

SECTION A - STANDARD FORM 33

SOLICITATION, OFFER AND AWARD		1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)		RATING	PAGE OF 1 191 Pages
2. CONTRACT NO. HSHQDC-09-D-00003	3. SOLICITATION NO. HSHQDC-09-R-00016	4. TYPE OF SOLICITATION <input type="checkbox"/> SEALED BID (IFB) <input checked="" type="checkbox"/> NEGOTIATED (RFP)		5. DATE ISSUED	6. REQUISITION/PURCHASE RSTR-09-00005
7. ISSUED BY U.S. DEPARTMENT OF HOMELAND SECURITY OFFICE OF PROCUREMENT OPERATIONS 245 MURRAY LANE, SW, BLDG 410 WASHINGTON, DC 20528		CODE DHS	8. ADDRESS OFFER TO (if other than Item 7) ANALYTIC SERVICES INC. 2900 SOUTH QUINCY STREET, SUITE 800 ARLINGTON, VA 22206-2285		

NOTE: In sealed bid solicitations "offer" and "offeror" mean "bid" and "bidder".

SOLICITATION

9. Sealed offers in original and 5 copies for furnishing the supplies or services in the Schedule will be received at the place spelled out in Item 8, or if hand carried, in the depository located in SEE SECTION L, 5 and L.9 until 12:00 Noon (Eastern) local time January 5, 2009.
(Hour) (Date)

CAUTION - LATE Submissions, Modifications, and Withdrawals: See Section L, Provision No. 52.214-7 or 52.215-1. All offers are subject to all terms and conditions contained in this solicitation.

10. FOR INFORMATION CALL:	A. NAME Sharon Flowers	B. TELEPHONE NO. (NO COLLECT CALLS)		C. E-MAIL ADDRESS s&a ffrdc@hq.dhs.gov
		AREA CODE	NUMBER	EXT.

11. TABLE OF CONTENTS

(✓)	SEC.	DESCRIPTION	PAGE(S)	(✓)	SEC.	DESCRIPTION	PAGE(S)
PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES			
X	A	SOLICITATION/CONTRACT FORM	1	X	I	CONTRACT CLAUSES	40 - 52
X	B	SUPPLIES OR SERVICES AND PRICES/COSTS	2 - 3	PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.			
X	C	DESCRIPTION/SPECS./WORK STATEMENT	4 - 12	X	J	LIST OF ATTACHMENTS	54
X	D	PACKAGING AND MARKING	13 - 14	PART IV - REPRESENTATIONS AND INSTRUCTIONS			
X	E	INSPECTION AND ACCEPTANCE	15	X	K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	191
X	F	DELIVERIES OR PERFORMANCE	16 - 22	PART V - INSTRS., CONDS., AND NOTICES TO OFFER			
X	G	CONTRACT ADMINISTRATION DATA	23 - 28	X		INSTRS., CONDS., AND NOTICES TO OFFER	
X	H	SPECIAL CONTRACT REQUIREMENTS	29 - 39	X		EVALUATION FACTORS FOR AWARD	

OFFER (Must be fully completed by offeror)

NOTE: Item 12 does not apply if the solicitation includes the provisions at 52.214-16, Minimum Bid Acceptance Period.

12. In compliance with the above, the undersigned agrees, if this offer is accepted within 180 calendar days from the date for receipt of offers specified above, to furnish any or all items upon which prices are offered at the price set opposite each item, delivered at the designated point(s), within the time specified in the schedule.

13. DISCOUNT FOR PROMPT PAYMENT (See Section I, Clause No. 52.232-8)	10 CALENDAR DAYS	20 CALENDAR DAYS	30 CALENDAR DAYS	CALENDAR DAYS
	%	%	%	%
14. ACKNOWLEDGMENT OF AMENDMENTS (The offeror acknowledges receipt of amendments to the SOLICITATION for offers and related)	AMENDMENT NO.	DATE	AMENDMENT NO.	DATE

15A. NAME AND ADDRESS OF OFFEROR Analytic Services Inc. 2900 South Quincy Street Ste 800, Arlington, VA 22206	CODE	FACILITY 44458	16. NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER (Type or Print) Ruth A. David President and Chief Executive Officer
15B. TELEPHONE NUMBER AREA CODE: 703 NUMBER: 716 EXT.: 2000	15C. CHECK IF REMITTANCE ADDRESS IS DIFFERENT FROM ABOVE - ENTER SUCH ADDRESS IN SCHEDULE. <input type="checkbox"/>		17. SIGNATURE (b) (6)
			18. OFFER DATE 5 Mar 2009

AWARD (To be completed by Government)

19. ACCEPTED AS TO ITEMS NUMBERED	20. AMOUNT	21. ACCOUNTING AND APPROPRIATION See G.1	
22. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION: <input type="checkbox"/> 10 U.S.C 2304(c) () <input type="checkbox"/> 41 U.S.C. 253(c) ()		23. SUBMIT INVOICES TO ADDRESS SHOWN IN (4 copies unless otherwise specified)	ITEM
24. ADMINISTERED BY (if other than Item 7) CODE		25. PAYMENT WILL BE MADE BY CODE As specified on individual orders	
26. NAME OF CONTRACTING OFFICER (Type or print) Sharon Flowers		27. UNITED STATES OF AMERICA <i>Sharon Flowers</i> (Signature of Contracting Officer)	28. AWARD DATE 3-5-2009

IMPORTANT - Award will be made on this Form, or on Standard Form 26, or by other authorized official written notice.

AUTHORIZED FOR LOCAL REPRODUCTION
Previous edition is unusable

STANDARD FORM 33 (REV. 9-97)
Prescribed by GSA - FAR (48 CFR) 53.214(c)

U.S. Department of Homeland Security



HSSAI

Homeland Security Studies and Analysis Institute

HSHQDC-09-D-00003

(This page is intentionally left blank.)

Table of Contents

SECTION A – STANDARD FORM 33.....	1
SECTION B - SUPPLIES OR SERVICES AND PRICE/COSTS.....	2
B.1 Period of Performance.....	2
B.2 Type of Contract.....	2
B.3 Contract Line Items	2
B.4 Indirect Cost	3
B.5. Fixed Fee.....	3
B.6 Minimum Guarantee and Maximum Limitation.....	3
B.7 Adding New Labor Categories after Contract Award.....	3
SECTION C – STATEMENT OF OBJECTIVES... ..	4
C.1 Scope of Contract.....	4
C.2 Tasks Performed for Federal Agencies Other Than the DHS Sponsors.....	5
C.3 Use of Performance Based Procedures in FFRDC Contract.....	6
C.4 Management Plan.....	6
C.5 Research Plan.....	9
C.6 Contractor Quality Control (QC)	11
C.7 Task Ordered Projects.....	11
C.8 Contractor Employees.....	11
C.9 Contract Security Classification Specification	12
C.10 Environmental Protection.....	12
SECTION D - PACKAGING AND MARKING.....	13
D.1 Markings.....	13
D.2 Branding.....	13
D.3 Publication & Communications Concerning Work Performed Under this Contract.....	13
D.4 Dissemination of Contract Information.....	14
SECTION E - INSPECTION AND ACCEPTANCE.....	15
E.1 Clauses Incorporated by Reference.....	15
E.2 Scope of Inspection.....	15
E.3 Evaluation and Acceptance.....	15
SECTION F - DELIVERIES OR PERFORMANCE.....	16
F.1 General.....	16
F.2 Clauses Incorporated by Reference.....	16
F.3 FFRDC Period of Performance.....	16
F.4 Task Order Performance Period and Pricing.....	16
F.5 Reporting Requirements.....	16
F.5.1 Technical and Progress Reporting Requirements.....	16
F.5.2 Task and FFRDC Monthly Status Report.....	19
F.5.3 Verbal Reports and Liaison.....	20
F.6 Place of Performance.....	20

