
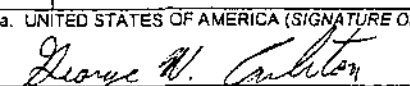


Offeror

Grant Thornton, LLP

b3

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30				1. REQUISITION NUMBER 21-05-205-FIN-005		PAGE 1 OF 41		
2. CONTRACT NO. GS-23-F-8196H		3. AWARD EFFECTIVE DATE See Block 31c	4. ORDER NUMBER HSTS03-05-P-FIN005	5. SOLICITATION NUMBER HSTS03-05-Q-FIN005		6. SOLICITATION ISSUE DATE		
7. FOR SOLICITATION INFORMATION CALL:		a. NAME		b. TELEPHONE NUMBER (No collect calls)		8. OFFER DUE DATE/ LOCAL TIME		
9. ISSUED BY U.S. DEPARTMENT OF HOMELAND SECURITY TRANSPORTATION SECURITY ADMINISTRATION 701 SOUTH 12 TH STREET (WEST TOWER) ARLINGTON, VA 22202 POC: GEORGE W. CARLETON PHONE: (571) 227-3733 EMAIL: GEORGE.CARLETON@DHS.GOV			10. THIS ACQUISITION IS <input type="checkbox"/> UNRESTRICTED <input type="checkbox"/> SET ASIDE: %FOR <input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> SMALL DISADV. BUSINESS <input type="checkbox"/> 8(A) <input type="checkbox"/> Service Disabled Veteran SIC: SIZE STANDARD:		11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input type="checkbox"/> SEE SCHEDULE <input type="checkbox"/> 13a. THIS CONTRACT IS A RATED ORDER UNDER OPAS (15 CFR 700) 13b. RATING 14. METHOD OF SOLICITATION <input checked="" type="checkbox"/> RFO <input type="checkbox"/> IFB <input type="checkbox"/> RFP		12. DISCOUNT Net 30	
15. DELIVER TO SEE PAGE 2			16. ADMINISTERED BY SAME AS BLOCK 9		18. PAYMENT WILL BE MADE BY Transportation Security Administration United States Coast Guard Finance Center TSA Commercial Invoices P.O. Box 4111 Chesapeake, VA 23326-4111			
17a. CONTRACTOR/OFFEROR Grant Thornton, LLP 333 John Carlyle Street, #500 Alexandria, VA 22314-5745 Tel: 703-837-4536 Fax: 703-837-4455 POC: Deirdre Pender			CODE	FACILITY	18a. PAYMENT WILL BE MADE BY Transportation Security Administration United States Coast Guard Finance Center TSA Commercial Invoices P.O. Box 4111 Chesapeake, VA 23326-4111	18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED. <input type="checkbox"/> SEE ADDENDUM		
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. <input type="checkbox"/> SEE ADDENDUM					
19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES			21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT	
See Page 2	See Page 2							
25. ACCOUNTING AND APPROPRIATION DATA 5 AD056000D 2005 HQA010 GE0000 7700 3C00 FIN000 3C13000000000000 2510					26. TOTAL AWARD AMOUNT (For Govt. Use Only) Not-to-Exceed \$563,960.00			
<input type="checkbox"/> 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4, FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED								
<input type="checkbox"/> 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY FULL TEXT FAR 52.212-4 & FAR 52.212-5. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED								
28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN COPIES TO <input type="checkbox"/> 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: REFERENCE _____ OFFER <input type="checkbox"/> 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) Larry Goode, Partner		30c. DATED SIGNED 9/19/05		31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT) GEORGE W. CARLETON CONTRACTING OFFICER		31c. DATE SIGNED 9/20/05		
32a. QUANTITY IN COLUMN 21 HAS BEEN <input type="checkbox"/> RECEIVED <input type="checkbox"/> INSPECTED <input type="checkbox"/> ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS				33. SHIP NUMBER <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL		34. VOUCHER NUMBER		
32b. SIGNATURE OF AUTHORIZED GOVT. REPRESENTATIVE				35. AMOUNT VERIFIED CORRECT FOR		37. CHECK NUMBER		
32c. DATE				36. PAYMENT <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL		37. CHECK NUMBER		
41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT				38. S/R ACCOUNT NUMBER		39. S/R VOUCHER NUMBER		
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER				40. PAID BY		42a. RECEIVED BY (Print)		
41c. DATE				42b. RECEIVED AT (Location)		42c. DATE REC'D (YYMMDD)		
				42d. TOTAL CONTAINERS				

This is a Fixed-Price Level of Effort type Delivery Order for Financial Management Control Support Services under the Contractors GSA Schedule. The Contractor shall provide the necessary support personnel, management, and supervision to perform the applicable work requirements in accordance with the attachment A Statement of Work that provides a description of the services to be provided hereunder.

Period of Performance: The Period of Performance for this Delivery Order is for one Base Year and one (1) one-year option as follows:

Basic Period	October 1, 2005 to September 30, 2006
Option Year I	October 1, 2006 to September 30, 2007

The Contractor shall perform the work under this Delivery Order during the base year, period of performance, and during the option period (if and when the option year is exercised by the Government). The Government reserves the right to exercise the option year upon providing thirty days written notice to Contractor in accordance with the clause 3.2.4-35 Option to Extend the Term of the Contract (February 2003) incorporated herein in full text.

Hard Copy of Deliverables shall be submitted to:

Transportation Security Administration
Office of Financial Management,
Attention: David Lanagan
701 South 12th Street
Arlington, VA. 22202
Tel: 571-227-3091

Contract Ceiling/Funding:

The total contract ceiling for the Base Period of Performance and all Options shall not exceed **\$1,250,000.00**. The contract funded amount is the cumulative value of the funding levels authorized through individual Delivery Order modifications issued hereunder. Unless otherwise provided herein, the price of the supplies/services include all applicable Federal, State, and Local taxes, customs duties, import fees of any kind, and shipping/delivery charges. This contract award is for the Base Year effort only. This contract does not authorize delivery or performance of any supplies or services nor the incurrence of any costs above the funded amount currently set at **\$563,960.00**. Delivery or performance and allocation of funding shall be made only as authorized by fully executed modifications to provide additional funding. Performance above the funded amount will be at the contractor's risk.

B Table**Base Period: October 1, 2005 to September 30, 2006**

CLIN	Description	Unit Price	Hours	Total
0001	Partner	\$		
0002	Director (Senior Manager)	\$		
0003	Project Manager (Manager)	\$		
0004	Management Advisor (Manager)	\$		
0005	Senior Accountants (Senior Consultants)	\$		
			Subtotal Labor	\$543,960.00
0006	Travel		Not-to-Exceed	\$ 20,000.00
			Total Not-to-Exceed	\$563,960.00

b4

Option I: October 1, 2006 to September 30, 2007

CLIN	Description	Unit Price	Hours	Total
1001	Partner	\$		
1002	Director (Senior Manager)	\$		
1003	Project Manager (Manager)	\$		
1004	Management Advisor (Manager)	\$		
1005	Senior Accountants (Senior Consultants)	\$		
			Subtotal Labor	\$565,718.40
1006	Travel		Not-to-Exceed	\$ TBD
			Total Not-to-Exceed	\$581,297.60

b4

Terms and Conditions: The terms and conditions of the GSA Schedule shall govern except the disputes, protest, protest after award, and nondisclosure agreement requirements. The following TSA clauses, attached hereto in full text, shall govern on any disputes, and protests. All Contractor personnel working in support of this effort are required to submit a completed Non-disclosure Agreement found at Attachment B, prior to commencement of work. The solicitation, amendments and clarifications are incorporated herein by reference as applicable.

- **TSAAMS 3.9.1-1 Contract Disputes** (February 2003),
- **TSAAMS 3.9.1_3 Protest** (February 2003)
- **TSAAMS 3.9.1-2 Protest After Award** (February 2003)
- **Observance of Legal Holidays and Administrative Leave**

Submittal of a quotation constitutes concurrence to abide by the referenced clauses for the resolution of any disputes.

In addition, contractor must comply with the requirements of clauses:

- **TSAAMS 3.3.1-25 Mandatory Information for Electronic Funds Transfer (EFT) Payment - Central Contractor Registration (CCR)** (February 2003)
- **TSAAMS 3.14.6 Pre-Employment Security Screening of Contractor Employees** (July 2004)
- **TSAAMS 3.2.4-35 Option to Extend the Term of the Contract** (February 2003)

TSAAMS 3.9.1-1 Contract Disputes (February 2003) All contract disputes arising under or related to this contract shall be resolved through the Transportation Security Administration (TSA) dispute resolution system at the FAA Office of Dispute Resolution for Acquisition (ODRA) and shall be governed by the procedures set forth in 14 C.F.R. Parts 14 and 17, which are hereby incorporated by reference. Judicial review, where available, will be in accordance with 49 U.S.C. 46110 and shall apply only to final agency decisions. A contractor may seek review of a final TSA decision only after its administrative remedies have been exhausted.

(b) The filing of a contract dispute with the ODRA may be accomplished by mail, overnight delivery, hand delivery, or by facsimile. A contract dispute is considered filed on the date it is received by the ODRA.

