media/networking capability next week and wanted to share some thoughts regarding ***"what can we do to take the MMC effort to the next level?"*** One easy thing that most recognize, is ***WE NEED TO RELY ON EACH OTHER MORE, YOU ALL COLLECTIVELY ON THOSE WHO HAVE BEEN THERE MUCH LONGER, AND ALL OF YOU ON BRAD, MITCH AND THE SENIOR REVIEWERS.*** There are simply times when the measureable gain in terms of speed and confidence that the MMC watch standers will get from using Brad, Mitch, or me as a sounding board is clear and significant. I want to review briefly what some of those times are from my perspective. These are times when you MUST call Brad, Mitch or the Senior Reviewer:

1) ***Something significant has occurred***

2) ***A particular report seems IOI worthy, but there are no corroborating reports***

3) ***The initial IOI worthy report and the corroborating report are not from the Source List we typically use***

4) ***The IOI worthy report reflects negatively on DHS or some other federal agency***

5) *It appears the IOI worthy report will require numerous updates and potentially be an enduring topic*

6) *You are not sure if an event has already been reported during a previous watch*

7) *You feel a correction must be issued*

8) *You are experiencing system problems – even if you have addressed them*

9) *Whenever you have to employ your backup system capabilities*

10) *You are simply not sure about a particular report and want a second opinion*

<u>MMC CONOPs GOING FORWARD</u>

1) *Relate MMC IOIs and social networking/media (SN) reports to standing CIRs, incident specific CIRs, and/or NOC Priorities and Monitoring Report*

2) *Corroborate IOI report with other SN posts, MMC reports, or other sources*

3) *Apply 1-5 IOI Assessment Scoring Construct to all potential IOIs*

4) *Generate IOIs through the MMC application (effective 16 Aug 2010)*

5) *Coordinate w/NOC SWO and Watch to closely monitor ongoing events*

6) *Coordinate all IOIs w/ social and traditional media watch counterpart*

7) *Determine IOI report has DHS incident or strategic value*

8) *Provide senior level review of draft IOI report*

9) *Distribute IOI reports to appropriate distribution list*
   A. *Distribution List A – full distribution group*
   B. *Distribution List B – limited distribution group (Internal MMC +* (b) (6) (b) (7)(E)
   C. *Distribution List C – special distribution group*

10) Complete a daily (Mon-Fri 1500) post processing review of all IOI reports (scoring the IOI's relevance, regular QC efforts still apply)

11) Provide structured daily feedback to MMC watch standers (spot check feedback on weekends)

Remember, if there is any doubt, call!

V/r, (b) (6)

Exercises:

Quiz: Drill trainee on basic terminology once they've read about the program basics and reviewed IOIs. What's the NOC? What's a SWO? Who gets our reports? What is an IOI? Who's (b) (6) Who's (b) (6) ? What are some of the differences between a MMC IOI and a SN IOI? Do the same for internal topics – What is the combined daily log? What is QC? How is it done? What do you do on a Project Time shift? Come up with any other questions you can think to ask.

Keywords: Have trainee think up his/her own list of keywords for a specific topic area, ie., border violence, drugs, weather, LNG. Critique that list, giving pointers from your experience on what works and what doesn't.
Then, have the trainee apply those keywords to twitter and blog searches. Ask the trainee to build a list of items that he/she feels would be candidates for IOIs. Critique that list.

Building IOIs without the App: Have the trainee build one IOI every 15 minutes, for 1 hour, based on different breaking news items. The content is not as important, the format is. The trainee should take a news article about anything and form it into an IOI, by hand in outlook.

Getting acquainted with the App (Testing Environment): Ask the trainee enter 10 fake IOIs on any topic, just to get used to entering things into the App. Review the IOIs produced. Make sure trainee also creates Steady-States, Phase reports.

PII: Prepare the trainee for the PII test

From: (b)(6),(b)(7)(C)
Sent: Thursday, May 07, 2009 7:10 PM
To: (b)(6),(b)(7)(C) DHS-RFI
Cc: (b)(6),(b)(7)(C)
Subject: (U) DHS Open Source Response to DHS RFI-461-CR-09-CIS
Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY

The DHS Open Source Response to (b)(6),(b)(7)(C) is as follows:

1) Open source has not found any information indicating that the subject of the RFI is involved in marriage fraud.

2) Open source has not found information that clarifies the status of any relationship between the subject and any publicly identified relatives or associates.

Social Networking Queries
A query of multiple social networking sites has not found any individual who is a match for the subject given the background information in the RFI. In addition, no individuals in an additional social networking query were name matches with the TPN number.

In general, social networking sites are open sources in so much as they are made publicly available. So if a match had been found, on USPER Facebook for example, that individual could restrict the availability of their profile to either members of networks they have joined or friends they have accepted. In that case, the individual would have a reasonable right to privacy, and access to that information would not be in the mission space of open source intelligence.

General Web Queries
Open source has not found any public statements by the subject related to immigration or marriage fraud.

There is a USPER ICQ website profile that matches the TPN name and country of birth information. If you have interest in this information, please let DHS Open Source know. As per your previous e-mail guidance, information relating to the subject's spouse has not been included.

Open source, given only the country and date of birth of the subject, could not independently verify that other individuals with variations of the subject's name or aliases, with a relationship to the subject's country of birth, are a match to the name given in the original RFI or the name amended to match with the TPN for the subject. For this reason, information about those individuals is not included.

Any feedback regarding these Open Source CORE Reports should be directed to the Department of Homeland Security Open Source Enterprise via unclassified e-mail at: (b) (6) Please include the OS Report Serial Number and Summary when corresponding about these reports.

v/r

(b)(6),(b)(7)(C)
DHS I&A CR
(b)(6),(b)(7)(C)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message

---

From: (b)(6),(b)(7)(C)
Sent: Thursday, May 07, 2009 3:23 PM
To: (b)(6),(b)(7)(C)
Subject: RE: Additional Information Request (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

I appreciate your quandary and I believe this could be an issue that would pop up again with this process. The problem is that we are in essence looking for indicators of immigration fraud. It is difficult to explain all the possible indicators briefly.