F.7	Notice to the Government of Delays.....	20
F.8	DHS-Furnished Information.....	20
F.9	DHS-Furnished Property.....	21
F.10	Deliverable Requirements.....	21

SECTION G - CONTRACT ADMINISTRATION DATA.....23

G.1	Accounting and Appropriation Data.....	23
G.2	Points of Contact.....	23
G.2.1	Contracting Officer's Authority.....	24
G.2.2	Contracting Officer's Technical Representative	24
G.2.3	Task Order Manager.....	24
G.3	Task Order Process and Delivery	24
G.4	Preparation of Vouchers	27
G.5	Payment Information	28
G.6	Travel.....	28
G.6.1	Travel Outside of the United States	28

SECTION H – SPECIAL CONTRACTING REQUIREMENTS

H.1	Standard of Conduct at Government Installation.....	29
H.2	Advertisements, Publicizing Awards & News Releases.....	29
H.3	Observance of Legal Holidays & Excused Absence	29
H.4	Insurance.....	30
H.5	Information Technology Accessibility for Persons with Disabilities.....	30
H.6	Organizational Conflict of Interest.....	31
H.7	Task Performed for Federal Agencies Other than the Sponsors.....	33
H.8	Consultants.....	33
H.9	Investigating & Reporting Possible Scientific Misconduct	33
H.10	Security Requirements	34
H.10.1	Top Secret, SCI Personnel & Facility Clearance Requirement	35
H.10.2	General Security Requirements	35
H.10.3	Employment Eligibility	36
H.10.4	Security Management.....	36
H.10.5	Information Technology Security Clearance.....	36
H.10.6	Information Technology Security Training & Oversight	36
H.11	Conflict of Interest.....	37
H.12	Reporting Waste, Fraud, Abuse and Theft.....	37
H.13	Interface with Participating Associate Contractors (PAC).....	37
H.14	Freedom of Information Act (FOIA) and Privacy Act.....	37
H.15	Handling of Data.....	37
H.16	Key Personnel or Facilities	39
H.17	Strikes or Picketing Affecting Access to a DHS Facility.....	39
H.18	DCAA.....	39

SECTION I - CONTRACT CLAUSES

I.1	General.....	40
I.2	Clauses Incorporated By Reference.....	40
I.3	Security Requirements.....	42
I.4	Notification of Ownership Changes.....	43
I.5	Ordering	43
I.6	Order Limitations.....	44
I.7	Indefinite Quantity	44
I.8	Option to Extend Services.....	45
I.9	Option to Extend the Term of the Contract	45
I.10	Notification of Employees concerning payment of union dues and fees.....	46
I.11	Rights to proposal data (Technical).....	48
I.12	Notification of Changes.....	48
I.13	Security Requirements for unclassified information Technology Resources.....	50
I.14	Limitation of Future Contracting.....	51
I.15	Small Business Subcontracting Reporting.....	52
I.16	DHS Mentor-Protégé Program.....	52

SECTION J – LIST OF ATTACHMENTS.....	54
--------------------------------------	----

ATTACHMENTS

ATTACHMENT J-1 – Sponsoring Agreement.....	55
ATTACHMENT J-2 – Monthly Contractor Financial Report.....	67
ATTACHMENT J-3 – Non-disclosure Agreement, DHS Form 11000-6.....	70
ATTACHMENT J-4 – Contract Security Classification Specification, DD254.....	73
ATTACHMENT J-5 – Small Business Concerns Subcontracting Plan.....	74
ATTACHMENT J-6 – DHS Certification and Accreditation Guide/Templates.....	85
ATTACHMENT J-7 – DHS Directive #0143-04.....	172
Section K Representations and Certifications.....	191

SECTION A – STANDARD FORM 33

SOLICITATION, OFFER AND AWARD		1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	RATING	PAGE OF 1 191 Pages
2. CONTRACT NO. HSHQDC-09-D-00003	3. SOLICITATION NO. HSHQDC-09-R-00016	4. TYPE OF SOLICITATION <input type="checkbox"/> SEALED BID (IFB) <input checked="" type="checkbox"/> NEGOTIATED (RFP)	5. DATE ISSUED	6. REQUISITION/PURCHASE RSTR-09-00005
7. ISSUED BY U.S. DEPARTMENT OF HOMELAND SECURITY OFFICE OF PROCUREMENT OPERATIONS 245 MURRAY LANE, SW, BLDG 410 WASHINGTON, DC 20528		CODE DHS	8. ADDRESS OFFER TO (If other than Item 7) ANALYTIC SERVICES INC. 2900 SOUTH QUINCY STREET, SUITE 800 ARLINGTON, VA 22206-2265	

NOTE: In sealed bid solicitations "offer" and "offeror" mean "bid" and "bidder".

SOLICITATION

9. Sealed offers in original and 5 copies for furnishing the supplies or services in the Schedule will be received at the place spelled out in Item 8, or if hand carried, in the depository located in SEE SECTION L.5 and L.9 until 12:00 Noon (Eastern) local time January 5, 2009.
(Hour) (Date)

CAUTION - LATE Submissions, Modifications, and Withdrawals: See Section L, Provision No. 52.214-7 or 52.215-1. All offers are subject to all terms and conditions contained in this solicitation.

10. FOR INFORMATION CALL:	A. NAME Sharon Flowers	B. TELEPHONE NO. (NO COLLECT CALLS) AREA CODE NUMBER EXT.	C. E-MAIL ADDRESS s&a ffrdc@hq.dhs.gov
---------------------------	---------------------------	--	---

11. TABLE OF CONTENTS

(✓)	SEC.	DESCRIPTION	PAGE(S)	(✓)	SEC.	DESCRIPTION	PAGE(S)
PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES			
X	A	SOLICITATION/CONTRACT FORM	1	X	I	CONTRACT CLAUSES	40 - 52
X	B	SUPPLIES OR SERVICES AND PRICES/COSTS	2 - 3	PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.			
X	C	DESCRIPTION/SPECS./WORK STATEMENT	4 - 12	X	J	LIST OF ATTACHMENTS	54
X	D	PACKAGING AND MARKING	13 - 14	PART IV - REPRESENTATIONS AND INSTRUCTIONS			
X	E	INSPECTION AND ACCEPTANCE	15	X	K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	191
X	F	DELIVERIES OR PERFORMANCE	16 - 22				
X	G	CONTRACT ADMINISTRATION DATA	23 - 28	X		INSTRS., CONDS., AND NOTICES TO OFFER	
X	H	SPECIAL CONTRACT REQUIREMENTS	29 - 39	X		EVALUATION FACTORS FOR AWARD	

OFFER (Must be fully completed by offeror)

NOTE: Item 12 does not apply if the solicitation includes the provisions at 52.214-16, Minimum Bid Acceptance Period.