(c) Contract disputes are to be in writing and shall contain:

- (1) The contractor's name, address, telephone and fax numbers and the name, address, telephone and fax numbers of the contractor's legal representative(s) (if any) for the contract dispute;
- (2) The contract number and the name of the Contracting Officer;
- (3) A detailed chronological statement of the facts and of the legal grounds for the contractor's positions regarding each element or count of the contract dispute (i.e., broken down by individual claim item), citing to relevant contract provisions and documents and attaching copies of those provisions and documents;

- (4) All information establishing that the contract dispute was timely filed;
- (5) A request for a specific remedy, and if a monetary remedy is requested, a sum certain must be specified and pertinent cost information and documentation (e.g., invoices and cancelled checks) attached, broken down by individual claim item and summarized; and
- (6) The signature of a duly authorized representative of the initiating party.

(d) Contract disputes shall be filed at the following address:

Office of Dispute Resolution, AGC-70
Federal Aviation Administration
800 Independence Avenue S.W. Room 323
Washington, DC 20591
Telephone: (202) 267-3290, Facsimile: (202) 267-3720

(2) other address as specified in 14 CFR Part 17.

(e) A contract dispute against the TSA shall be filed with the ODRA within two (2) years of the accrual of the contract claim involved. A contract dispute by the TSA against a contractor (excluding contract disputes alleging warranty issues, fraud or latent defects) likewise shall be filed within two (2) years after the accrual of the contract claim. If an underlying contract entered into prior to the effective date of this part provides for time limitations for filing of contract disputes with the ODRA which differ from the aforesaid two (2) year period, the limitation periods in the contract shall control over the limitation period of this section. In no event will either party be permitted to file with the ODRA a contract dispute seeking an equitable adjustment or other damages after the contractor has accepted final contract payment, with the exception of TSA claims related to warranty issues, gross mistakes amounting to fraud or latent defects. TSA claims against the contractor based on warranty issues must be filed within the time specified under applicable contract warranty provisions. Any TSA claims against the contractor based on gross mistakes amounting to fraud or latent defects shall be filed with the ODRA within two (2) years of the date on which the TSA knew or should have known of the presence of the fraud or latent defect.

(f) A party shall serve a copy of the contract dispute upon the other party, by means reasonably calculated to be received on the same day as the filing is to be received by the ODRA.

(g) After filing the contract dispute, the contractor should seek informal resolution with the Contracting Officer.

(h) The TSA requires continued performance with respect to contract disputes arising under this contract, in accordance with the provisions of the contract, pending a final TSA decision.

(i) The TSA will pay interest on the amount found due and unpaid from (1) the date the Contracting Officer receives the contract dispute, or (2) the date payment otherwise would be

due, if that date is later, until the date of payment. Simple interest on contract disputes shall be paid at the rate fixed by the Secretary of the Treasury that is applicable on the date the Contracting Officer receives the contract dispute and then at the rate applicable for each 6-month period as fixed by the Treasury Secretary until payment is made.

(j) Additional information and guidance about the ODRA dispute resolution process for contract disputes can be found on the ODRA Website at <http://www.faa.gov>.

TSAAMS 3.9.1_3 Protest (February 2003)

AS A CONDITION OF SUBMITTING AN OFFER OR RESPONSE TO THIS RFI/RFP (OR OTHER SOLICITATION, IF APPROPRIATE), THE OFFEROR OR POTENTIAL OFFEROR AGREES TO BE BOUND BY THE FOLLOWING PROVISIONS RELATING TO PROTESTS:

(a) Protests concerning Transportation Security Administration's (TSA) Request For Information/Request For Proposals (RFI/RFPs) or awards of contracts shall be resolved through the dispute resolution system at the FAA Office of Dispute Resolution for Acquisition (ODRA), and shall be governed by the procedures set forth in 14 C.F.R. Parts 14 and 17, which are hereby incorporated by reference. Judicial review, where available, will be in accordance with 49 U.S.C. 46110 and shall apply only to final agency decisions. A protestor may seek review of a final TSA decision only after its administrative remedies have been exhausted.

(b) Offerors initially should attempt to resolve any issues concerning potential protests with the Contracting Officer. The Contracting Officer should make reasonable efforts to answer questions promptly and completely, and, where possible, to resolve concerns or controversies. The protest time limitations, however, will not be extended by attempts to resolve a potential protest with the Contracting Officer.

(c) The filing of a protest with the ODRA may be accomplished by mail, overnight delivery, hand delivery, or by facsimile. A protest is considered filed on the date it is received by the ODRA.

(d) Only an interested party may file a protest. An interested party is one whose direct economic interest has been or would be affected by the award or failure to award a TSA contract. Proposed subcontractors are not "interested parties" within this definition.

(e) A written protest must be filed with the ODRA within the times set forth below, or the protest shall be dismissed as untimely:

(1) Protests based upon alleged improprieties in a solicitation or a RFI/RFP that are apparent prior to bid opening or the time set for receipt of initial proposals shall be filed prior to bid opening or the time set for the receipt of initial proposals.

(2) In procurements where proposals are requested, alleged improprieties that do not exist in

the initial solicitation, but which are subsequently incorporated into the solicitation, must be protested not later than the next closing time for receipt of proposals following the incorporation.

(3) For protests other than those related to alleged solicitation improprieties, the protest must be filed on the later of the following two dates:

(i) Not later than seven (7) business days after the date the protester knew or should have known of the grounds for the protest; or

(ii) If the protester has requested a post-award debriefing from the TSA Integrated Business Team, not later than five (5) business days after the date on which the Business Team holds that debriefing.

(f) Protests shall be filed at:

(1) Office of Dispute Resolution, AGC-70
Federal Aviation Administration
800 Independence Avenue S.W. Room 323
Washington, DC 20591
Telephone: (202) 267-3290, Facsimile: (202) 267-3720

(2) other address as specified in 14 CFR Part 17.

(g) At the same time as filing the protest with the ODRA, the protester shall serve a copy of the protest on the Contracting Officer and any other official designated in the RFI/RFP for receipt of protests by means reasonably calculated to be received by the Contracting Officer on the same day as it is to be received by the ODRA. The protest shall include a signed statement from the protester, certifying to the ODRA the manner of service, date, and time when a copy of the protest was served on the Contracting Officer and other designated official(s).

(h) Additional information and guidance about the ODRA dispute resolution process for protests can be found on the ODRA Website at <http://www.faa.gov>.

TSAAMS 3.9.1-2 Protest After Award (February 2003)

(a) Upon receipt of a notice that a protest has been filed with the FAA Office of Dispute Resolution for Acquisition (ODRA), or a determination that a protest is likely, the (Undersecretary or his designee may instruct the Contracting Officer) to direct the Contractor to stop performance of the work called for by this contract. The order to the Contractor shall be in writing, and shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Upon receipt of the final decision or other resolution of the protest, the Contracting Officer shall either--

(1) Cancel the stop-work order; or

(2) For other than cost-reimbursement contracts, terminate the work covered by the order as provided in the "Default" or the "Termination for Convenience of the Government" clause(s) of this contract; or

(3) For cost-reimbursement contracts, terminate the work covered by the order as provided in the "Termination" clause of this contract.

(b) If a stop-work order issued under this clause is canceled either before or after the final resolution of the protest, the Contractor shall resume work. The Contracting Officer shall make for other than cost-reimbursement contracts, an equitable adjustment in the delivery schedule or contract price, or both; and for cost-reimbursement contracts, an equitable adjustment in the delivery schedule, the estimated cost, the fee, or a combination thereof, and in any other terms of the contract that may be affected; and the contract shall be modified, in writing, accordingly, if--

(1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

(2) The Contractor asserts its right to an adjustment within 30 days after the end of the period of work stoppage; provided, that if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon a proposal submitted at any time before final payment under this contract.

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

(d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

(e) The Government's rights to terminate this contract at any time are not affected by action taken under this clause.

Observance of Legal Holidays and Administrative Leave

Government personnel observe the listed days as holidays:

New Year's Day	Martin Luther King, Jr.'s Birthday
President's Day	Memorial Day
Independence Day	Labor Day
Columbus Day	Veteran's Day
Thanksgiving Day	Christmas Day

Any other day designated by Federal Statute, Executive Order or Presidential Proclamation

The contractor shall observe above holidays on the date observed by the Government. It is understood and agreed between the Government and the contractor that observance of such days by Government personnel shall not "on-its-face" be the cause for an additional period of performance, or entitlement of compensation except as set forth within the contract. No form of holiday or other premium compensation will be reimbursed.

Further, when the Government grants administrative leave to its employees, contractor personnel performing duties at a Government site shall also be dismissed. When administrative leave is granted to contractor personnel as a result of inclement weather, potentially hazardous conditions, and other special circumstances, etc., it will be without loss to the contractor. In this instance, the salaries and wages to the contractor for the period of such excused absence shall be reimbursable item of direct cost hereunder for employees whose regular time is normally direct charged, and a reimbursable item of indirect cost for employees whose regular time is normally charged indirect (in accordance with the contractor's accounting policy).

All contractor personnel assigned to this contract shall limit their observation of holidays to those set forth above.