What we do know in this particular case is that marriage fraud was committed between the subject and the spouse you found. The spouse and child's information is not necessary or requested. However, the mention of a spouse and/or relative in connection to the subject would be permitted if publicly found on open networks. Identification would not be necessary or requested. For the sake of the trial run, I wanted to determine the benefit of the RFI process to see if there are indicators of marriage fraud in social network sites or personal websites with the subject. Any information found relating to marriage fraud would be publicly available information and could be valuable for investigation.

From the publicly available information you discovered on open source networks, we would see what we do not contain in our records and the relevancy to our investigations as well adjudications on immigration cases. I realize this makes it difficult for you since you need to determine the appropriate information to distribute. At this time, I would say that the subject's biographical information and any public statements by the subject on open source networks would be of potential value. The public statements would be anything that indicates possible abuses of the immigration system.

Does this help you understand what we are looking for? The goal essentially is to compare the subject's biographical information, statements that are related to immigration and is publicly available on open networks to official documents in order to determine immigration fraud.

V/r,

(b)(6),(b)(7)(C)
Intelligence Research Specialist
Intelligence Branch
Fraud Detection and National Security Division
Department of Homeland Security, USCIS
Washington, DC. HQFDNS.
E-mail: (b)(6),(b)(7)(C)
SIPR:
Fax: (b)(6),(b)(7)(C)

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE
WARNING: This document is FOR OFFICIAL USE ONLY. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C.552). This document is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to Sensitive But Unclassified (SBU) information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval from the originator. If you have received this document by mistake please contact the originator for specific handling and destruction procedures.

From: (b)(6),(b)(7)(C)
Sent: Thursday, May 07, 2009 1:58 PM
To: (b)(6),(b)(7)(C)
Subject: RE: Additional Information Request (b)(6),(b)(7)(C)

Hi (b)(6),(b)(7)(C)

I think that it would be easier for me to explain where we are at in the process by e-mailing you.

We are unsure about the exact information that you are looking for. We've found some information on people who have the same name as your subject. However, it is very difficult to verify that the individual we have found is in fact your subject because rarely are there multiple verifiers to corroborate that individual to the subject. Examples of that would be a birthdate or a specific location. It is a bit harder because of the aliases and the amount of individuals out there that can have variations on that name.

Because your subject has a TPN number, we are unsure about what you know and what you are actually looking for. We do have more information on the female that married him. We found where she works and that she has a son. Is this information that you know? If not we can send it along. If not, we are unsure that we will be able to provide you with information that you do not already know.

I have to go to a meeting right now that should last about 20 minutes.

I can respond to your reply after that.

Thanks,

(b)(6),(b)(7)(C)

v/r

(b)(6),(b)(7)(C)
DHS I&A CR
(b)(6),(b)(7)(C)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message

From: (b)(6),(b)(7)(C)
Sent: Thursday, May 07, 2009 7:08 AM
To: (b)(6),(b)(7)(C)
Cc:
Subject: RE: Additional Information Request (b)(6),(b)(7)(C)

Good morning (b)(6), (b)(7)(C)

Thank you for getting in touch. The name you have is correct, but is one of multiple aliases for the subject. The TPN you have is also correct.

Please let me know if you require more information, and we will wait for you to get in today. Ideally, we would like to limit the need for PII inputs and restrict it to the basics – name, DOB, COB and only if necessary, current residence and occupancy. Let me know if you would like the multiple aliases.

V/r,

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)
Intelligence Research Specialist
Intelligence Branch
Fraud Detection and National Security Division
Department of Homeland Security, USCIS
Washington, DC. HQFDNS.
E-m (b)(6),(b)(7)(C)
SIP
Fax:

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE
WARNING: This document is FOR OFFICIAL USE ONLY. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C.552). This document is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to Sensitive But Unclassified (SBU) information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval from the originator. If you have received this document by mistake please contact the originator for specific handling and destruction procedures.

From: Walsh, Danie (b)(6),(b)(7)(C)
Sent: Wednesday, May 06, 2009 7:39 PM
To (b)(6),(b)(7)(C)
Cc
Subject: RE: Additional Information Request (b)(6),(b)(7)(C)

Dear (b)(6),(b)(7)(C)

As per your RFI, we have been collecting, and have found, open source information on USPER (b)(6),(b)(7)(C) [first name, last name].

However, we believe the subject you are looking for is USPER (b)(6),(b)(7)(C) first name, last name], who is a name match with (b)(6),(b)(7)(C) According to our research, he is associated with USPER J (b)(6),(b)(7)(C) name match to (b)(6),(b)(7)(C) If this information is correct, we need an amendment to the RFI reflecting the name change. This would allow us to conduct open source research on this subject and then be able to disseminate it to you.

I would like to follow up with you in the morning. I get in at about 9.

Thanks,

(b)(6),(b)(7)(C)

v/r

(b)(6),(b)(7)(C)

DHS I&A CR
(b)(6),(b)(7)(C)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message

---

From: (b)(6),(b)(7)(C)
Sent: Wednesday, May 06, 2009 4:54 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: Additional Information Request (b)(6),(b)(7)(C)

Dear (b)(6),(b)(7)(C)

We have been corresponding with your colleague, (b)(6),(b)(7)(C) on this RFI. We are trying to find the specific analyst that is requesting this information, and you are listed on the RFI, so we are reaching out to you.

We have the following information on possible persons associated with the name (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)ocated in the Baltimore area:

- Possible aliases
- Related social security numbers
- Possible females associated with the subject

However, we are unable to confirm the subject's identity. Without further personal identifiable information, we will not be able to release any of the information we have collected thus far. If possible, can you provide a recent known address, social security number, or additional known aliases or associates for verification purposes?