12. In compliance with the above, the undersigned agrees, if this offer is accepted within 180 calendar days from the date for receipt of offers specified above, to furnish any or all items upon which prices are offered at the price set opposite each item, delivered at the designated point(s), within the time specified in the schedule.

13. DISCOUNT FOR PROMPT PAYMENT (See Section I, Clause No. 52.232-8)	10 CALENDAR DAYS %	20 CALENDAR DAYS %	30 CALENDAR DAYS %	CALENDAR DAYS %
14. ACKNOWLEDGMENT OF AMENDMENTS (The offeror acknowledges receipt of amendments to the SOLICITATION for offerors and related	AMENDMENT NO.		DATE	

15A. NAME AND ADDRESS OF OFFEROR	CODE	FACILITY	16. NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER (Type of Print)
15B. TELEPHONE NUMBER AREA CODE NUMBER EXT.	15C. CHECK IF REMITTANCE ADDRESS IS DIFFERENT FROM ABOVE - ENTER SUCH ADDRESS IN SCHEDULE. <input type="checkbox"/>		17. SIGNATURE
			18. OFFER DATE

AWARD (To be completed by Government)

19. ACCEPTED AS TO ITEMS NUMBERED	20. AMOUNT	21. ACCOUNTING AND APPROPRIATION See G.1	
22. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION: <input type="checkbox"/> 10 U.S.C 2304(c)() <input type="checkbox"/> 41 U.S.C. 253(c)()		23. SUBMIT INVOICES TO ADDRESS SHOWN IN (4 copies unless otherwise specified)	ITEM
24. ADMINISTERED BY (If other than Item 7)	CODE	25. PAYMENT WILL BE MADE BY As specified on individual orders	
26. NAME OF CONTRACTING OFFICER (Type or print) Sharon Flowers		27. UNITED STATES OF AMERICA (Signature of Contracting Officer)	28. AWARD DATE

IMPORTANT – Award will be made on this Form, or on Standard Form 26, or by other authorized official written notice.

SECTION B - SUPPLIES OR SERVICES AND PRICES/COSTS

The Contractor shall provide specialized technical expertise to the Department of Homeland Security (DHS) leadership to transform mission-level goals into strategies, operational requirements, and performance metrics, constrained by cost and schedule. The technical expertise including all management, labor, facilities, and materials necessary for performance shall be in accordance with issued task order (TOs). TOs will be Cost-Plus-Fixed-Fee and will be issued in accordance with the procedures set forth in Section G of this contract.

B.1 Period of Performance

The contract will be for a twelve month base year from date of award with four (4) one year option periods. In accordance with FAR 35.017-1(e), the term of the contract will not exceed five (5) years but can be renewed, as a result of periodic review, in increments not to exceed five (5) years. This is not a multi-year contract as defined in FAR 17.1. Task orders (TOs) will be issued with specific performance periods.

B.2 Type of Contract

This is an indefinite delivery, indefinite quantity (IDIQ) type with task orders to be issued on a cost plus fixed fee (CPFF) basis.

B.3 Contract Line Items (CLINs)

CLIN	Description	POP	Est. Cost	Fixed Fee (2.5%)	Total
0001	Establishment and Operation of a Federally Funded Research and Development Center (Base Year)	12 months	(b) (4)	(b) (4)	\$50,426,990
1001	HSSAI Studies & Analysis (Option Year 1)	12 months	(b) (4)	(b) (4)	\$51,225,723
2001	HSSAI Studies & Analysis (Option Year 2)	12 months	(b) (4)	(b) (4)	\$53,447,761
3001	HSSAI Studies & Analysis (Option Year 3)	12 months	(b) (4)	(b) (4)	\$55,683,123
4001	HSSAI Studies & Analysis (Option Year 4)	12 months	(b) (4)	(b) (4)	<u>\$57,927,693</u>
Total			(b) (4)	(b) (4)	\$268,711,291
Total Estimated Cost-Plus-Fixed-Fee -					\$268,711,291

B.4 Indirect Costs

The Contractor will be reimbursed for indirect costs at the following rate(s) subject to appropriate adjustment when the final rate(s) for the period are established:

Cost Center	Base Year	Option Year 1	Option Year 2	Option Year 3	Option Year 4
Fringe	(b) (4)				
Overhead	(b) (4)				
Fringe	(b) (4)				
G&A	(b) (4)				

B.5 Fixed-Fee

The fixed-fee percentage of this contract is (b) (4). The fixed-fee amount of an issued task order shall be established at the issuance of the task. Should the cost of the order increase during performance, the amount of the fee shall not change but remain fixed at the value established when the task was issued. The fixed-fee withholding provisions contained in clause 52.216-8, Fixed-Fee, are applicable to individual task orders. A modification or change to a task order directing additional or new work shall be fee bearing. If the cost of the contract does not reach the maximum value contained in clause, Estimated Cost and Fixed Fee, then the total contract fee shall be the sum of all fee dollars under issued tasks. Conversely, if the cost of the contract exceeds the maximum value contained in this Paragraph, then the Contractor's fee shall not be increased.

B.6 Minimum Dollar Guarantee and Maximum Contract Limitation

The minimum value and guarantee of this contract is \$25,000 (Estimated cost and Fixed Fee). Orders beyond the minimum will be determined by user needs. The exercise of any option period does not re-establish the contract minimum. The Government shall issue one or more task orders for an amount not less than this minimum. There will be no further obligation on the part of the Government to issue additional orders thereafter. The maximum value of this contract is \$268,711,291 (Estimated Cost and Fixed Fee) over a five year period.

B.7 Adding New Labor Categories After Contract Award

The labor categories listed in the pricing tables within the Contractor's proposal represent the Contractor's best analysis of current and projected SAI requirements. The Government does not intend to add any labor categories to the SAI contract after contract award. However, changes in the DHS mission, the emergence of new technologies, and other fundamental changes affecting the SAI requirements may necessitate the addition of new labor categories. Either annually, or at the Government's request, the Contractor may propose additional labor categories/descriptions/rates to add to the contract that are necessary for performance. The Government will negotiate these rates on a case by case basis.