TSAAMS 3.3.1-25 Mandatory Information for Electronic Funds Transfer (EFT) Payment - Central Contractor Registration (CCR) (February 2003)

(a) Method of payment. For any payment to be made after June 1, 2001, the Contractor shall provide EFT information to the CCR database. Payments by the TSA under this contract, including invoice and contract financing payments, will be made by EFT, except as provided in paragraph (a)(1). If payment is made by EFT, the TSA may, at its option, also forward the associated payment information by electronic transfer. As used in this clause, the term "EFT" refers to the funds transfer and may also include the information transfer.

(1) In the event the TSA is unable to release one or more payments by EFT, the Contractor agrees to either:

(i) Accept payment by check or some other mutually agreeable method of payment; or

(ii) Request the TSA to extend the payment due date until such time as the TSA can make payment by EFT (but see paragraph (d) of this clause).

(b) Mandatory submission of Contractor's EFT information.

(1) The Contractor is required, as a condition to any payment under this contract, to provide the Central Contractor Registration (CCR) database with the information required in the CCR to make payment by EFT. The Contractor may register to the CCR online at www.ccr2000.com, or call the CCR Assistance Center toll free at (888)-227-2423 and request the necessary registration forms.

The Contractor must have a DUNS number to begin registration. To obtain a DUNS number, call Dun & Bradstreet, Inc. at (800) 234-3867. In the event that the EFT information changes, the Contractor shall be responsible for providing the updated information to the CCR database.

(2) If the Contractor has identified multiple payment receiving points (i.e., more than one remittance address and/or EFT information set) in the CCR database, and the Contractor has not notified the TSA of the payment receiving point applicable to this contract, the TSA shall make payment to the first payment receiving point (EFT information set or remittance address as applicable) listed in the CCR database.

(c) Mechanisms for EFT payment. The TSA may make payment by EFT through either an Automated Clearing House (ACH) subject to the banking laws of the United States or the Federal Reserve Wire Transfer System at the TSA's option. The rules governing Federal payments through the ACH are contained in 31 CFR part 210.

(d) Suspension of payment.

(1) Notwithstanding the provisions of any other clause of this contract, the TSA is not required to make any payment under this contract until after the correct EFT payment information from the Contractor has been provided to the CCR database. No invoice or contract financing request shall be deemed to be valid, as defined by the Prompt Payment Act, until correct EFT information is received into the CCR database.

(2) Changes made to an existing record in the CCR database will become effective not later than the 30th day after receipt in the CCR database. However, the Contractor may request that no further payments be made until the changed EFT information is implemented into the CCR database. If such suspension would result in a late payment under the Prompt Payment clause of this contract, the Contractor's request for suspension shall extend the due date for payment by the number of days of the suspension.

(e) Contractor EFT arrangements. The Contractor shall designate a single financial agent capable of receiving and processing the electronic funds transfer using the EFT methods described in paragraph (c) of this clause. The Contractor shall pay all fees and charges for receipt and processing of transfers.

(f) Liability for uncompleted or erroneous transfers.

(1) If an uncompleted or erroneous transfer occurs because the TSA failed to use the Contractor-provided EFT information in the CCR database in the correct manner, the TSA remains responsible for

(i) making a correct payment,

(ii) paying any prompt payment penalty due, and

(iii) recovering any erroneously directed funds.

(2) If an uncompleted or erroneous transfer occurs because Contractor-provided EFT information in the CCR database was incorrect, or was revised within 30 days at the time of TSA release of the EFT payment transaction instruction to the Federal Reserve System, and:

(i) If the funds are no longer under the control of the payment office, the TSA is deemed to have made payment and the Contractor is responsible for recovery of any erroneously directed funds; or

(ii) If the funds remain under the control of the payment office, the TSA retains the right to either make payment by mail or suspend the payment in accordance with paragraph (d) of this clause.

(g) EFT and prompt payment.

(1) A payment shall be deemed to have been made in a timely manner in accordance with the Prompt Payment clause of this contract if, in the EFT payment transaction instruction given to the Federal Reserve System, the date specified for settlement of the payment is on or before the prompt payment due date, provided the specified payment date is a valid date under the rules of the Federal Reserve System.

(2) When payment cannot be made by EFT because of incorrect EFT information provided by the Contractor to the CCR database, no interest penalty is due after the date of the uncompleted or erroneous payment transaction, provided that notice of the defective EFT information is issued to the Contractor within 7 days after the TSA is notified of the defective EFT information.

(h) EFT and assignment of claims. If the Contractor assigns the proceeds of this contract as provided for in the Assignment of Claims clause of this contract, the Contractor shall require as a condition of any such assignment, that the assignee shall register in the CCR database and shall be paid by EFT in accordance with the terms of this clause. In all respects, the requirements of this clause shall apply to the assignee as if it were the Contractor. EFT information, which shows the ultimate recipient of the transfer to be other than the Contractor, in the absence of a proper assignment of claims acceptable to the TSA, is incorrect EFT information within the meaning of paragraph (d) of this clause.

(i) Liability for change of EFT information by financial agent. The Contractor agrees that the Contractor's financial agent may notify the TSA of a change to the routing transit number, Contractor account number, or account type. The TSA shall use the changed data in accordance with paragraph (d)(2) of this clause. The Contractor agrees that the information provided by the

agent is deemed to be correct information as if it were provided by the Contractor. The Contractor agrees that the agent's notice of changed EFT data is deemed to be a request by the Contractor in accordance with paragraph (d)(2) that no further payments be made until the changed EFT information is implemented by the payment office. The TSA is not liable for errors resulting from changes to EFT information made by the Contractor's financial agent.

TSAAMS 3.14.6 PRE-EMPLOYMENT SECURITY SCREENING OF CONTRACTOR EMPLOYEES (July 2004)

A. All employees assigned to work in a Transportation Security Administration (TSA) facility, inclusive of all airports nationwide, under this contract will be required to undergo a pre-employment security screening investigation prior to being permitted to report to work. The Contractor shall ensure that each employee meets the following criteria:

- 1) Contractor employees must be US Citizens or Legal Permanent Residents. Only US Citizens can access TSA's Information Technology (IT) Systems.
- 2) Contractor employees must undergo a favorable Background Investigation.
 - a) The following Background Investigation Security Paperwork must be completed by the contractor employee and given to the Contracting Officer's Technical Representative (COTR) at least thirty-five (35) days prior to the employment start date:
 - 1) Standard Form (SF) 86, Questionnaire for National Security. (The SF 86 is available at www.opm.gov under standard forms.)
 - 2) Form FD 258, Fingerprint Cards. (Two (2) original Fingerprint Cards are required to be completed and signed by the person taking the fingerprints. Fingerprints can be taken by local law enforcement agencies.)
 - 3) TSA Form 2201, Fair Credit Reporting Act Form.
 - b) The COTR will submit the Background Investigation Security Paperwork to the TSA Credentialing Program Office (CPO). This submission must take place at least thirty (30) days prior to the employment start date.
 - c) When a contractor employee voluntarily or involuntarily leaves his/her employment under a contract with TSA, the contractor must obtain and return the contractor employee's badge to the COTR on the contractor employee's last day of work at a TSA facility, inclusive of all airports nationwide. The COTR will return the contractor employee's badge to the Office of Security, Physical Security Division.

B. As stated above, contractor employees requiring staff-like access to TSA facilities on a recurring basis (more than 14 days per year) must have a favorably adjudicated fingerprint based criminal history record check, credit check and search of the Office of Personnel Management,

Security/Suitability Investigations Index, prior to being issued a permanent TSA Headquarters photo access pass. COTRs should advise the Office of Security, Physical Security Division, if the contract on which the contractor is working will last 90 days or less. Record checks may be conducted prior to or concurrently with a National Agency Check and Inquiries and Credit (NACIC) investigation. The NACIC is the minimum investigative standard for TSA contractor employees.

C. Contractor employees requiring temporary facility access for one to fourteen days or facility maintenance, routine delivery, etc., require only a fingerprint check and/or National Crime Information Center (NCIC) records check.

D. A contractor that participates in the National Industrial Security Program (NISP) may, through their COTR certify, in writing, that their employees have met the standard defined in Paragraph B. above.

3.3.1-17 Prompt Payment (February 2003)

Notwithstanding any other payment clause in this contract, the Government will make invoice payments and contract financing payments under the terms and conditions specified in this clause. Payment shall be considered as being made on the day a check is dated or an electronic funds transfer is made. All days referred to in this clause are calendar days, unless otherwise specified.

(a) Invoice Payments.

(1) For purposes of this clause, invoice payment means a Government disbursement of monies to a Contractor under a contract or other authorization for supplies or services accepted by the Government. This includes payments for partial deliveries that have been accepted by the Government, final payments under T&M and labor-hour contracts, and final cost or fee payments where amounts owed have been settled between the Government and the Contractor.

(2) Except as indicated in subparagraph (a)(3) and paragraph (c) of this clause, the due date for making invoice payments by the designated payment office shall be the later of the following two events:

(i) The 30th day after the designated billing office has received a proper invoice from the Contractor.