If you have information that you would like to give us on the highside, please send to me at:
(b)(6),(b)(7)(C)

Also, due to a recent policy change from I&A leadership regarding dissemination; the report must be reviewed by CRCL, PRIV, OGC and IO prior to final distribution outside of I&A.

v/r

(b)(6),(b)(7)(C)
DHS I&A CR
(b)(6),(b)(7)(C)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message

---

From: (b)(6),(b)(7)(C)
Sent: Wednesday, April 22, 2009 10:28 AM
To:
Cc: (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
Subject: Access to Open Source Information

Attachments: UNCLASS DHS RFI Submission Form.doc

(b)(6),(b)(7)(C)

I work down in the NSRV IT PEO and have been working with OIT and DHS to come up with a solution to allow for FDNS users to gain access to open source information on individuals/groups (i.e. MySpace, Facebook, etc.). While a solution to allow each FDNS user the ability to opening search the internet may be a little ways off, I stumbled across an organization up at DHS I&A that does this work for the DHS Enterprise as requested by the RFI process. For example, Identify an relationship between Individual X and any extremist organizations/websites.

Would you be willing to sit down for 30 minutes this week to talk about conducting a pilot test to see if this option is a viable one for FDNS?

FDNS Intel…with your permission I'd like to work this pilot directly with my Collection Management contacts at DHS and work with you to come up with the formal process if we decide to implement this as an FDNS-wide solution.

I'm attaching the RFI form that we'll need to submit.

Thank you,
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)
U.S. Citizenship & Immigration Services
NSRV IT Program Executive Office
(b)(6),(b)(7)(C)

FOR OFFICIAL USE ONLY (FOUO) - This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C.§ 552). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

From: (b)(6),(b)(7)(C)
Sent: Thursday, April 23, 2009 11:30 AM
To: (b)(6),(b)(7)(C)
Subject: FW: DHS Open Source Enterprise/Program

Attachments: UNCLASS DHS RFI Submission Form.doc

Here is the RFI form…

(b)(6),(b)(7)(C)

U.S. Citizenship & Immigration Services

NSRV IT Program Executive Office

(b)(6),(b)(7)(C)

FOR OFFICIAL USE ONLY (FOUO) - This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C.§ 552). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

From: (b)(6),(b)(7)(C)
Sent: Tuesday, April 21, 2009 8:21 AM
To: (b)(6),(b)(7)(C)
Subject: RE: DHS Open Source Enterprise/Program

Hey (b)(6),(b)(7)(C)

Although I'd like to find out a bit more as to the nature of the requests (for my own understanding), Components should submit their requests using the standard RFI process (i.e. the form sent to DHS-RFI). I've attached a copy of the form in case you need to pass it along. I'll drop you a line later on today,

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Monday, April 20, 2009 4:26 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: DHS Open Source Enterprise/Program

(b)(6),(b)(7)(C)

Just had a mtg w/ subject office and need to find out how Components can submit requests for Open Source information on individuals and groups?

Thanks

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)
U.S. Citizenship & Immigration Services
NSRV IT PEO
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Wednesday, May 06, 2009 7:39 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: RE: Additional Information Request (b)(6),(b)(7)(C)

Dear (b)(6),(b)(7)(C)

As per your RFI, we have been collecting, and have found, open source information on USPER (b)(6),(b)(7)(C) [first name, last name].

However, we believe the subject you are looking for is USPER (b)(6), (b)(7)(C) [first name, last name], who is a name match with (b)(6),(b)(7)(C) According to our research, he is associated with USPER (b)(6),(b)(7)(C) name match to (b)(6),(b)(7)(C) If this information is correct, we need an amendment to the RFI reflecting the name change. This would allow us to conduct open source research on this subject and then be able to disseminate it to you.

I would like to follow up with you in the morning. I get in at about 9.

Thanks,

(b)(6),(b)(7)(C)

v/r

(b)(6),(b)(7)(C)
DHS I&A CR
(b)(6),(b)(7)(C)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message

---

From: (b)(6),(b)(7)(C)
Sent: Wednesday, May 06, 2009 4:54 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: Additional Information Request (b)(6),(b)(7)(C)

Dea(b)(6),(b)(7)(C)

We have been corresponding with your colleague, (b)(6),(b)(7)(C)n this RFI. We are trying to find the specific analyst that is requesting this information, and you are listed on the RFI, so we are reaching out to you.

We have the following information on possible persons associated with the name(b)(6),(b)(7)(C) (b)(6),(b)(7)(C)cated in the Baltimore area:

- Possible aliases
- Related social security numbers
- Possible females associated with the subject

However, we are unable to confirm the subject's identity. Without further personal identifiable information, we will not be able to release any of the information we have collected thus far. If possible, can you provide a recent known address, social security number, or additional known aliases or associates for verification purposes?

If you have information that you would like to give us on the highside, please send to me at:
(b)(6),(b)(7)(C)

Also, due to a recent policy change from I&A leadership regarding dissemination; the report must be reviewed by CRCL, PRIV, OGC and IO prior to final distribution outside of I&A.

v/r

(b)(6),(b)(7)(C)
DHS I&A CR
(b)(6),(b)(7)(C)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message

---

From: (b)(6),(b)(7)(C)
Sent: Friday, May 08, 2009 7:47 AM
To: (b)(6),(b)(7)(C)
Cc:
Subject: RE: (U) DHS Open Source Response to(b)(6),(b)(7)(C)

Good morning,

For everyone's visibility/records, this RFI has been processed and completed. We will close it in our database. If there are any further questions, please contact any of our team members listed below.

Thank you.

Very Respectfully,

Customer Assurance Branch (DHS-RFI)
Office of Intelligence and Analysis / Reporting and Production Division
Department of Homeland Security

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Thursday, May 07, 2009 7:10 PM
To:
Cc: (b)(6),(b)(7)(C)

Subject: (U) DHS Open Source Response to DHS(b)(6),(b)(7)(C)

Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY

The DHS Open Source Response to (b)(6),(b)(7)(C)s as follows:

1) Open source has not found any information indicating that the subject of the RFI is involved in marriage fraud.

2) Open source has not found information that clarifies the status of any relationship between the subject and any publicly identified relatives or associates.

<u>Social Networking Queries</u>
A query of multiple social networking sites has not found any individual who is a match for the subject given the background information in the RFI. In addition, no individuals in an additional social networking query were name matches with the TPN number.

In general, social networking sites are open sources in so much as they are made publicly available. So if a match had been found, on USPER Facebook for example, that individual could restrict the availability of their profile to either members of networks they have joined or friends they have accepted. In that case, the individual would have a reasonable right to privacy, and access to that information would not be in the mission space of open source intelligence.