(End of Section B)

SECTION C – STATEMENT OF OBJECTIVES

C.1 Scope of Contract

The Science and Technology (S&T) Directorate of DHS proposes to establish a contract for a Federally Funded Research and Development Center (FFRDC) on behalf of the Department to be known as the “Homeland Security Studies and Analysis Institute” (HSSAI). The purpose of this FFRDC is to provide specialized technical expertise to Department program managers to transform mission-level goals into strategies, operational requirements, and performance metrics, constrained by cost and schedule. Through studies and analysis, the Institute shall provide recommendations for policy and operational changes, as well as technology insertion concepts, throughout the federal, state, local, tribal, public and private sector organizations that make up the homeland security enterprise. The SAI shall generally work on the most complex homeland security issues and problems. The SAI will promote fair and open competition for the development and delivery of homeland security enterprise capabilities by providing independent and objective technical expertise in: cross-cutting mission analysis, strategic studies and assessments, modeling of operational concepts and policy trade-offs within and across mission areas, system simulations and technical assessments to evaluate mission trade-offs, creation and evolution of high-level concepts of operation, development of top-level system and operational requirements and performance metrics, operational analysis across the homeland security enterprise, and analytic support for operational testing and evaluation in tandem with the Government’s acquisition process. The SAI shall ensure a logical optimization of mission and system-of-system tradeoffs from a long term perspective based on system/program lifecycle costs. Over time, this FFRDC will help the Department develop a homeland security enterprise “system of systems” approach and leadership that will promote efficiencies and synergies across all missions. Through its long term relationship with the Department, the SAI shall promote frameworks and strategies to enhance the general understanding of the trade-offs inherent in reducing our Nation’s risk to terrorism and catastrophic incidents through, among other things, improved interoperability and information sharing across the homeland security enterprise.

The role of the S&T Directorate is to provide an SAI program office that supports the FFRDC in terms of developing long-term and short-term strategies for reaching across the Department to negotiate task orders in support of the most critical and strategic programs. The SAI program office shall consist of an Executive Agent (EA), Program Manager (PM), and Contracting Officer’s Technical Representative (COTR), who shall be the focal point for negotiating tasks between the SAI and the various DHS components. The SAI program office will also negotiate issue resolutions between the SAI and task sponsors after tasks have been awarded. Primary direction and technical feedback on specific task orders will come from sponsoring component officials. The SAI program office will provide additional guidance on technical quality and consistency throughout the term of the contract; and will also provide contract administration support, for example: task order processing, security, IT certification, invoice payments and progress reporting, etc. Most tasks will be sponsored by program offices located throughout the Department and include most of the twenty two legacy agencies that make up the Department.

The Department’s systems engineering FFRDC will generally provide program level concept evolution, system and sub-system modeling and simulation, system engineering and program management best practices, sub-system standards frameworks focused particularly on interface

management and interoperability, as well as development test and evaluation analysis for the most critical homeland security programs. DHS laboratory FFRDC(s) and national laboratory FFRDCs will generally provide system and component prototypes and threat analysis support that is not normally available in the private sector.

The Homeland Security Act of 2002 (Section 305 of PL 107-296, as codified in 6 U.S.C. 185), herein referred to as the “Act,” authorizes the Secretary, acting through the Under Secretary for Science and Technology, to establish one or more FFRDCs to provide independent analysis of homeland security issues, or to carry out other responsibilities under the Act. The SAI is intended to provide the government with the necessary expertise to conduct: cross-cutting mission analysis, strategic studies and assessments, development of models that baseline current capabilities, development of simulations and technical evaluations to evaluate mission trade-offs, creation and evolution of high-level operational and system concepts, development of top-level system and operational requirements and performance metrics, operational analysis across the homeland security enterprise, and analytic support for operational testing and evaluation in tandem with the government’s acquisition process. The SAI shall ensure a logical optimization of mission and system-of-system tradeoffs from a long term perspective based on system lifecycle costs. Over time, this FFRDC will help the Department develop a homeland security enterprise “system of systems” approach that will promote efficiencies and synergies across all homeland security mission areas.

Performance shall be in accordance with all terms and conditions and specifications as stipulated herein.

C.2 Tasks Performed for Federal Agencies Other Than the DHS Sponsors

It is not the Government’s intent that a FFRDC use its privileged information or access to compete with the private sector. However, the HSSAI FFRDC may perform work for non-sponsors provided that such work is in compliance with FAR 35.017-3 and applicable DHS policies. Projects may be performed by the HSSAI FFRDC for other Federal, State, local government agencies and non-profit organizations, provided that the following conditions are met. The HSSAI FFRDC Contractor may only perform work for non-sponsors when authorized by the Government Contracting Officer under the following conditions:

- The task is consistent with the purpose, mission, general scope of effort, or special competencies of the HSSAI FFRDC as specified in the contract and sponsoring agreement, and is subject to any established STE ceiling;
- The HSSAI FFRDC has received the prior written approval of the DHS S&T Executive Agent, generally based on co-advocacy for the project from a particular office within the Department;
- Funds for the projects have been transferred from the funding agency or entity to DHS for disbursement under the HSSAI FFRDC contract;
- The HSSAI FFRDC and the tasking agency or agencies agree to fully disclose all aspects of the work being performed, including draft documents, to DHS upon request;
- DHS receives copies of all final reports;
- Interagency funds may also be used to support and/or augment Sponsor tasks, with the prior consent of the Contracting Officer; and
- For DoD users, DHS will require a copy of their notification to Congress in accordance with FAR subpart 35.017-7 prior to award of the task order.

C.3 Use of Performance Based Procedures in FFRDC Contract

This contract will be evaluated using performance management techniques and insight of Contractor performance rather than strict oversight. The ability to make decisions based on performance data analysis is the cornerstone of this type of performance management. The use of Contractor developed metrics for both the basic contract and task orders shall focus on desired outcomes and not interim process steps.

Interim process metrics will be developed and delegated to the Contractor who shall manage the processes and practices used to achieve contract outcomes by a Contractor Quality Control Plan. Use of an outcome focus provides the Contractor with the flexibility to continuously improve and innovate over the course of the contract as long as the critical outcomes expected are being achieved. Deliverables that can provide measures of technical quality toward accomplishing task goals shall be established prior to award of task orders.

The Contractor shall have the ability and opportunity to negotiate the task specific approach performance to meet the quality and requirements standards of individual Task Orders. Incentives or disincentives are not applicable to any task order issued during the base period or any option period.

The only exceptions to outcome-focused process procedures will be those services and performance items required by law, (local, state, and federal) and compelling business situations such as safety and security that the Contractor must follow. All objectives, as appropriate, will be incorporated into the Contractor's Quality Control Plan. The Contractor shall furnish and otherwise accomplish all things necessary for or incident to the complete performance of the work as described throughout this Statement of Objectives (SOO) and the contract provisions.