(ii) The 30th day after Government acceptance of supplies delivered or services performed by the Contractor. On a final invoice where the payment amount is subject to contract settlement actions, acceptance shall be deemed to have occurred on the effective date of the contract settlement. However, if the designated billing office fails to annotate the invoice with the actual date of receipt, the invoice payment due date shall be deemed to be the 30th day after the date the Contractor's invoice is dated, provided a proper invoice is received and there is no disagreement over quantity, quality, or Contractor compliance with contract requirements.

(3) An invoice is the Contractor's bill or written request for payment under the contract for supplies delivered or services performed. An invoice shall be prepared and submitted to the designated billing officer specified in the contract. A proper invoice must include the items listed in subdivisions (a)(3)(i) through (a)(3)(viii) of this clause. If the invoice does not comply with

these requirements, then the Contractor will be notified of the defect within 7 days after receipt of the invoice at the designated billing office. Untimely notification will be taken into account in the computation of any interest penalty owed the Contractor in the manner described in subparagraph (a)(6) of this clause.

(i) Name and address of the Contractor.

(ii) Invoice date.

(iii) Contract number or other authorization for supplies delivered or services performed (including order number and contract line item number).

(iv) Description, quantity, unit of measure, unit price, and extended price of supplies delivered or services performed.

(v) Shipping and payment terms (e.g., shipment number and date of shipment, prompt payment discount terms). Bill of lading number and weight of shipment will be shown for shipments on Government bills of lading.

(vi) Name and address of Contractor official to whom payment is to be sent (must be the same as that in the contract or in a proper notice of assignment).

(vii) Name (where practicable), title, phone number and mailing address of person to be notified in event of a defective invoice.

(viii) Any other information or documentation required by other requirements of the contract (such as evidence of shipment).

(4) An interest penalty shall be paid automatically by the Government, without request from the contractor, if payment is not made by the due date and the conditions listed in subdivisions (a)(4)(i) through (a)(4)(iii) of this clause are met, if applicable.

(i) A proper invoice was received by the designated billing office.

(ii) A receiving report or other Government documentation authorizing payment was processed and there was no disagreement over quantity, quality, or contractor compliance with any contract term or condition.

(iii) In the case of a final invoice for any balance of funds due the Contractor for supplies delivered or services performed, the amount was not subject to further contract settlement actions between the Government and the Contractor.

(5) The interest penalty shall be as specified in the "Interest" clause. The interest penalty amount, interest rate and the period for which the interest penalty was computed, will be separately stated by the designated payment office on the check, in accompanying remittance advice, or, in the case of wire transfers, by an appropriate electronic data message accompanying the wire transfer. If the designated billing office failed to notify the Contractor of a defective invoice within the periods prescribed in subparagraph (a)(3) of this clause, then the due date on the corrected invoice will be adjusted by subtracting the number of days taken beyond the prescribed notification of defects period. Any interest penalty owed the Contractor will be based on this adjusted due date. Adjustments will be made by the designated payment office for errors in calculating interest penalties, if requested by the Contractor.

(i) For the sole purpose of computing an interest penalty that might be due the contractor, Government acceptance shall be deemed to have occurred constructively on the 7th day (unless otherwise specified in this contract) after the contractor delivered the supplies or performed the services in accordance with the terms and conditions of the contract, unless there is a disagreement over quantity, quality, or contractor compliance with a contract provision. In the event that actual acceptance occurs within the

constructive acceptance period, the determination of an interest penalty shall be based on the actual date of acceptance. The constructive acceptance requirement does not, however, compel Government officials to accept supplies or services, perform contract administration functions, or make payment prior to fulfilling their responsibilities.

(ii) The following periods of time will not be included in the determination of an interest penalty:

(A) The period taken to notify the Contractor of defects in invoices submitted to the Government, but this may not exceed 7 days.

(B) The period between the defects notice and resubmission of the corrected invoice by the Contractor.

(C) Any period of delay caused by incorrect electronic funds transfer (EFT) information, in accordance with the EFT clause of this contract.

(iii) Interest penalties will not continue to accrue after the filing of a claim for such penalties under Federal Aviation Administration (TSA) contract disputes resolution procedures. Interest penalties of less than \$1.00 need not be paid.

(iv) Interest penalties are not required on payment delays due to disagreement between the Government and Contractor over the payment amount or other issues involving contract compliance or on amounts temporarily withheld or retained in accordance with the terms of the contract. Contract disputes, and any interest that may be payable, will be resolved in accordance with TSA contract disputes resolution procedures.

(6) An interest penalty shall also be paid automatically by the designated payment office, without request from the contractor, if a discount for prompt payment is taken improperly. The interest penalty will be calculated as described in subparagraph (a)(5) of this clause on the amount of discount taken for the period beginning with the first day after the end of the discount period through the date when the contractor is paid.

(b) Contract Financing Payments.

(1) For purposes of this clause, contract financing payments mean Government disbursements of monies to a Contractor under a contract clause or other authorization without regard to acceptance of supplies or services by the Government. Contract financing payments include but are not limited to payments made according to commercial terms and installment payments. They also include interim vouchers under T&M, labor-hour, and cost reimbursement contracts (regardless of whether goods or services were delivered and received by the Government).

(2) For contracts that provide for contract financing payments, requests for payment shall be submitted to the designated billing office as specified in this contract or as directed by the Contracting Officer. Payments shall be made on the 30th day after receipt of a proper payment request by the designated billing office. In the event that an audit or other review of a specific payment request is required to ensure compliance with the terms and conditions of the contract, the designated payment office is not compelled to make payment by the due date specified.

(3) Contract financing payments shall not be assessed an interest penalty for payment delays.

(c) If this contract contains the Fast Payment Procedures, payments will be made within 15 days after the date of receipt of the invoice.

TSAAMS 3.2.4-35 Option to Extend the Term of the Contract (February 2003)

(a) The Government may extend the term of this contract by written notice to the Contractor within 15 days; provided that the Government shall give 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 provision.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed one (5) year.

TSAAMS 3.1.7-2 Organizational Conflicts of Interest (February 2003)

(a) By submitting and offer or proposal the offeror or Contractor warrants that, to the best of the Contractor's knowledge and belief, there are no relevant facts or circumstances which could give rise to an organizational conflict of interest (OCI), as defined in the TSA Acquisition Management System, "Organizational Conflicts of Interest", or that the Contractor has disclosed all such relevant information.

(b) The offeror or Contractor agrees that if an actual or potential OCI is discovered after award, the Contractor shall make a full disclosure in writing to the Contracting Officer. The disclosure shall include a mitigation plan describing actions the Contractor has taken or proposes to take, to avoid, mitigate, or neutralize the actual or potential conflict. Changes in the Contractor's relationships due to mergers, consolidations or any unanticipated circumstances may create an unacceptable organizational conflict of interest might necessitate such disclosure.

(c) The TSA reserves the right to review and audit OCI mitigation plans as needed after award, and to reject mitigation plans if the OCI, in the judgment of the Contracting Officer cannot be avoided, or mitigated.

(d) The Contracting Officer may terminate this contract for convenience in whole or in part, if it deems such termination necessary to avoid an OCI. If the Contractor was aware of a potential OCI prior to award or discovered an actual or potential conflict after award and did not disclose or misrepresented relevant information to the Contracting Officer, the Government may terminate this contract for default, debar the Contractor from government contracting, or pursue such other remedies as may be permitted by law or this contract.

(e) The Contractor further agrees to insert provisions which shall conform substantial to the language of this clause including this paragraph (d) in any subcontract or consultant agreement hereunder.

TSAAMS 3.10.1-22 Contracting Officer's Technical Representative

(a) The Contracting Officer may designate other Government personnel (known as the Contracting Officer's Technical Representative) to act as his or her authorized representative for contract administration functions which do not involve changes to the scope, price, schedule, or terms and conditions of the contract. The designation will be in writing, signed by the Contracting Officer, and will set forth the authorities and limitations of the representative(s) under the contract. Such designation will not contain authority to sign contractual documents, order contract changes, modify contract terms, or create any commitment or liability on the part of the Government different from that set forth in the contract.

(b) The Contractor shall immediately contact the Contracting Officer if there is any question regarding the authority of an individual to act on behalf of the Contracting Officer under this contract.

STATEMENT OF WORK

- 1.0 Title of Requirement
- 2.0 Requiring Office/Organization
- 3.0 Background
- 4.0 Scope
- 5.0 Applicable Documents
- 6.0 Deliverables
- 7.0 Performance/Delivery Period
- 8.0 Place of Performance
- 9.0 Government Furnished Resources and Information
- 10.0 Requirements for Handling Sensitive and/or Proprietary Information
- 11.0 Travel
- 12.0 Administrative Information

1.0 TITLE OF REQUIREMENT

Management Control Support Services

2.0 REQUIRING ORGANIZATION

The Transportation Security Administration (TSA), Finance & Administration, Office of Financial Management, Management Control Section.

3.0 BACKGROUND

The Transportation Security Administration (TSA) was established on November 19, 2001 in response to the events of September 11, 2001. It has a workforce of approximately 52,000 employees located at over 400 airports and field locations throughout the United States and the world. TSA headquarters is located in Arlington, Virginia.