<u>General Web Queries</u>
Open source has not found any public statements by the subject related to immigration or marriage fraud.

There is a USPER ICQ website profile that matches the TPN name and country of birth information. If you have interest in this information, please let DHS Open Source know. As per your previous e-mail guidance, information relating to the subject's spouse has not been included.

Open source, given only the country and date of birth of the subject, could not independently verify that other individuals with variations of the subject's name or aliases, with a relationship to the subject's country of birth, are a match to the name given in the original RFI or the name amended to match with the TPN for the subject. For this reason, information about those individuals is not included.

Any feedback regarding these Open Source CORE Reports should be directed to the Department of Homeland Security Open Source Enterprise via unclassified e-mail at: (b)(6),(b)(7)(C) Please include the OS Report Serial Number and Summary when corresponding about these reports.

v/r

(b)(6),(b)(7)(C)
DHS I&A CR
(b)(6),(b)(7)(C)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message

From: (b)(6),(b)(7)(C)
Sent: Thursday, May 07, 2009 3:23 PM
To: (b)(6),(b)(7)(C)
Subject: RE: Additional Information Request (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

I appreciate your quandary and I believe this could be an issue that would pop up again with this process. The problem is that we are in essence looking for indicators of immigration fraud. It is difficult to explain all the possible indicators briefly.

What we do know in this particular case is that marriage fraud was committed between the subject and the spouse you found. The spouse and child's information is not necessary or requested. However, the mention of a spouse and/or relative in connection to the subject would be permitted if publicly found on open networks. Identification would not be necessary or requested. For the sake of the trial run, I wanted to determine the benefit of the RFI process to see if there are indicators of marriage fraud in social network sites or personal websites with the subject. Any information found relating to marriage fraud would be publicly available information and could be valuable for investigation.

From the publicly available information you discovered on open source networks, we would see what we do not contain in our records and the relevancy to our investigations as well adjudications on immigration cases. I realize this makes it difficult for you since you need to determine the appropriate information to distribute. At this time, I would say that the subject's biographical information and any public statements by the subject on open source networks would be of potential value. The public statements would be anything that indicates possible abuses of the immigration system.

Does this help you understand what we are looking for? The goal essentially is to compare the subject's biographical information, statements that are related to immigration and is publicly available on open networks to official documents in order to determine immigration fraud.

V/r,

(b)(6),(b)(7)(C)
Intelligence Research Specialist
Intelligence Branch
Fraud Detection and National Security Division
Department of Homeland Security, USCIS
Washington, DC. HQFDNS.
(b)(6),(b)(7)(C)

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE
WARNING: This document is FOR OFFICIAL USE ONLY. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C.552). This document is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to Sensitive But Unclassified (SBU) information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval from the originator. If you have received this document by mistake please contact the originator for specific handling and destruction procedures.

From: (b)(6),(b)(7)(C)
Sent: Thursday, May 07, 2009 1:58 PM

To: (b)(6),(b)(7)(C)
Subject: RE: Additional Information Request (b)(6),(b)(7)(C)

Hi (b)(6),(b)(7)(C)

I think that it would be easier for me to explain where we are at in the process by e-mailing you.

We are unsure about the exact information that you are looking for. We've found some information on people who have the same name as your subject. However, it is very difficult to verify that the individual we have found is in fact your subject because rarely are there multiple verifiers to corroborate that individual to the subject. Examples of that would be a birthdate or a specific location. It is a bit harder because of the aliases and the amount of individuals out there that can have variations on that name.

Because your subject has a TPN number, we are unsure about what you know and what you are actually looking for. We do have more information on the female that married him. We found where she works and that she has a son. Is this information that you know? If not we can send it along. If not, we are unsure that we will be able to provide you with information that you do not already know.

I have to go to a meeting right now that should last about 20 minutes.

I can respond to your reply after that.

Thanks,

(b)(6),(b)(7)(C)

v/r

(b)(6),(b)(7)(C)
DHS I&A CR
(b)(6),(b)(7)(C)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message

---

From: (b)(6),(b)(7)(C)
Sent: Thursday, May 07, 2009 7:08 AM
To:
Cc: (b)(6),(b)(7)(C)
Subject: RE: Additional Information Request (b)(6),(b)(7)(C)

Good morning (b)(6),(b)(7)(C)

Thank you for getting in touch. The name you have is correct, but is one of multiple aliases for the subject. The TPN you have is also correct.

Please let me know if you require more information, and we will wait for you to get in today. Ideally, we would like to limit the need for PII inputs and restrict it to the basics – name, DOB, COB and only if necessary, current residence and occupancy. Let me know if you would like the multiple aliases.

V/r,

(b)(6),(b)(7)(C)

Intelligence Research Specialist
Intelligence Branch
Fraud Detection and National Security Division
Department of Homeland Security, USCIS
Washington, DC, HQFDNS
(b)(6),(b)(7)(C)

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE
WARNING: This document is FOR OFFICIAL USE ONLY. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C.552). This document is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to Sensitive But Unclassified (SBU) information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval from the originator. If you have received this document by mistake please contact the originator for specific handling and destruction procedures.

From: (b)(6),(b)(7)(C)
Sent: Wednesday, May 06, 2009 7:39 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: RE: Additional Information Request (b)(6),(b)(7)(C)

Dear (b)(6),(b)(7)(C)

As per your RFI, we have been collecting, and have found, open source information on USPER Ismail Abdelwahab [first name, last name].

However, we believe the subject you are looking for is USPER (b)(6),(b)(7)(C) [first name, last name], who is a name match with (b)(6),(b)(7)(C). According to our research, he is associated with USPER (b)(6),(b)(7)(C) name match to (b)(6),(b)(7)(C) If this information is correct, we need an amendment to the RFI reflecting the name change. This would allow us to conduct open source research on this subject and then be able to disseminate it to you.

I would like to follow up with you in the morning. I get in at about 9.