C.4 Management Plan

The Contractor shall deliver an FFRDC Management Plan that describes how they intend to operate and perform to the requirements of this RFP, and in particular, how they intend to meet the requirements of this section. This plan shall be updated annually, as required, throughout the performance of the Contract. The Contractor shall be responsible for providing technical and integration expertise to DHS senior leadership as a trusted agent, particularly in the evolution of the most complex and critical homeland security mission areas. The purpose of the HSSAI FFRDC is to help the Department address what must be accomplished, in a risk-informed manner, to meet and measure performance of homeland security mission goals and objectives with limited resources. The general goal is to maximize risk reduction across the gamut of terrorism and major disaster scenarios based on available funding and dual-use solution strategies. The SAI FFRDC will provide the Government with the necessary expertise to conduct: cross-cutting mission analysis, strategic studies and assessments, development of models that baseline current capabilities, development of simulations and technical evaluations to evaluate mission trade-offs, creation and evolution of high-level operational and system concepts, development of top-level system and operational requirements and performance metrics, operational analysis across the homeland security enterprise, and analytic support for operational testing and evaluation in tandem with the Government's acquisition process. The SAI shall ensure a logical optimization of mission and system-of-system tradeoffs from a long

term perspective based on system lifecycle costs. Over time, this FFRDC will help the Department develop a homeland security enterprise system-of-systems approach that will promote efficiencies and synergies across all homeland security mission areas.

The FFRDC shall operate based on an annual research plan that will consist of core tasks funded by the S&T program office and task order studies funded from sponsors across the Department. The core program is expected to be maintained at roughly 20% of the total Institute funding that is envisioned to enable the Institute to provide, among other things:

- Quick-response and strategic forward and field analysts wherever and whenever required
- Leadership on cross-cutting and homeland security enterprise-wide critical and strategic issues
- Development of risk and other models and methods for understanding and comparing the mission requirements, performance metrics, and measures of effectiveness across the homeland security enterprise

Task order funding from the Department will address a variety of studies and analysis, including:

- Conduct strategic assessments of homeland security threats, vulnerabilities and consequences as well as national and international strategies for addressing the risk to the Nation.
- Examine broad security topics such as countering vulnerabilities to critical infrastructures; proliferation of nuclear, chemical, and biological weapons; regional political, economic, military, and terrorist trends; and international terrorist cooperation and assess domestic and international implications of trade and technology cooperation, plans, and controls.
- Develop top level mission risk and risk reduction (threat, vulnerability, consequence) resource allocation models, component tradeoff simulations, and tools and metrics to evaluate mission tradeoffs and mission integration strategies.
- Develop system and system-of-system concepts through analysis of alternatives to address the most strategic and critical needs of the homeland security enterprise.
- Analyze the risk (threat, vulnerability, consequence) reduction potential of constrained resources by analyzing synergies obtained through common homeland security enterprise systems developments, interoperability, and common hardware/software interfaces and protocols.
- Develop top-level program requirements and system performance and effectiveness metrics based on mission goals.
- Develop and promote standardization of effective and efficient operational modeling, simulation, test and evaluation best practices for homeland security programs to provide independent and objective assessments based on mission and program goals.
- Develop methods for identification, particularly within the various DHS Integrated Process Teams (IPTs), of critical capability gaps particularly in areas where policy, operations, and/or technology may be expected to contribute substantially to solutions; and develop trade-off studies and roadmaps for “filling the gap.”

- Design and provide support for the conduct of homeland security-related exercises, games, and simulations, including the examination of past incidents, tabletop and operational exercises, and nominal operations to determine lessons learned and the implications for homeland security planning. A principal focus of these studies also will be on assessing national response and multi-agency collaboration and coordination; interoperability of federal with state and local personnel and systems; and logistics support.
- Provide assistance to the homeland security enterprise in establishing test-beds requirements to evaluate the effectiveness of technologies under development and assess the appropriateness of such technologies for deployment; and conduct assessments of technology feasibility, performance, producibility, demonstrations, and development risks.
- Conduct operational analysis, particularly at field activities for extended (months to 1-2 years) periods, to provide objective assessments, systems evaluations, and other technical and analytic support that promotes the identification and understanding of the interplay of operation elements, like: doctrine, organization, training, material, leadership, education, personnel, facilities, etc. in the need for identifying solutions to new and evolving mission requirements including the creation of capabilities to provide and promote security, privacy, and the protection of civil rights and civil liberties.
- Use economic (lifecycle) and policy analyses to assess the distributed costs and benefits of alternative approaches to enhancing security including leveraging of homeland security, particularly R&D, assets across the Nation and with international partners.
- Examine infrastructure and support activities, including issues related to major acquisitions and R&D planning; advanced manufacturing practices; the governmental and commercial technology base; mobilization and stockpiling of critical materials; the training establishment; logistics needs; and environmental technologies.
- Promote ethics in acquisition through an understanding of: the need for objective development of operational requirements and performance metrics, and operational test and evaluation planning and analysis independent from the development program; promotion of fair and open competition in acquisitions through high quality technical data packages and quality oversight, trusted agent relationships with the government task sponsors and the FFRDC program office, establishment of staff and organizational conflict or interest protocols.

Within and across these core areas, DHS sponsors' specific needs are expected to evolve over time, and the HSSAI FFRDC's capabilities and areas of concentration will evolve accordingly. The assigned tasks will include some quick-response ad-hoc analysis and reviews (up to three months in duration). Most tasks will be for medium-term studies (3-12 months) to provide in-depth strategic, technology and/or operational support to components or field activities. However, some tasks are expected to be long-term tasks (more than 1 year) that align with the most complex and critical issues facing the homeland security enterprise.

The Contractor will also implement a broad-based consultative strategy to extend beyond the in-house staff and include perspectives from experts in industry, academia, and the non-profit sector. On occasion, foreign nationals may be required to collaborate as consultants on particular task orders. Any foreign national to be used as a consultant will require the approval of the S&T FFRDC Executive Agent, and the S&T International Affairs Division prior to work on

this contract. Foreign national consultants shall not be permitted access to FFRDC work spaces or FFRDC/DHS IT networks or systems. The Contractor will also be expected to have broad access to facilities that can provide unique capabilities for simulation and modeling in support of mission trade-off analysis and operational analysis across all homeland security mission areas, including but not limited to (classified and unclassified): information technology and management, intelligence and information sharing, borders and maritime security (sensor and data networks), chemical and biological detection and protection, transportation system and critical infrastructure protection and security, cyber security and protection, biometric identification, communications interoperability and security, and emergency planning and response. The Contractor shall operate and maintain a DHS approved IT system, at a minimum of FISMA “medium” level, on which it will maintain an intranet that is remotely accessible to S&T program manager and COTR. The Contractor may be required to maintain a classified DHS HSDN or equivalent access.

The Contractor may propose subcontracting arrangements with other corporate entities to provide or enhance proposed capabilities. To receive credit for sub-contractor capabilities, the prime will need to guarantee that particular types of tasks and required expertise and facilities will be provided by the sub-contracted partner.

The Contractor shall provide a phase-in plan that demonstrates the initial ability to begin executing technical task work upon award. The initial phase-in plan includes: an organization structure and staffing plan for phasing in technical and managerial talent in accordance with the needs of the Department demonstrated with task orders, including the use of partners, reach-back, and sub-contractors. The initial phase-in plan shall demonstrate compliance with quality assurance and organizational / staff conflict-of-interest protocols. The initial phase-in plan also includes an outreach strategy to familiarize the DHS with the SAI capabilities and goals, including the development of the first Research Plan. The initial phase-in plan includes the task order processing procedures, security planning and implementation, IT system(s) accreditation, and test facility planning and operations. The overall management planning for the SAI shall demonstrate the capacity to rapidly build the organization and infrastructure to support up to 200 STE.