Public Laws require that Federal agencies establish, monitor, and report on internal controls associated with their daily operations. Specific requirements include establishing internal controls to reasonably assure that; obligations and costs comply with public law; personnel safeguard assets against waste, fraud, loss, unauthorized use, and misappropriation; proper accountability for government resources used to operate the agency; and that program and administrative functions follow applicable laws and administrative policy.

TSA's mission is to protect the Nation's transportation systems to ensure freedom of movement for people and commerce. TSA has implemented policies and procedures designed to fulfill that mission. At this time, the TSA program for internal/management control requires assistance to ensure compliance with the Federal Managers Financial Integrity Act (FMFIA) and the recently enacted Department of Homeland Security Financial Accountability Act, which requires an audit opinion on internal control over financial reporting beginning in FY 2006.

4.0 SCOPE

This procurement requests professional support services required to implement OMB Circular A-123 and DHS Financial Accountability Act Implementation guidance with a goal of obtaining an “unqualified” audit opinion on TSA’s internal controls over financial reporting. Additionally, the procurement will assist the TSA in implementing and maintaining a Management Control program that will meet current and future Federal requirements and standards. In reviewing this document the terms “Internal Control” and “Management Control” are synonymous. Specific support services to be provided by the contractor are as follows:

4.1 CONTROL ASSESSMENT AND IMPROVEMENT PLAN.

Assess TSA’s current Management Control environment and prepare a plan identifying control improvements and a process for the TSA to follow in complying with OMB and DHS guidance. Specific tasks include, but are not limited to the following:

4.1.1 Control Assessment

- a) Meet with management to gain understanding of TSA mission and overall objectives of the assessment.
- b) Review existing policies, procedures, organizational structure, and process flows to determine the level of effort needed to receive a “clean” opinion on an internal control audit.
- c) Identification of:
 - a. significant accounts, disclosure and business processes/sub processes/cycles and map to accounts and disclosures.
 - b. relevant financial statement assertions for each significant account and disclosure
- d) Conduct risk assessments of the business process and sub-processes.
- e) Assess, test, and classify existing TSA controls according to the effectiveness of each. Classifications should range from unreliable to optimal and include an identification of weaknesses in internal controls and related documentation, which, if not corrected, would likely cause TSA to fail an internal control audit.

4.1.2 Control Improvement Plan

- a) Document existing TSA controls and categorize according to the five Government Accountability Office Standards for Internal Control in the Federal Government as follows:
 1. Control Environment
 2. Risk Assessment
 3. Control Activity
 4. Communication
 5. Monitoring
- b) Prepare remediation plan that details control improvements and steps TSA must take to comply with OMB and DHS guidance. The plan must include controls to ensure that TSA is able to provide assurance

that its system of internal controls over financial reporting complies with Appendix A, OMB A-123 and with the audit opinion requirements associated with the DHS Financial Accountability Act.

4.2 TSA MANAGEMENT CONTROL PROGRAM

Provide all professional support to conduct management control meetings at TSA headquarters; provide professional assistance to TSA Management Control Managers at headquarters; develop management control checklists for field offices, airports, and headquarters operations designated high risk in accordance with Contracting Officer Representative (COR) direction; prepare, disseminate, and analyze management control data calls associated with normal management of an agency Management Control Program. Specific tasks include, but are not limited to the following:

4.2.1 Management Control Checklists.

Develop, maintain, coordinate, and disseminate management control checklists and other management control tools to TSA headquarters and field offices.

4.2.2 Management Control Data Calls.

Prepare, disseminate, and analyze management control data calls to TSA organizations in order to meet Departmental or other suspense.

4.2.3 Statements of Assurance.

Analyze the Federal Managers Financial Integrity Act Annual Statements of Assurance submitted by all TSA mission area managers to include the following:

- a) Provide support to obtain information and support the TSA Annual Statement of Assurance submission for the Administrators signature.
- b) Provide recommendation for COTR review and Management Control Council approval on whether internal controls issues reported in Assurance Statements warrant reporting as a material weakness.
- c) Maintain documentation to support the Statement of Assurance in accordance with TSA Documentation guidelines

4.2.4 Management Control Training.

Review existing TSA Management Control Training Program and propose updates to include requirements associated with Appendix A of OMB A-123 and the DHS Financial Accountability Act.

4.2.5 Management Control Council Meetings.

Provide all professional and administrative support to conduct quarterly Management Control Council Meetings at TSA headquarters involving TSA senior managers across the agency to include the following:

- a) Develop quarterly Management Control Council meeting agenda for COTR approval in accordance with TSA program manager guidance.

- b) Provide presentation support to the Management Control Council Committee Chairperson as required in accordance with COTR guidance.
- c) Provide recorder for Management Control Council Committee meetings each quarter.
- d) Prepare minutes of Management Control Council for Committee Chairpersons approval in accordance with COTR guidance.
- e) Disseminate Management Control Council meeting minutes to committee members.
- f) Maintain files on all Management Control Council business in accordance with TSA documentation guidelines. All files will be provided to TSA upon completion of the contract.
- g) Monitor tasks assigned for Management Control Council Committee business and brief status of assigned tasks at the next meeting held at headquarters in accordance with COTR guidance.
- h) Perform other duties associated with conducting regular Management Control Council meetings for the TSA in accordance COTR guidance.

4.2.6 Management Control Issue Summaries

Review and analyze federal government management/internal control reports for impact on TSA operations. The review will include the following:

- a) Department of Homeland Security (DHS) Inspector General (IG) reports,
- b) Government Accountability Office (GAO) audit reports and other management/internal control reviews.
- c) Management/Internal Control Specific Audit Reports from other federal government agencies.
- d) Other information pertinent to the TSA Management Control Program as requested by the COTR.

5.0 APPLICABLE DOCUMENTS

- Federal Managers Financial Integrity Act (FMFIA) of 1982
- Office of Management and Budget Circular A-123, Management's Responsibility for Internal Control, December 2004.
- Government Accountability Office (GAO) GAO/AIMD-00-21.3.1, Standards for Internal Control in the Federal Government, November 1999.
- Department of Homeland Security (DHS) Financial Accountability Act, October 2004.
- Transportation Security Administration (TSA) Management Directive 3100.3, Management Control Program, February 2005.
- TSA Program Managers Training Book, December 2004
- DHS Financial Accountability Act Implementation Guidance, April 2005.

6.0 DELIVERABLES

Unless otherwise specified, the TSA requires delivery of one (1) electronic copy and one (1) hard copy of each deliverable. Support designated "As required" will be documented in the monthly status reports. Electronic copies shall be delivered via email attachment or other media by mutual agreement of the parties to David.Lanagan@dhs.gov or to TSA Office of Financial Management, Management Control Section, TSA Headquarters, West Tower, 12th Floor, Room 126S, TSA-14, 601 South 12th Street, Arlington, VA. 22203-4204. The electronic copy shall be in the appropriate MS Office 2000 application or later version as mutually agreed to by the parties. The contractor shall deliver products in accordance with the requirements of this SOW as detailed below and indicated in the Delivery Schedule Table.

6.1 CONTROL ASSESSMENT AND IMPROVEMENT PLAN

6.1.1 TSA Control Assessment Report. Final assessment report which summarizes major control deficiencies in such a way that patterns of deficiencies and systemic problems are identified. The report must make a recommendation for prioritization of corrective actions, based on complexity and level of resources required to implement.

6.1.2 TSA Control Improvement Plan. A plan which documents and recommends a process that TSA take in order to comply with the DHS Financial Accountability Act and any implementing guidance issued by DHS. The plan will provide remedy to internal control audit issues identified in the Assessment Report provided in 6.1.1. The plan will include recommendations on procedural changes, personnel requirements, and a timeline by which corrections to ensure compliance may reasonably be expected to be completed.

6.2 TSA MANAGEMENT CONTROL PROGRAM

6.2.1 Management control checklists and tools. Management control checklists and other tools will be developed and disseminated to TSA activities at Headquarters and Airport locations as required. Performance will be documented in monthly status reports.

6.2.2 Management control data calls. Management control data calls will be analyzed, prepared, and disseminated to TSA Senior Managers to meet Departmental and other requirements. Performance will be documented in monthly status reports.

6.2.3 TSA Annual Statement of Assurance. Support will be provided to disseminate data calls and analyze data submitted by TSA managers to support the Annual Statement of Assurance. Performance will be documented in monthly status reports.

6.2.4 TSA Management Control Training Updates. Management Control Training recommendations required to ensure compliance with Appendix A of OMB A-123 and the DHS Financial Accountability Act.

6.2.5 Management Control Council Meetings. Professional and administrative support in conducting quarterly TSA Management Control Council meetings at TSA headquarters. Performance will be documented in monthly status reports.

6.3 STATUS AND RECURRING REPORTS

6.3.1 Monthly Project Status Reports. The contractor will designate a staff member (Program Manager) as a single point of contact for administration of this contractual action. Monthly status reports are considered project deliverables and the contractor will submit these reports to the TSA Program manager. Reports are due on the tenth workday following the end of the month and will be delivered via email to the COTR. The monthly status report will include:

- a) A synopsis of task activities completed and or worked on during the past month.
- b) Planned task activities scheduled for the following month.
- c) An identification of all issues/problems and recommended solutions.