Thanks,

(b)(6),(b)(7)(C)

v/r

(b)(6),(b)(7)(C)
DHS I&A CR
(b)(6),(b)(7)(C)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message

---

From: (b)(6),(b)(7)(C)
Sent: Wednesday, May 06, 2009 4:54 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: Additional Information Request (b)(6),(b)(7)(C)

Dear (b)(6),(b)(7)(C)

We have been corresponding with your colleague, (b)(6),(b)(7)(C) on this RFI. We are trying to find the specific analyst that is requesting this information, and you are listed on the RFI, so we are reaching out to you.

We have the following information on possible persons associated with the name Ismail Abdelwahab located in the Baltimore area:

- Possible aliases
- Related social security numbers
- Possible females associated with the subject

However, we are unable to confirm the subject's identity. Without further personal identifiable information, we will not be able to release any of the information we have collected thus far. If possible, can you provide a recent known address, social security number, or additional known aliases or associates for verification purposes?

If you have information that you would like to give us on the highside, please send to me at:
(b)(6),(b)(7)(C)

Also, due to a recent policy change from I&A leadership regarding dissemination; the report must be reviewed by CRCL, PRIV, OGC and IO prior to final distribution outside of I&A.

v/r

(b)(6),(b)(7)(C)
DHS I&A CR
(b)(6),(b)(7)(C)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message

---

From: (b)(6),(b)(7)(C)
Sent: Wednesday, May 06, 2009 9:55 AM

To: (b)(6),(b)(7)(C)
Subject: Re: RFI Trial

Ok. Will need to provide some more info if we hope to get some valuable information back. Occupation or school shouldn't be too sensitive to provide.

(b)(6),(b)(7)(C)
U.S. Citizenship & Immigration Services
NSRV IT PEO
Phon(b)(6),(b)(7)(C)
Cell:
(b)(6),(b)(7)(C)

----- Original Message -----
From: (b)(6),(b)(7)(C)
To: (b)(6),(b)(7)(C)
Sent: Wed May 06 09:52:33 2009
Subject: RE: RFI Trial

The subject has an extensive employment history and did attend an identified U.S. School. The subject resides primarily in Maryland, and his immigration history to date is limited to Maryland.

Beyond that, I do not want to provide further private information on the subject. We can discuss this in person to determine what information would be necessary to provide.

V/r,

(b)(6),(b)(7)(C)
Intelligence Research Specialist
Intelligence Branch
Fraud Detection and National Security Division Department of Homeland Security,
USCIS Washington, DC HQFDNS
E-ma(b)(6), (b)(7)(C)
SIPR
Fax:

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE
WARNING: This document is FOR OFFICIAL USE ONLY. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C.552). This document is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to Sensitive But Unclassified (SBU) information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval from the originator. If you have received this document by mistake please contact the originator for specific handling and destruction procedures.

-----Original Message-----
From: (b)(6),(b)(7)(C)
Sent: Wednesday, May 06, 2009 9:44 AM
To: (b)(6),(b)(7)(C)
Subject: RE: RFI Trial

(b)(6),(b)(7)(C)

I just received a call from the Open Source Office. Can you provide any more clarifying information on the individual we need info on? Occupation, School, etc.

They have come up with a few individuals from Egypt with the same name and want to get us information on the right guy.

Thanks,
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)
U.S. Citizenship & Immigration Services
NSRV IT Program Executive Office
Phone: (202)272-9658
(b)(6),(b)(7)(C)

FOR OFFICIAL USE ONLY (FOUO) - This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C.§ 552). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

-----Original Message-----
From: (b)(6),(b)(7)(C)
Sent: Wednesday, April 29, 2009 1:26 PM
To: (b)(6),(b)(7)(C)
Subject: RE: RFI Trial

(b)(6),(b)(7)(C)

Attached is the form with the modifications to my request that we discussed. Thank you for taking the time to meet with me to discuss it.

Please let me know if there any questions and have a nice week.

V/r,

(b)(6),(b)(7)(C)
Intelligence Research Specialist
Intelligence Branch
Fraud Detection and National Security Division Department of Homeland Security,
USCIS Washington, DC. HQFDNS.
(b)(6),(b)(7)(C)

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE
WARNING: This document is FOR OFFICIAL USE ONLY. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C.552). This document is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to Sensitive But Unclassified (SBU) information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval from the originator. If you have received this document by mistake please contact the originator for specific handling and destruction procedures.

-----Original Message-----
From: (b)(6),(b)(7)(C)
Sent: Wednesday, April 29, 2009 10:21 AM
To: (b)(6),(b)(7)(C)
Subject: Re: RFI Trial

How about 1130?

(b)(6),(b)(7)(C)
U.S. Citizenship & Immigration Services
NSRV IT PEO
(b)(6),(b)(7)(C)

----- Original Message -----
From: (b)(6),(b)(7)(C)
To: (b)(6),(b)(7)(C)
Sent: Wed Apr 29 10:20:16 2009
Subject: RE: RFI Trial

Would 11:15 work for you? If not, I can meet at a time preferable for you after 1 PM.

-----Original Message-----
From: (b)(6),(b)(7)(C)
Sent: Wednesday, April 29, 2009 10:20 AM
To (b)(6),(b)(7)(C)
Subject: Re: RFI Trial

Sure. What time?

(b)(6),(b)(7)(C)
U.S. Citizenship & Immigration Services
NSRV IT PEO
(b)(6),(b)(7)(C)

----- Original Message -----
From: (b)(6),(b)(7)(C)
To: (b)(6),(b)(7)(C)
Sent: Wed Apr 29 10:18:56 2009
Subject: RFI Trial

Good morning (b)(6),(b)(7)(C)

I have a name I would like to submit for the trial run we discussed last week. However, I do have a concern I would like to address in person. Do you have time today to discuss it briefly? If you don't have time, perhaps we can discuss it next week?

V/r,

(b)(6),(b)(7)(C)

Intelligence Research Specialist

Intelligence Branch

Fraud Detection and National Security Division

Department of Homeland Security, USCIS

Washington, DC. HQFDNS.

E-mail: (b)(6),(b)(7)(C)

SIPR:

Fax: (b)(6),(b)(7)(C)

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE
WARNING: This document is FOR OFFICIAL USE ONLY. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C.552). This document is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to Sensitive But Unclassified (SBU) information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval from the originator. If you have received this document by mistake please contact the originator for specific handling and destruction procedures.