The Contractor will be subject to independent audits by a Government accounting agency, the DHS Inspector General, and/or the Government Accountability Office (GAO). The Contractor shall be responsible for hiring a certified public accounting firm to conduct: (1) annual financial audits of the operations of the HSSAI FFRDC (and certify annual financial statements), and (2) all audits required by law or applicable regulation.

C.5 Research Plan

To conduct its mission of providing analytic support to its DHS sponsors in an efficient, effective and responsive manner, the HSSAI FFRDC will develop and operate an annual Research Plan. The HSSAI FFRDC shall develop an annual Research Plan based on a clear understanding of the Government’s requirements as determined by direction from the Under Secretary for Science and Technology (DHS HSSAI FFRDC program office) and DHS Headquarters Components or their designees. Input and review of the plan shall occur primarily through the Homeland Security SAI Advisory Group, chaired by the DHS (SAI) Executive Agent and made up of senior leadership from throughout the Department appointed by the Executive Agent.

The annual Research Plan will be approved by the DHS Executive Agent (SAI program office) and submitted annually to the Contracting Officer for approval. It will be viewed as a flexible and dynamic document that will be periodically reviewed with the DHS HSSAI FFRDC Advisory Group and revised as necessary to meet the DHS sponsors' needs. The Research Plan will include at least two parts: (1) Core projects and (2) Task Orders. The DHS HSSAI FFRDC program office will direct/approve the allocation of contract resources within the Core projects and any changes to these elements will require prior written approval by the HSSAI FFRDC Executive Agent / Program Manager. Core projects will typically be reviewed with the SAI Advisory Group on a semi-annual basis. In no case will the SAI initiate and perform work that is not previously approved by the DHS HSSAI FFRDC CO. Task orders will be coordinated with the SAI program office and the sponsoring program office. All work shall commence with the approval of the CO. Changes to the task orders may not be made without a modification to the TO and must be approved by the CO prior to commencement of work. Any changes to core project or task order deliverables, delivery dates, periods of performance, or scope may occur only with the direction and approval of the CO.

The CO will authorize funding for the SAI based on the annual Research Plan approved by the DHS Executive Agent. The annual core project budget may be adjusted with additional funding in future years to meet the needs of the DHS sponsors. The annual research plan shall be based on the calendar year rather than the fiscal year.

The HSSAI FFRDC shall perform the work as stated in the approved Research Plan, but in no event is it authorized to incur costs in excess of the authorized costs included in any/all approved Task Orders issued hereunder, or in other initiation of funds procedures set forth in the Research Plan, without the written approval of the CO.

The Research Plan shall be primarily funded through DHS S&T core funding, which may be supplemented by an allocation of 5% of each task order that is issued. The allocations, if authorized by the DHS HSSAI FFRDC program office, shall be administered by the SAI as a sub-task of each task order and shall report technical progress as a part of the core Research Plan progress reports. If implemented, the SAI shall use the 5% allocation for the benefit of all task orders by using the funding for establishing procedures to: quickly initiate new tasks or new task direction; provide critical quick-response analysis, develop strategic mission concept evolution capabilities, and track and document lessons learned and best practices. These tasks will be referred to as core projects of the research plan, because they will have benefits across the Department and the entire homeland security enterprise, although they are developed within specific task orders. The Research Plan core allocation includes:

- Addressing the most critical and strategic issues of the homeland security enterprise
- Providing best practices that efficiently and effectively promote the identification of operational performance baselines and desired and acceptable performance and effectiveness metrics prioritized to national goals
- Effectively balancing an interdisciplinary staff across areas of strategic assessments, strategic planning, operation analysis, operational test and evaluation, and other required functions
- Consulting with representatives from other DHS FFRDCs, private industry, institutions of higher education, and nonprofit institutions; and
- Exercising sound financial control over the HSSAI FFRDC's resources.

C.6 Contractor Quality Control (QC)

The Contractor shall establish as an independent function a quality program that encompasses all aspects of the contract, including Task Orders issued hereunder. The Contractor shall ensure the Government's interests are protected through this clearly separate entity that is independent of site management as concerns the FFRDC QC Program. The QC Manager shall have sufficient, well-defined responsibility, authority, and the organizational freedom to identify and evaluate quality problems and to initiate, recommend, and provide solutions. Personnel performing management functions shall have distinct, well-defined duties and responsibilities within the quality program. The Contractor shall implement the quality program in accordance with the Contractor's Quality Control Plan. The Plan shall be provided with the Contractor's initial proposal. The Contractor's inspection instructions shall be documented and shall be available for review, on-line, by the S&T PM and COTR or CO, throughout the life of the contract. A Contractor QC Plan may be prepared for each Task Order and a copy shall be provided to the COTR (See Section F Deliverable Requirements).

C.7 Task Order (TO) Projects

Task Order (TO) projects are specific, time limited, deliverable-oriented projects. They shall contain, at a minimum, the following information based on a task Statement of Objectives provided by the Government:

- Subject and description of objectives including deliverables, milestones and their associated delivery dates;
- Discussion of the major program issues to be addressed;
- Special experimental or development test equipment and facilities required;
- Recommended approach for performing the work;
- Estimate of the total level of effort (STE equal to 1810 hours) by labor category and dollars required to perform the task;
- Estimated period of performance, including start and end dates;
- Reporting requirements and other relevant information as applicable; and
- Funding.

C.8 Contractor Employees

1. The Contractor shall not employ, or continue employment, of persons for work on this contract if such employee is identified to the Contractor by the CO as a potential threat to the health, safety, security, general well being, or operational mission of the installation or its population. The Contractor will develop policies and procedures to discourage "walk off" (e.g., task engineers/analysts resign prior to task completion) of employees and shall implement a method for replacement that will ensure performance standards continue to be met.

2. The Contractor shall ensure that none of its employees involved in the performance of any specific task have financial or other interests that could affect those employees' objective and effective performance of the task.

C.9 Contract Security Classification Specification

To qualify as a responsible Contractor, the Offeror shall possess a facility clearance and safeguarding capability equal to the highest classification stated on the Contract Security Classification Specification (DD Form 254) attached to this contract.

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the DHS S&T Security Office and the Defense Security Service (DSS) through the COTR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

C.10 Environmental Protection

The Contractor shall comply with all applicable Federal, State, and local environmental protection laws, and all stated regulations and standards, including applicable Executive Orders.

(End of Section C)

SECTION D - PACKAGING AND MARKING

D.1 Markings

All deliverables submitted to the SAI CO, the SAI PM, the TO CO or the TO COTR shall be accompanied by a packing list or other suitable shipping documentation that shall clearly indicate the following:

- (a) Contract number;
- (b) Task order number;
- (c) Name and address of point of contact

Specific or unique marking requirements may be addressed in individual TOs.