6.3.2 Management Control Summary Reports.

Provide professional review and analysis of management control reports for impact on TSA operations. The review will include Department of Homeland Security (DHS) Inspector General (IG) reports, Government Accountability Office (GAO) audits and other reviews, Management Control Specific Audit Reports, and any other information pertinent to the TSA Management Control Program.

DELIVERY SCHEDULE TABLE

Deliverable Title	SOW Reference	Due Date
TSA Control Assessment Report	6.1.1	NLT 120 days following task award.
Control Improvement Plan	6.1.2	NLT 60 days following completion of task 4.1.1.
Management control checklist and other tool development and dissemination.	6.2.1	As Required following task award.
Management control data call preparation and dissemination.	6.2.2	As Required following task award.
Annual Statements of Assurance analysis support.	6.2.3	NLT 31 August, In accordance with DHS suspense.
Management Control Training review and update	6.2.4	NLT 60 days following

Deliverable Title	SOW Reference	Due Date
recommendation.		completion of task 4.1.1.
Management Control Council Meeting facilitation.	6.2.5	Quarterly, as required following task award.
Project Status Reports.	6.3.1	Monthly, NLT 10 work days following the end of the month
Management Control Report summaries.	6.3.2	Monthly, NLT 10 work days following the end of the month.

Note: Each deliverable schedule assumes 5 Business days for Government review and comment. The contractor shall deliver the final version of the deliverable 5 days after receipt of Government comments. *These timeframes shall apply unless otherwise specified on the task orders issued by the TSA.*

7.0 PERFORMANCE/DELIVERY PERIOD

Services will be provided upon contract award for a base year and one option year.

8.0 PLACE/LOCATION OF PERFORMANCE/DELIVERY

Performance will take place at TSA and contractor's facilities. All Management Control Council meetings and support required to comply with provisions of the DHS Financial Accountability Act Implementation Guide will be performed at TSA Headquarters. Contract performance will be supported and monitored by TSA Headquarters located at the following address:

U.S. Department of Homeland Security
 Transportation Security Administration
 Office of Financial Management, TSA-14
 701 South 12th St., West Tower
 Arlington, VA 22202
 Phone: (571) 227-3091
 Facsimile: (571) 227-2567

9.0 GOVERNMENT FURNISHED RESOURCES AND INFORMATION

TSA will provide current copies or access via the TSA Web site to all documents required to complete tasks associated with this Statement of Work.

10.0 REQUIREMENTS FOR HANDLING SENSITIVE AND/OR PROPRIETARY INFORMATION

Contractor personnel will be required to understand and a nondisclosure agreement form before beginning to work under this contract.

11.0 TRAVEL REQUIREMENTS

Travel may be required to support analysis, assessments, and management control training to fit the needs of TSA as requested. Reimbursement will be based on actual costs incurred in accordance with the Federal Travel Regulations (FTR). All travel must be approved in advance by the Contracting Officer's Technical Representative. No other travel charges will be reimbursed in support of this contract.

12.0 ADMINISTRATIVE INFORMATION

12.1 Government Contacts.

12.1.1 Technical Points of Contact.

Program Manager, Jeffrey Bobich, Office of Financial Management, Deputy Director, Jeffrey.Bobich@dhs.gov, 571-227-2118.

Contracting Officer Technical Representative, David Lanagan, Office of Financial Management, Management Control, David.Lanagan@dhs.gov, 571-227-3091.

12.1.2 **Contracting Officer**, George W. Carleton, Office of Acquisition; George.Carleton@dhs.gov, 571-227-3733.

NON-DISCLOSURE AGREEMENT

I, _____, an individual official, employee, consultant, or subcontractor of or to _____ (the Authorized Entity), intending to be legally bound, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain information, specified below, that is owned by, produced by, or in the possession of the United States Government.

(Signer will acknowledge the category or categories of information that he or she may have access to, and the signer's willingness to comply with the standards for protection by placing his or her initials in front of the applicable category or categories.)

Initials:	Protected Critical Infrastructure Information (PCII)
-----------	---

I attest that I am familiar with, and I will comply with all requirements of the PCII program set out in the Critical Infrastructure Information Act of 2002 (CII Act) (Title II, Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296, 196 Stat. 2135, 6 USC 101 et seq.), as amended, the implementing regulations thereto (6 CFR Part 29), as amended, and the applicable PCII Procedures Manual, as amended, and with any such requirements that may be officially communicated to me by the PCII Program Manager or the PCII Program Manager's designee.

Initials:	Sensitive Security Information (SSI)
-----------	---

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of SSI information as cited in this Agreement and in accordance with 49 CFR Part 1520, "Protection of Sensitive Security Information," "Policies and Procedures for Safeguarding and Control of SSI," as amended, and any supplementary guidance issued by an authorized official of the Department of Homeland Security.

Initials:	Other Sensitive but Unclassified (SBU)
-----------	---

As used in this Agreement, sensitive but unclassified information is an over-arching term that covers any information, not otherwise indicated above, which the loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, as amended, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information categorized by DHS or other government agencies as: For Official Use Only (FOUO); Official Use Only (OUO); Sensitive Homeland Security Information (SHSI); Limited Official Use (LOU); Law Enforcement Sensitive (LES); Safeguarding Information (SGI); Unclassified Controlled Nuclear Information (UCNI); and any other identifier used by other government agencies to categorize information as sensitive but unclassified.

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of the information to which I am granted access as cited in this Agreement and in accordance with the guidance provided to me relative to the specific category of information.

I understand and agree to the following terms and conditions of my access to the information indicated above:

1. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of information to which I have been provided conditional access, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.
2. By being granted conditional access to the information indicated above, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to the specific categories of information to which I am granted access.
3. I attest that I understand my responsibilities and that I am familiar with and will comply with the standards for protecting such information that I may have access to in accordance with the terms of this Agreement and the laws, regulations, and/or directives applicable to the specific categories of information to which I am granted access. I understand that the United States Government may conduct inspections, at any time or place, for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding information under this Agreement.

4. I will not disclose or release any information provided to me pursuant to this Agreement without proper authority or authorization. Should situations arise that warrant the disclosure or release of such information I will do so only under approved circumstances and in accordance with the laws, regulations, or directives applicable to the specific categories of information. I will honor and comply with any and all dissemination restrictions cited or verbally relayed to me by the proper authority.

5. (a) For PCII - (1) Upon the completion of my engagement as an employee, consultant, or subcontractor under the contract, or the completion of my work on the PCII Program, whichever occurs first, I will surrender promptly to the PCII Program Manager or his designee, or to the appropriate PCII officer, PCII of any type whatsoever that is in my possession.

(2) If the Authorized Entity is a United States Government contractor performing services in support of the PCII Program, I will not request, obtain, maintain, or use PCII unless the PCII Program Manager or Program Manager's designee has first made in writing, with respect to the contractor, the certification as provided for in Section 29.8(c) of the implementing regulations to the CII Act, as amended.

(b) For SSI and SBU - I hereby agree that material which I have in my possession and containing information covered by this Agreement, will be handled and safeguarded in a manner that affords sufficient protection to prevent the unauthorized disclosure of or inadvertent access to such information, consistent with the laws, regulations, or directives applicable to the specific categories of information. I agree that I shall return all information to which I have had access or which is in my possession 1) upon demand by an authorized individual; and/or 2) upon the conclusion of my duties, association, or support to DHS; and/or 3) upon the determination that my official duties do not require further access to such information.

6. I hereby agree that I will not alter or remove markings, which indicate a category of information or require specific handling instructions, from any material I may come in contact with, in the case of SSI or SBU, unless such alteration or removal is consistent with the requirements set forth in the laws, regulations, or directives applicable to the specific category of information or, in the case of PCII, unless such alteration or removal is authorized by the PCII Program Manager or the PCII Program Manager's designee. I agree that if I use information from a sensitive document or other medium, I will carry forward any markings or other required restrictions to derivative products, and will protect them in the same matter as the original.

7. I hereby agree that I shall promptly report to the appropriate official, in accordance with the guidance issued for the applicable category of information, any loss, theft, misuse, misplacement, unauthorized disclosure, or other security violation, I have knowledge of and whether or not I am personally involved. I also understand that my anonymity will be kept to the extent possible when reporting security violations.

8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to the information covered by this Agreement. This may serve as a basis for denying me conditional access to other types of information, to include classified national security information.

9. (a) With respect to SSI and SBU, I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of the information not consistent with the terms of this Agreement.

(b) With respect to PCII I hereby assign to the entity owning the PCII and the United States Government, all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of PCII not consistent with the terms of this Agreement.

10. This Agreement is made and intended for the benefit of the United States Government and may be enforced by the United States Government or the Authorized Entity. By granting me conditional access to information in this context, the United States Government and, with respect to PCII, the Authorized Entity, may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I understand that if I violate the terms and conditions of this Agreement, I could be subjected to administrative, disciplinary, civil, or criminal action, as appropriate, under the laws, regulations, or directives applicable to the category of information involved and neither the United States Government nor the Authorized Entity have waived any statutory or common law evidentiary privileges or protections that they may assert in any administrative or court proceeding to protect any sensitive information to which I have been given conditional access under the terms of this Agreement.