From (b)(6),(b)(7)(C)
Sent: Wednesday, May 21, 2008 10:13 AM
To (b)(6),(b)(7)(C)
Cc
Subject: Social Networking Sites

Attachments: MySpace Case 5-21-08 (2).doc
(b)(6),(b)(7)(C)

Here is the report you asked for on the MySpace case. If you have any questions or need anything else just let me know.

Thanks,

(b)(6)

(b)(6)
District Adjudications Officer
U.S. Department of Homeland Security
U.S. Citizenship & Immigration Services
415 N. 3rd Street
Yakima, WA 98903
(b)(6)

Before printing, please think about the environment

U.S. Department of Homeland Security
415 North 3rd St.
Yakima, WA 98901

U.S. Citizenship
and Immigration
Services

Social Networking Sites and Their Importance to FDNS

The Internet has made it increasingly easier for people to get connected with each other whether that is with long-distance family, friends, or to find new loves and friendships. Social networking sites such as MySpace, Facebook, Classmates, Hi-5, and other similar sites are designed to allow people to share their creativity, pictures, and information with others. Sometimes people do this to find romance, sometimes they do it to find friends with similar interests, and sometimes they do it to keep in touch with family. Narcissistic tendencies in many people fuels a need to have a large group of "friends" link to their pages and many of these people accept cyber-friends that they don't even know. This provides an excellent vantage point for FDNS to observe the daily life of beneficiaries and petitioners who are suspected of fraudulent activities. Generally, people on these sites speak honestly in their network because all of their friends and family are interacting with them via IM's (Instant Messages), Blogs (Weblog journals), etc. This social networking gives FDNS an opportunity to reveal fraud by browsing these sites to see if petitioners and beneficiaries are in a valid relationship or are attempting to deceive CIS about their relationship. Once a user posts online, they create a public record and timeline of their activities. In essence, using MySpace and other like sites is akin to doing an unannounced cyber "site-visit" on a petitioners and beneficiaries.

Here is a step-by-step process of how a generic social networking website works:

1. A user registers an email address and password with the site thus creating a unique account.
2. Typically, the website sends a confirmation email to the user's address to validate that person's identity.
3. The user may then create a profile. This profile may contain whatever information the user decides to publish online. The user can decide whether to make the profile public or private. The user may change or manipulate information in his profile at any time. In this step, the new user can become a member of a number of networks. These networks can be based on high school, hometown, job, church, or any other type of social group.
4. Anyone may search for another user by complete name, screen name or email address and request to be that user's "friend." That user can deny or agree to the "friend" request.
5. When adding a user as a "friend" the accepting user can now see your profile including all the personal information entered into the profile. The new friend can also see any new information the user may add at a later date such as an online journal entry or photographs.

6. By repeating steps four and five the user will gradually accumulate a large list of friends effectively becoming part of the social network.

A list of social networking sites and the countries where they are popular can be found on Wikipedia at this link: http://en.wikipedia.org/wiki/List_of_social_networking_websites

Here are a few social networking sites that most people are familiar with; the number of registered users is astounding.

Name	Description/Focus	Registered users	Registration	Global Page ranking (May 08)	Active Users
Badoo	General, Popular in Europe	13,000,000[9]	Open to people 18 and older	213[10]	
Bebo	General, Popular in the US, UK, Ireland, NZ and the Pacific Islands	40,000,000[13]	Open to people 13 and older	108[14]	
Buzznet	Music and pop-culture	10,000,000[18]	Open	498[19]	
Classmates.com	School, college, work and the military	50,000,000[21]	Open	923[22]	12,800,000[23]
Cyworld	Young South Koreans	2,100,000[24]	Open	223[25]	
Facebook	General. Popular Worldwide.	70,000,000[26]	Open to people 13 and older.	8[27]	
Habbo	General. Over 31 communities worldwide. Chat Room and user profiles.	82,000,000[46]	Open to people 13 and older	4,050[47]	
hi5	General. Teen based. Popular in Cyprus, Romania and Latin America.	70,000,000[48]	Open to people 13 and older	19[49]	
imeem	Music, Video, Photos, Blogs	26,000,000[51]	Open	140[52]	
MiGente.com	Latinos	2,800,000[62]	Open	5,266[63]	
Muxlim	Muslim social networking	2,400,000[69]	Open to people 13 and older	150[70]	
MySpace	General. Popular Worldwide.	110,000,000[72]	Open to people 14 and older.	6[73]	
myYearbook	General	5,100,000[74]	Open to age 13 and up & Grades 9 and up	894[75]	
Netlog	Formerly known as Facebox.	28,000,000[78]	Open	112[79]	
Reunion.com	Locating friends and family, keeping in touch	32,000,000[87]	Open	2,311[88]	
Windows LiveSpaces	Blogging (formerly MSN Spaces)	120,000,000[109]	Open	4[110]	

From: (b)(6),(b)(7)(C)
Sent: Monday, October 26, 2009 4:24 PM
To: (b)(6),(b)(7)(C)
Subject: FW: Anonymous Web Surfing

Importance: High

Follow Up Flag: Follow up
Flag Status: Purple

More of the same…

(b)(6),(b)(7)(C)
Chief of Staff - HQ FDNS
(b)(6),(b)(7)(C)

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C.§ 552). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

From: (b)(6),(b)(7)(C)
Sent: Monday, September 15, 2008 12:10 PM
To:
Cc: (b)(6),(b)(7)(C)
(b)(6),(b)(7
Subject: FW: Anonymous Web Surfing
Importance: High

(b)(6),(b)(7)(C)

Let me know if you need additional real-world examples of how these inexplicable limitations to our intelligence and immigration officers to access "un-trusted" websites are seriously degrading our national security and public safety missions.

V/R,
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) | DHS | USCIS | HQFDNS | **Chief Intelligence Branch** | (b)(6),(b)(7)(C) *BlackBerry*:
(b)(6),(b)(7)(C)

WARNING: This email contains a document (s) categorized as FOR OFFICIAL USE ONLY (FOUO). The document (s) contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). This email and its attachment (s) are to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to Sensitive But Unclassified (SBU) information and are not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval from the originator.