D.2 Branding

The Contractor shall comply with the requirements of any DHS Branding and Marking policies. As a matter of law, Federal criminal statutes prohibit unauthorized uses of the DHS Seal. In addition, DHS policy prohibits granting authorization for certain commercial uses of the Seal. It is permissible to reference DHS in materials if the reference is limited to true, factual statements. The words DHS and/or Homeland Security should appear in the same color, font, and size as the rest of the text in the document. Moreover, such references shall not imply in any way an endorsement of a product, company, or technology.

Requests to use the DHS Seal shall be submitted using *DHS Official Seal Usage Approval*, available from the COTR. The Comments section should be used to describe why use of the Seal is being requested and how it will be used. Completed forms should be sent via e-mail to the Director of Special Projects and Protocol for Public Affairs (TBD at time of contract) at branding@dhs.gov (phone number 202-282-8010) and to the CO.

D.3 Publications and Communications Concerning Work Performed Under This Contract

All public communication referencing the work performed under this contract shall be coordinated between the Contractor, the task sponsor, and the S&T Executive Agent and will require the approval of the S&T Executive Agent. The Contractor will route technical communication products such as reports, journal articles, presentations, and white papers and public communication products such as brochures and fliers through the Contractor's information review and release process before providing the deliverable to S&T for review and approval 30 days before any release to an external audience.

Public and technical communications shall contain the following language:

Acknowledgement

"The U.S. Department of Homeland Security (DHS) sponsored the production of this material under a Contract No.HSHQDC-09-D-0003 with Analytic Services Inc."

D.4 Dissemination of Contract Information (HSAR 3052.242-71) (DEC 2003)

The Contractor shall not publish, permit to be published, or distribute for public consumption, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this contract, without the prior written consent of the Contracting Officer. An electronic or printed copy of any material proposed to be published or distributed shall be submitted to the Contracting Officer.

(End of clause)

(End of Section D)

SECTION E - INSPECTION AND ACCEPTANCE

E.1 Clauses Incorporated by Reference (FAR 52.252-2) (Feb 1998)

This contract incorporates the following clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address: <http://www.acquisition.gov>

FAR Clause No.	Title and Date
52.246-5	Inspection of Services—Cost-Reimbursement (APR 1984)
52.246-9	Inspection of Research and Development (Short Form) (APR 1984)
52.246-16	Responsibility for Supplies (APR 1984)
52.246-20	Warranty of Services (MAY 2001)
52.246-25	Limitation of Liability-Services (FEB 1997)

E.2 Scope of Inspection

All deliverables will be inspected for content, completeness, accuracy and conformance to TO requirements by the TO COTR or as detailed in individual TOs. Inspection may include validation of information or software through the use of automated tools and/or testing of the deliverables, as specified in the TO. The scope and nature of this testing must be negotiated prior to TO issuance and will be sufficiently comprehensive to ensure the completeness, quality and adequacy of all deliverables.

The Government requires a period not to exceed thirty (30) calendar days after receipt of final deliverable items for inspection and acceptance or rejection unless otherwise specified in the TO.

E.3 Evaluation and Acceptance

The CO or authorized representative will accomplish evaluation and acceptance of services delivered under this contract. For the purpose of this clause, the COTR named in this contract is the authorized representative. The CO reserves the right to unilaterally designate a different Government agent as the authorized representative. The Contractor will be notified by a written notice or by a copy of the delegation of authority if a different representative is designated.

(End of Section E)

SECTION F - DELIVERIES OR PERFORMANCE

F.1 General

The DHS CO may include additional deliveries or performance requirements in TOs, other than those enumerated in this section, such as (1) optional FAR clauses, (2) component specific clauses, and (3) task order specific clauses.

F.2 Clauses Incorporated by Reference (FAR 52.252-2) (Feb 1998)

This contract incorporates the following clause(s) by reference with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text can be accessed electronically at this Internet address: <http://www.acquisition.gov>

FAR Clause No.	Title and Date
FAR 52.242-15	Stop-Work Order (AUG 1989) – Alternate I (APR 1984)

F.3 FFRDC Period of Performance

In accordance with FAR 35.017-1(e), the period of performance for the Contract Ordering Period (COP) will not exceed 5 years – a twelve month base year from date of award with four (4) one year option periods – but can be renewed, as a result of periodic reviews, in increments not to exceed five (5) years.

F.4 Task Order Performance Period and Pricing

TOs may be issued at any time during the COP. The performance period of each TO will be specified in the TO and may include option periods which, if exercised, may extend the TO period of performance for up to twelve (12) months beyond the COP of the base period and option periods. TOs shall be priced using Section B indirect rates that will be applicable to the TO's anticipated period of performance.

TOs issued in the final option year shall not extend beyond six (6) months after the COP of the final option year. At all times each order's terms shall be consistent with its funding appropriation.

F.5 Reporting Requirements

F.5.1 Technical and Progress Reporting Requirements

During the performance of this contract the contractor shall submit the following reports:

a. Quarterly Progress Reviews

The FFRDC management shall prepare and conduct a quarterly progress review of work accomplished during each quarter of contract performance for the DHS Executive Agent, PM and COTR. These reviews shall present a summary of all work performed, including highlights of individual tasks for the period, technical findings and accomplishments and any new issues, problems or dependencies. Reviews are expected to be no longer than four (4) hours. They shall also include a summary work plan for the upcoming reporting period and any action required on the part the Sponsors. Reviews are to be conducted within 20 working days following the end of the reporting period.

b. Technical Reports

Drafts of Technical Reports

Technical reports required by the Research Plan shall be submitted in draft form to the Sponsors for review and comment. Any comment that may be made shall not be implemented by the Contractor without the prior written approval of the CO if:

- It results in a change to the terms and/or conditions of the contract; or
- It constitutes an assignment of work outside the general scope of the contract.

Final Technical Reports

HSSAI FFRDC shall provide all deliverables (including point papers, white papers, briefings, presentations, background studies and interim reports) directly to the DHS Task Sponsor (two (2) hard copies and one (1) electronic copy on CD unless otherwise specified in the SOO or PWS), DHS Program Manager (three (3) hard copies and two (2) electronic copies on CDs) with a copy of the transmittal letter to the CO. Unless otherwise specified in this SOO, an electronic draft of major deliverables shall be provided 28 calendar days prior to the due date for a 10 calendar day review and comment period by the Government. This will allow for additional coordination suggestions, expanded points-of-contact to be identified, and a robust inclusion of comments from subject matter experts within the Federal Government. Major deliverables are final reports and major presentations, as opposed to briefs, memos, whitepapers and program plans that may be reviewed by the sponsor using a less formal process. The final deliverables shall be printed and bound and shall include an electronic version provided in Microsoft Office format or other format(s) pre-approved by the task sponsor and DHS program office. The Contractor shall maintain up-to-date records of all work results, developments, accomplishments, computations, etc. for the preparation of the report. All reports shall generally include, but not be limited to, a detailed description of:

- (1) Detailed findings and analysis of alternatives;
- (2) Mission and operational concept evolutions, including supporting analysis and simulation and modeling data;
- (3) Analysis of operational test and evaluation procedures and results, including all negative results obtained, if applicable;
- (4) All new and revised processes, techniques, and procedures for integration of best practices developed under this contract;
- (5) Independent and objective development and assessments of DHS and National risk models for the allocation of resources;

- (6) Sketches and schematics as necessary to clarify and amplify; and
- (7) Recommendations and/or conclusions.