11. Unless and until I am released in writing by an authorized representative of the Department of Homeland Security (if permissible for the particular category of information), I understand that all conditions and obligations imposed upon me by this Agreement apply during the time that I am granted conditional access, and at all times thereafter.

12. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.

13. My execution of this Agreement shall not nullify or affect in any manner any other secrecy or non-disclosure Agreement which I have executed or may execute with the United States Government or any of its departments or agencies.

14. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958, as amended; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 USC 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

15. Signing this Agreement does not bar disclosures to Congress or to an authorized official of an executive agency or the Department of Justice that are essential to reporting a substantial violation of law.

16. I represent and warrant that I have the authority to enter into this Agreement.

17. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me any laws, regulations, or directives referenced in this document so that I may read them at this time, if I so choose.

DEPARTMENT OF HOMELAND SECURITY
NON-DISCLOSURE AGREEMENT
Acknowledgement

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:
---------------------	---	-------------------

I make this Agreement in good faith, without mental reservation or purpose of evasion.

Signature:

WITNESS:

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:
---------------------	---	-------------------

Signature:

Issue Date: 5/11/2004

SAFEGUARDING SENSITIVE BUT UNCLASSIFIED (FOR OFFICIAL USE ONLY) INFORMATION

1. Purpose

This directive establishes Department of Homeland Security (DHS) policy regarding the identification and safeguarding of sensitive but unclassified information originated within DHS. It also applies to other sensitive but unclassified information received by DHS from other government and non-governmental activities.

2. Scope

This directive is applicable to all DHS Headquarters, components, organizational elements, contractors, consultants, and others to whom access to information covered by this directive is granted.

3. Authorities

Homeland Security Act of 2002.

4. Definitions

Access: The ability or opportunity to gain knowledge of information.

For Official Use Only (FOUO): The term used within DHS to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.

Need-to-know: The determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to

perform or assist in a lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Organizational Element: As used in this directive, organizational element is as defined in DHS MD Number 0010.1, Management Directive System and DHS Announcements.

Protected Critical Infrastructure Information (PCII): Critical infrastructure information (CII) is defined in 6 U.S.C. 131(3) (Section 212(3) of the Homeland Security Act). Critical infrastructure information means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. Protected Critical Infrastructure Information is a subset of CII that is voluntarily submitted to the Federal Government and for which protection is requested under the PCII program by the requestor.

Sensitive Security Information (SSI): Sensitive security information (SSI) is defined in 49 C.F.R. Part 1520. SSI is a specific category of information that requires protection against disclosure. 49 U.S.C. 40119 limits the disclosure of information obtained or developed in carrying out certain security or research and development activities to the extent that it has been determined that disclosure of the information would be an unwarranted invasion of personal privacy; reveal a trade secret or privileged or confidential commercial or financial information; or be detrimental to the safety of passengers in transportation.

5. Responsibilities

A. The DHS Office of Security will:

1. Be responsible for practical application of all aspects of the program to protect FOUO.
2. Promulgate Department-wide policy guidance.

B. Heads of DHS Organizational Elements will:

1. Ensure compliance with the standards for safeguarding sensitive but unclassified information as cited in this directive.
2. Designate an official to serve as a Security Officer or Security Liaison.

C. The organizational element's Security Officer/Security Liaison will:

Be responsible for implementation and oversight of the FOUO information protection program and will serve as liaison between the DHS Office of Security and other organizational security officers.

D. DHS employees, contractors, consultants and others to whom access is granted will:

1. Be aware of and comply with the safeguarding requirements for FOUO information as outlined in this directive.
2. Be aware that divulging information without proper authority could result in administrative or disciplinary action.
3. Execute a DHS Form 11000-6, Sensitive But Unclassified Information Non-Disclosure Agreement (NdA), upon initial assignment to DHS. Other individuals not assigned to or contractually obligated to DHS, but to whom access to information will be granted, may be requested to execute an NdA as determined by the program manager to which they will have access.

E. Supervisors and managers will:

1. Ensure that an adequate level of education and awareness is established and maintained that serves to emphasize safeguarding and prevent unauthorized disclosure of FOUO information.
2. Take appropriate corrective actions, to include administrative or disciplinary action as appropriate, when violations occur.

6. Policy and Procedures

A. General

1. The Computer Security Act of 1987, Public Law 100-235, defines "sensitive information" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy." However, with the exception of certain types of information protected by statute, specific, standard criteria and terminology defining the types of information warranting designation as "sensitive information" does not exist within the Federal government. Such designations are left to the discretion of each individual agency.
2. Within the "sensitive but unclassified" arena, in addition to the various categories of information specifically described and protected by statute or regulation, e.g., Tax Return Information, Privacy Act Information, Sensitive Security Information (SSI), Critical Infrastructure Information (CII), Grand Jury

Information, etc. There are numerous additional caveats used by various agencies to identify unclassified information as sensitive, e.g., For Official Use Only; Law Enforcement Sensitive; Official Use Only; Limited Official Use; etc. Regardless of the caveat used to identify it, however, the reason for the designation does not change. Information is designated as sensitive to control and restrict access to certain information, the release of which could cause harm to a person's privacy or welfare, adversely impact economic or industrial institutions, or compromise programs or operations essential to the safeguarding of our national interests.

3. Designation of information as FOUO is not a vehicle for concealing government negligence, ineptitude, illegalities, or other disreputable circumstances embarrassing to a government agency.
4. Information designated as FOUO is not automatically exempt from disclosure under the provisions of the Freedom of Information Act, 5 U.S.C. 552, (FOIA). Information requested by the public under a FOIA request must still be reviewed on a case-by-case basis.

B. For Official Use Only

Within DHS, the caveat "FOR OFFICIAL USE ONLY" will be used to identify sensitive but unclassified information within the DHS community that is not otherwise specifically described and governed by statute or regulation. The use of these and other approved caveats will be governed by the statutes and regulations issued for the applicable category of information.

C. Information Designated as FOUO

1. The following types of information will be treated as FOUO information. Where information cited below also meets the standards for designation pursuant to other existing statutes or regulations, the applicable statutory or regulatory guidance will take precedence. For example, should information meet the standards for designation as Sensitive Security Information (SSI), then SSI guidance for marking, handling, and safeguarding will take precedence.

(a) Information of the type that may be exempt from disclosure per 5 U.S.C. 552, Freedom of Information Act, and its amendments. Designation of information as FOUO does not imply that the information is already exempt from disclosure under FOIA. Requests under FOIA, for information designated as FOUO, will be reviewed and processed in the same manner as any other FOIA request.

(b) Information exempt from disclosure per 5 U.S.C. 552a, Privacy Act.

- (c) Information within the international and domestic banking and financial communities protected by statute, treaty, or other agreements.
- (d) Other international and domestic information protected by statute, treaty, regulation or other agreements.
- (e) Information that could be sold for profit.
- (f) Information that could result in physical risk to personnel.
- (g) DHS information technology (IT) internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 12958, as amended, will be classified as appropriate.
- (h) Systems security data revealing the security posture of the system. For example, threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, and Certification and Accreditation documentation.
- (i) Reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities, whether to persons, systems, or facilities, not otherwise eligible for classification under Executive Order 12958, as amended.
- (j) Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security.
- (k) Developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.

2. Other government agencies and international organizations may use different terminology to identify sensitive information, such as "Limited Official Use (LOU)," and "Official Use Only (OUO)." In most instances the safeguarding requirements for this type of information are equivalent to FOUO. However, other agencies and international organizations may have additional requirements concerning the safeguarding of sensitive information. Follow the safeguarding guidance provided by the other agency or organization. Should there be no such

guidance, the information will be safeguarded in accordance with the requirements for FOUO as provided in this manual. Should the additional guidance be less restrictive than in this directive, the information will be safeguarded in accordance with this directive.

D. Designation Authority

Any DHS employee, detailee, or contractor can designate information falling within one or more of the categories cited in section 6, paragraph C, as FOUO. Officials occupying supervisory or managerial positions are authorized to designate other information, not listed above and originating under their jurisdiction, as FOUO.

E. Duration of Designation

Information designated as FOUO will retain its designation until determined otherwise by the originator or a supervisory or management official having program management responsibility over the originator and/or the information.

F. Marking

1. Information designated as FOUO will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of FOUO markings on materials does not relieve the holder from safeguarding responsibilities. Where the FOUO marking is not present on materials known by the holder to be FOUO, the holder of the material will protect it as FOUO. Other sensitive information protected by statute or regulation, e.g., PClI and SSI, etc., will be marked in accordance with the applicable guidance for that type of information. Information marked in accordance with the guidance provided for the type of information need not be additionally marked FOUO.

(a) Prominently mark the bottom of the front cover, first page, title page, back cover and each individual page containing FOUO information with the caveat "FOR OFFICIAL USE ONLY."

(b) Materials containing specific types of FOUO may be further marked with the applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE," in order to alert the reader of the type of information conveyed. Where the sensitivity of the information warrants additional access and dissemination restrictions, the originator may cite additional access and dissemination restrictions. For example:

WARNING: *This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This*

information shall not be distributed beyond the original addressees without prior authorization of the originator.