From: (b)(6),(b)(7)(C)
Sent: Monday, September 15, 2008 11:52 AM
To: (b)(6),(b)(7)(C)
Cc:
Subject: Re: Anonymous Web Surfing

(b)(6),(b)(7)(C)

Definitely...you've been on my latest emails concerning this, correct?

If not, 'll talk to you this afternoon.

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)
U.S. Citizenship & Immigration Services
NSRV IT PEO
(b)(6),(b)(7)(C)

----- Original Message -----
From (b)(6),(b)(7)(C)
To (b)(6),(b)(7)(C)
Sent: Mon Sep 15 11:37:45 2008
Subject: FW: Anonymous Web Surfing

(b)(6),(b)(7)(C)

Can we discuss this?

Thanks.

(b)(6),(b)(7)(C)

From (b)(6),(b)(7)(C)
Sent: Monday, September 15, 2008 11:28 AM
To: (b)(6),(b)(7)(C)
Subject: Anonymous Web Surfing

Good Morning,

I'm hoping that you can help me or forward this to the appropriate POC. Some time ago there was a request from the field for a browsing solution to visit possible benefit fraud target websites without loudly broadcasting that DHS was checking on them. At that time it appeared that HQ was looking at Proxify as the solution. (Not the best but better than nothing) I am trying to find out the status of this project. The inability to anonymously search websites severely hampers our anti-fraud efforts. Additionally, it presents the opportunity for FDNS to inadvertently alert the target(s) that might be under investigation by local, state or federal LEA. This clearly creates operational and officer safety concerns for the LEA.

Would it be possible to get an update on this issue?

(b)(6),(b)(7)(C)

Supervisory Immigration Officer

Northeast Regional Office- FDNS

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Monday, October 26, 2009 4:24 PM
To: (b)(6),(b)(7)(C)
Subject: FW: Open Source Unfettered Access

Follow Up Flag: Follow up
Flag Status: Purple

Here is what I thought I would find.

(b)(6),(b)(7)(C)
Chief of Staff - HQ FDNS
(b)(6),(b)(7)(C)

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C.§ 552). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

From: (b)(6),(b)(7)(C)
Sent: Tuesday, September 16, 2008 8:35 AM
To: (b)(6),(b)(7)(C)
Cc:
Subject: RE: Open Source Unfettered Access

(b)(5),(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) | **DHS| USCIS| HQFDNS| Chief Intelligence Branch** | ☎: (b)(6),(b)(7)(C) *BlackBerry*:
✉ (b)(6),(b)(7)(C)

WARNING: This email contains a document (s) categorized as FOR OFFICIAL USE ONLY (FOUO). The document (s) contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). This email and its attachment (s) are to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to Sensitive But Unclassified (SBU) information and are not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval from the originator.

From: (b)(6),(b)(7)(C)
Sent: Tuesday, September 16, 2008 7:14 AM
To: (b)(6),(b)(7)(C)

(b)(6)

Cc: (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
Subject: RE: Open Source Unfettered Access

(b)(6),(b)(7)(C)

I just left you a voicemail but wanted to follow up with an email in case you have access to your email while you're out of the office. Would you like to set up a meeting for Tuesday when you're back in with myself and the folks from FDNS?

Thank you,
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)
U.S. Citizenship & Immigration Services
NSRV IT Program Executive Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Monday, September 15, 2008 9:43 AM
To: (b)(6),(b)(7)(C)
Cc:
(b)(6),(b)(7)(C)
Subject: RE: Open Source Unfettered Access

(b)(6),(b)(7)(C)

I am waiting to hear fron (b)(6),(b)(7)(C)
Your estimate of 500 USCIS authorized users is adequate.

Thank you,
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) | **DHS| USCIS| HQFDNS| Chief Intelligence Branch** |☎: (b)(6),(b)(7)(C) |*BlackBerry:*
-✉: (b)(6),(b)(7)(C)

WARNING: This email contains a document (s) categorized as FOR OFFICIAL USE ONLY (FOUO). The document (s) contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). This email and its attachment (s) are to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to Sensitive But Unclassified (SBU) information and are not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval from the originator.

-----Original Message-----
From: (b)(6),(b)(7)(C)
Sent: Monday, September 15, 2008 8:54 AM
To: (b)(6),(b)(7)(C)
Cc:
(b)(6),(b)(7)(C)

(b)(6)

Subject: RE: Open Source Unfettered Access

(b)(6),(b)(7)(C)

Checking back in to see where we stood on this.

OIT is still working the solution...should we engineer this capability to support 500 users or is this number too high or too low?

Thanks,
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)
U.S. Citizenship & Immigration Services
NSRV IT Program Executive Office
(b)(6),(b)(7)(C)

-----Original Message-----
From: (b)(6),(b)(7)(C)
Sent: Tuesday, September 09, 2008 10:06 AM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)
Subject: RE: Open Source Unfettered Access

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) and I have been working on a solution to this critical issue since the first web access restrictions were implemented few months ago.
Let me know if you need additional information or clarification.
V/R,
Luis

(b)(6),(b)(7)(C)
Chief, Intelligence Branch
Fraud Detection & National Security
DHS-USCIS
(b)(6),(b)(7)(C)

-----Original Message-----
From: (b)(6),(b)(7)(C)
Sent: Tuesday, September 09, 2008 7:40 AM
To: (b)(6),(b)(7)(C)
Cc:
Subject: Re: Open Source Unfettered Access

Addin (b)(6),(b)(7)(C)

It is at the very least shallow cover that is not backstopped.
(b)(6),(b)(7)(C) Chief
National Security & Records Verification Law Division
USCIS Office of Chief Counsel
(b)(6),(b)(7)(C)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message. Thank you.

----- Original Message -----
From: (b)(6),(b)(7)(C)
To:
Cc:
Sent: Tue Sep 09 07:47:18 2008
Subject: RE: Open Source Unfettered Access

One question…when the analysts log into sites like MySpace or Facebook, what are they using as their profile? If they're making up email addresses and profiles, which are required by most sites to log in to, wouldn't that be considered covert actions and a potential issue?

(b)(6),(b)(7)(C)

U.S. Citizenship & Immigration Services

NSRV IT Program Executive Office

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Tuesday, September 09, 2008 7:45 AM

To: (b)(6),(b)(7)(C)
Cc:
Subject: RE: Open Source Unfettered Access
Importance: High

Nothing…, nada…, niente…, zilch…, zero…,

In the interim, the field has given up on HQ's ability to resolve this critical situation and they're implementing their own temporary solutions to unfettered open source access.

(b)(6),(b)(7)(C)

Chief, Intelligence Branch

Fraud Detection & National Security

DHS-USCIS

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Tuesday, September 09, 2008 7:19 AM
To: (b)(6),(b)(7)(C)
Subject: FW: Open Source Unfettered Access

(b)(6),(b)(7)(C)

Anything further come of this?

Thanks,

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

U.S. Citizenship & Immigration Services

NSRV IT Program Executive Office

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Tuesday, September 02, 2008 4:13 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: Re: Open Source Unfettered Access

(b)(6),(b)(7)(C)

Please provide any new requests you receive to Commercial Law (b)(6),(b)(7)(C) via the email listed above.

(b)(6), (b)(7)(C)
National Security & Records Verification Law Division
USCIS Office of Chief Counsel
(b)(6),(b)(7)(C)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message. Thank you.

----- Original Message -----

Fro (b)(6),(b)(7)(C)
To:
Cc:
Sent: Tue Sep 02 14:54:15 2008
Subject: RE: Open Source Unfettered Access

(b)(6),(b)(7)(C)

Since our meeting additional offices outside of FDNS have stated a requirement for a similar capability. Would this be handled by Commercial Law as well?

I'm having our IT SOC pull data on the number of requests and organizations affected by this situation so we know the scope of the issue.

Thank you,

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

U.S. Citizenship & Immigration Services

NSRV IT Program Executive Office

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Tuesday, September 02, 2008 2:49 PM
To: (b)(6),(b)(7)(C)

Cc: (b)(6),(b)(7)(C)
Subject: RE: Open Source Unfettered Access

(b)(6),(b)(7)(C)

I met with (b)(6),(b)(7)(C) today and described in a nutshell your request. We should be able to discuss in a day or so.

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Chief

National Security & Records Verification Law Division

Office of Chief Counsel

US Citizenship and Immigration Services

(b)(6),(b)(7)(C)

This e-mail (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain Attorney Work Product information that is privileged, confidential, or otherwise protected by applicable law. If the reader of this e-mail is not the intended recipient or the employee or agent responsible for delivering the e-mail to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this e-mail or its contents is strictly prohibited. If you have received this e-mail in error, please notify us immediately by replying to this message, and please destroy all copies of this e-mail.

(b)(6)

From: (b)(6),(b)(7)(C)
Sent: Tuesday, September 02, 2008 10:49 AM
To: (b)(6),(b)(7)(C)
Cc:
Subject: RE: Open Source Unfettered Access

(b)(6),(b)(7)(C)

Thank you.

I'm standing by.

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Chief, Intelligence Branch

Fraud Detection & National Security

DHS-USCIS

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Tuesday, September 02, 2008 10:28 AM
To: (b)(6),(b)(7)(C)
Cc:
Subject: Re: Open Source Unfettered Access

(b)(6),(b)(7)(C)

I will touch base with Commercial Law and see if they are available.

Tony
(b)(6),(b)(7)(C) Chief
National Security & Records Verification Law Division
USCIS Office of Chief Counsel
(b)(6),(b)(7)(C)

(b) (6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message. Thank you.

----- Original Message -----
Fro (b)(6),(b)(7)(C)
To:
Cc:
(b)(6),(b)(7)(
Sent: Tue Sep 02 10:25:51 2008
Subject: RE: Open Source Unfettered Access

(b)(6),(b)(7)(C)

I'm available to meet with you on a short notice.

Thanks,
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Chief, Intelligence Branch

Fraud Detection & National Security

DHS-USCIS
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Tuesday, September 02, 2008 10:14 AM
To: (b)(6),(b)(7)(C)
Cc:
Subject: Re: Open Source Unfettered Access

(b)(6),(b)(7)(C)

Let me know when the meeting is and I'll be sure to be there.

(b) (6)

(b)(6),(b)(7)(C) [redacted]

(b)(6),(b)(7)(C) [redacted]
U.S. Citizenship & Immigration Services
NSRV IT PEO
(b)(6),(b)(7)(C) [redacted]

----- Original Message -----
From: (b)(6),(b)(7)(C) [redacted]
To: (b)(6),(b)(7)(C) [redacted]
Cc:
(b)(6),(b)(7)(C) [redacted]
Sent: Fri Aug 29 15:40:03 2008
Subject: RE: Open Source Unfettered Access

(b)(6),(b)(7)(C) [redacted]

Let's talk on Tuesday. Commercial Law has been given the lead for this issue.

(b)(6),(b)(7)(C) [redacted]

(b)(6),(b)(7)(C) [redacted]

Chief

National Security & Records Verification Law Division

Office of Chief Counsel

US Citizenship and Immigration Services

(b)(6),(b)(7)(C) [redacted]

This e-mail (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain Attorney Work Product information that is privileged, confidential, or otherwise protected by applicable law. If the reader of this e-mail is not the intended recipient or the employee or agent responsible for delivering the e-mail to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this e-mail or its contents is strictly prohibited. If you have received this e-mail in error, please notify us immediately by replying to this message, and please destroy all copies of this e-mail.

From: (b)(6),(b)(7)(C)
Sent: Wednesday, August 27, 2008 6:55 PM
To (b)(6),(b)(7)(C)
Cc
Subject: Open Source Unfettered Access
Importance: High

(b)(6),(b)(7)(C)

I need to meet with you and get an OGC update on the Open Source access solution that (b)(6),(b)(7)(C) nailed you?

Thank you for your prompt consideration,

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Chief, Intelligence Branch

Fraud Detection & National Security

DHS-USCIS

(b)(6),(b)(7)(C)