(c) Materials being transmitted to recipients outside of DHS, for example, other federal agencies, state or local officials, etc. who may not be aware of what the FOUO caveat represents, shall include the following additional notice:

WARNING: *This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO 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 of an authorized DHS official.*

(d) Computer storage media, i.e., disks, tapes, removable drives, etc., containing FOUO information will be marked "FOR OFFICIAL USE ONLY."

(e) Portions of a classified document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only FOUO information will be marked with the abbreviation (FOUO).

(f) Individual portion markings on a document that contains no other designation are not required.

(g) Designator or originator information and markings, downgrading instructions, and date/event markings are not required.

G. General Handling Procedures

Although FOUO is the DHS standard caveat for identifying sensitive unclassified information, some types of FOUO information may be more sensitive than others and thus warrant additional safeguarding measures beyond the minimum requirements established in this manual. For example, certain types of information may be considered extremely sensitive based on the repercussions that could result should the information be released or compromised. Such repercussions could be the loss of life or compromise of an informant or operation. Additional control requirements may be added as necessary to afford appropriate protection to the information. DHS employees, contractors, and detailees must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel or property as the basis for determining the need for safeguards in excess of the minimum requirements and protect the information accordingly.

1. When removed from an authorized storage location (see section 6.I) and persons without a need-to-know are present, or where casual observation would reveal FOUO information to unauthorized persons, a "FOR OFFICIAL USE ONLY" cover sheet (Enclosure 1) will be used to prevent unauthorized or inadvertent disclosure.
2. When forwarding FOUO information, a FOUO cover sheet should be placed on top of the transmittal letter, memorandum or document.
3. When receiving FOUO equivalent information from another government agency, handle in accordance with the guidance provided by the other government agency. Where no guidance is provided, handle in accordance with the requirements of this directive.

H. Dissemination and Access

1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
2. Access to FOUO information is based on "need-to-know" as determined by the holder of the information. Where there is uncertainty as to a person's need-to-know, the holder of the information will request dissemination instructions from their next-level supervisor or the information's originator.
3. The holder of the information will comply with any access and dissemination restrictions.
4. A security clearance is not required for access to FOUO information.
5. When discussing or transferring FOUO information to another individual(s), ensure that the individual with whom the discussion is to be held or the information is to be transferred has a valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.
6. FOUO information may be shared with other agencies, federal, state, tribal, or local government and law enforcement officials, provided a specific need-to-know has been established and the information is shared in furtherance of a coordinated and official governmental activity. Where FOUO information is requested by an official of another agency and there is no coordinated or other official governmental activity, a written request will be made from the requesting agency to the applicable DHS program office providing the name(s) of personnel for whom access is requested, the specific information to which access is requested, and basis for need-to-know. The DHS program office shall then

determine if it is appropriate to release the information to the other agency official. (see section 6.F for marking requirements)

7. Other sensitive information protected by statute or regulation, i.e., Privacy Act, CII, SSI, Grand Jury, etc., will be controlled and disseminated in accordance with the applicable guidance for that type of information.

8. If the information requested or to be discussed belongs to another agency or organization, comply with that agency's policy concerning third party discussion and dissemination.

9. When discussing FOUO information over a telephone, the use of a STU III (Secure Telephone Unit), or Secure Telephone Equipment (STE), is encouraged, but not required.

I. Storage

1. When unattended, FOUO materials will, at a minimum, be stored in a locked file cabinet, locked desk drawer, a locked overhead storage compartment such as a systems furniture credenza, or similar locked compartment. Materials can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room, or an area where access is controlled by a guard, cipher lock, or card reader.

2. FOUO information will not be stored in the same container used for the storage of classified information unless there is a correlation between the information. When FOUO materials are stored in the same container used for the storage of classified materials, they will be segregated from the classified materials to the extent possible, i.e. separate folders, separate drawers, etc.

3. IT systems that store FOUO information will be certified and accredited for operation in accordance with federal and DHS standards. Consult the DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A, for more detailed information.

4. Laptop computers and other media containing FOUO information will be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure. Storage and control will be in accordance with DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A.

J. Transmission

1. Transmission of hard copy FOUO within the U.S. and its Territories:

(a) Material will be placed in a single opaque envelope or container and sufficiently sealed to prevent inadvertent opening and to show evidence of tampering. The envelope or container will bear the complete name and address of the sender and addressee, to include program office and the name of the intended recipient (if known).

(b) FOUO materials may be mailed by U.S. Postal Service First Class Mail or an accountable commercial delivery service such as Federal Express or United Parcel Service.

(c) FOUO materials may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access, e.g., sealed envelope.

2. Transmission to Overseas Offices: When an overseas office is serviced by a military postal facility, i.e., APO/FPO, FOUO may be transmitted directly to the office. Where the overseas office is not serviced by a military postal facility, the materials will be sent through the Department of State, Diplomatic Courier.

3. Electronic Transmission.

(a) Transmittal via Fax. Unless otherwise restricted by the originator, FOUO information may be sent via nonsecure fax. However, the use of a secure fax machine is highly encouraged. Where a nonsecure fax is used, the sender will coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end. The holder of the material will comply with any access, dissemination, and transmittal restrictions cited on the material or verbally communicated by the originator.

(b) Transmittal via E-Mail

(i) FOUO information transmitted via email should be protected by encryption or transmitted within secure communications systems. When this is impractical or unavailable, FOUO may be transmitted over regular email channels. For added security, when transmitting FOUO over a regular email channel, the information can be included as a password protected attachment with the password provided under separate cover. Recipients of FOUO information will comply with any email restrictions imposed by the originator.

(ii) Per DHS MD 4300, DHS Sensitive Systems Handbook, due to inherent vulnerabilities, FOUO information shall not be sent to personal email accounts.

(c) DHS Internet/Intranet

(i) FOUO information will not be posted on a DHS or any other internet (public) website.

(ii) FOUO information may be posted on the DHS intranet or other government controlled or sponsored protected encrypted data networks, such as the Homeland Security Information Network (HSIN). However, the official authorized to post the information should be aware that access to the information is open to all personnel who have been granted access to that particular intranet site. The official must determine the nature of the information is such that need-to-know applies to all personnel; the benefits of posting the information outweigh the risk of potential compromise; the information posted is prominently marked as FOR OFFICIAL USE ONLY; and information posted does not violate any provisions of the Privacy Act.

K. Destruction

1. FOUO material will be destroyed when no longer needed. Destruction may be accomplished by:

(a) "Hard Copy" materials will be destroyed by shredding, burning, pulping, pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.

(b) Electronic storage media shall be sanitized appropriately by overwriting or degaussing. Contact local IT security personnel for additional guidance.

(c) Paper products containing FOUO information will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

L. Incident Reporting

1. The loss, compromise, suspected compromise, or unauthorized disclosure of FOUO information will be reported. Incidents involving FOUO in DHS IT systems will be reported to the organizational element Computer Security Incident Response Center in accordance with IT incident reporting requirements.

2. Suspicious or inappropriate requests for information by any means, e.g., email or verbal, shall be report to the DHS Office of Security.

3. Employees or contractors who observe or become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of FOUO information will report it immediately, but not later than the next duty day, to the originator and the local Security Official.

4. Additional notifications to appropriate DHS management personnel will be made without delay when the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned or on-going operation.

5. At the request of the originator, an inquiry will be conducted by the local security official or other designee to determine the cause and affect of the incident and the appropriateness of administrative or disciplinary action against the offender.

12/14/2005

TSA FOIA DIVISION - 571-227-2300

FOIA CASE NO: 06-0245

RECEIVED: 12/30/05

SUSPENSE DATE: 1/11/06

SPECIAL INSTRUCTIONS: 10790 Parkridge Boulevard, Suite 200

Room 7480

Reston, VA 20191

Tel: (703) 707-3500

Fax: (703) 707-6201

www.input.com



Transportation Security Administration
TSA-20, West Tower, FOIA Division
601 South 12th Street
Arlington, VA 22202-4220

Dear FOIA Officer,

Under the Freedom of Information Act, 5 U.S.C. § 552, as amended, I am requesting documents regarding all contracts awarded under the MANAGEMENT CONTROL PROGRAM SUPPORT requirement. Specifically, I am requesting copies of the following information/documents:

- Awarded contract
- All related attachments and exhibits
- All task/delivery/purchase orders
- List of proposal submitters

If possible, I would prefer to receive the documents in electronic format. If not, hard copies of responsive documents will be more than adequate. If your office does not maintain these public records, please let me know who does and include the proper custodian's name and address.

Your response is respectfully requested within 20 working days of your receipt of this letter. §552(a)(6)(A)(1). I agree to accept clearly releasable portions of the requested documents, but if all or any part of this request is denied, please cite each specific exemption that justifies your withholding of information

I hereby agree to assume all the search, duplication, and review fees in the amount of \$100. Please notify me if the cost of fulfilling my request will exceed that amount.

Whenever possible, please refer to FOIA ID 7480 in any response letter, email, fax, or invoice.

Thank you for your assistance,


Michael Person
mperson@input.com