The Contractor will not publish and/or publicly disseminate any technical report, publication or any documentation resultant from tasks performed under this contract without the prior written consent of the Task Sponsor and the DHS S&T SAI Executive Agent. All requests for release shall be in writing and submitted to the DHS S&T PM with a copy to the COTR.

c. Monthly Financial Reporting

The Contractor shall prepare and include on a monthly basis (with the Task and FFRDC Monthly Report) a report that details expenditures by tasks of the Research Plan to include Core and other analysis and development tasks. The content of the reports shall, at minimum, contain the following reporting categories and levels and in accordance with Attachment J-2, Monthly Contractor Financial Report:

- Labor
- Travel/Commuting
- Subcontract Effort
- Direct Cost and Other Direct Costs (item description and cost)
- Indirect Costs/Fringe Benefits
- Fee

Financial reports shall be distributed to the CO and COTR as prescribed in each task order.

d. Annual Labor Report

The Contractor shall submit an annual fiscal year report of all employees to the CO and COTR by 1 November of each year. The data shall also be provided on the annual STE based on 1810 hours per STE including consultants and sub-contractors for the previous fiscal year.

e. Quality Control Matrices/Progress Reports

- a. The Quality Control (QC) Plan and inspection system shall satisfy the requirements in the Inspection Clauses and the Deliverables Summary of the Contract. It shall be designed to keep the Contractor's management informed of all issues affecting quality. The QC records of inspections shall indicate the nature of the deficiencies found and the corrective action taken as appropriate. Records will be available to the DHS S&T PM and COTR on-line, via remote access to the FFRDC's intranet site, and shall be maintained during the contract life.
- b. The Contractor shall make available to the CO and COTR, for each monthly period during the life of this contract, a copy of QC matrices for deliverable and performance items. Metrics must verify whether the performance requirements of the contract have been met. The Contractor must also provide required technical reports describing progress of the program, note all technical areas in which effort is being directed and indicate the status of work within these areas. The data may be included in the monthly progress reports and shall be available to the CO and the DHS S&T PM / COTR on-line, via remote access to the FFRDC's intranet site. Data shall include at a minimum:

- (1) A quantitative description of overall progress and applicable supporting data, as necessary, and in sufficient detail to comprehensively explain progress to date;
 - (2) An indication of any current problems that may impede performance and proposed corrective action; and
 - (3) Discussion of the work to be performed during the next reporting period.
- c. The reports shall be delivered not later than the dates set forth in the Deliverables Provision of the contract.

F.5.2 Task and FFRDC Monthly Status Report

The Contractor will deliver a task status report for the previous month to the Task Sponsor by ***the 15th of the month***. The report shall contain accomplishments, upcoming events, risks encountered and mitigation measures taken, and financial information (amount budgeted, amount received, amount in reserve, amount committed, amount obligated, amount expended, and available balance). The reports will be made available to the S&T COTR and PM via on-line access to the FFRDC's intranet site. The report will also contain the following metrics:

- Task Identifier and Accounting Data
- SAI Task Lead and Principal Task Sponsor
- Task start and end dates
- Deliverables and milestones with dates
- Reporting Period
- Stop-light indicator of status of technical performance, schedule and cost
- Technical Summary of monthly progress
- Technical and Financial Issues and proposed resolution(s)
- Quality Control findings and actions
- Graph indicating original, revised, actual and projected spending curves

The overall monthly FFRDC summary report shall be provided to the S&T Executive Agent, S&T PM and S&T COTR that includes all task status reports and a Director's report. The Director's report shall include a financial summary of all tasks (table listing the task identifier, task name, previous month's claims, total claimed, total budget, and available funds remaining), significant progress in achieving FFRDC mission objectives including significant milestones and meetings, a summary of the FFRDC industrial and IT security programs including status of personnel obtaining suitability and access / clearances, and a summary FFRDC personnel by labor category and discussion of staff changes for the previous month. In addition, the Contractor shall provide a discussion of the following:

- Task Plans for newly approved Tasks and Development efforts that update the Research Plan
- A description of newly initiated Core Support Efforts such as quick response special projects
- A summary of the resource allocation needed to accommodate such updates to the Research Plan

F.5.3 Verbal Reports and Liaison

The HSSAI FFRDC will meet with the DHS sponsors on an "as required" basis, to review work to date on the research program and to exchange views, ideas, and information concerning the methods and content of the work.

F.6 Place of Performance

The Contractor shall provide the necessary space, classified and unclassified, IT network and other equipment, and support and technical personnel to establish, set up and manage the HSSAI FFRDC. Contractor management and at least 50% of the full time staff are to be located in the Washington, DC metropolitan area. A substantial effort is expected to be deployed on-site at DHS headquarters offices. Other staff may be assigned to field offices, including Contractor activities, to provide independent analysis of operations. The Contractor will provide, at their Washington, D.C. area SAI headquarters, a room furnished with two desks, phones and computers for the DHS HSSAI FFRDC program officials or other visiting DHS officials. The Contractor shall also provide and maintain a list of accessible operational test and evaluation facilities, along with their address, capabilities, and ownership.

F.7 Notice to the Government of Delays

In the event the Contractor encounters difficulty in meeting performance requirements, or when the Contractor anticipates difficulty in complying with the contract delivery schedule or completion date, or whenever the Contractor has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this contract, the Contractor shall immediately notify the CO and the TO COTR, in writing, giving pertinent details. However, this data shall be informational only in character, and this provision shall not be construed as a waiver by the Government of any delivery schedule or date or any rights or remedies provided by law or under this contract.

F.8 DHS-Furnished Information

- a. DHS will provide unique information, materials, and forms to the Contractor to support tasks under this SOO. Such DHS-provided information, materials, and forms shall remain the property of DHS, unless otherwise indicated in writing by DHS, and may not be distributed beyond the Contractor's project performers without DHS's prior written permission.
- b. The S&T COTR identified in this SOO will be the point of contact (POC) for identifying required information to be supplied by DHS.
- c. DHS will provide guidelines to the Contractor to use in preparing any documentation (e.g., report deliverables or monthly status reports).

F.9 DHS-Furnished Property

Additional DHS property will not be provided to the SAI unless otherwise agreed in a task order issued under this SOO. In such cases, the SAI shall maintain property records. Before purchasing any individual item equal to or exceeding \$5,000 that is required to support technical tasks performed pursuant to this SOO, the SAI shall obtain the DHS Task Sponsor and DHS PM's prior written consent. SAI shall maintain any such items according to the contract property accountability procedures.

F.10 Deliverable Requirements

The Contractor shall provide research, analytical and computational models, simulations, and other technical and analytical support useful for program planning and management to support the DHS as specified in Task Orders issued pursuant to the paragraph in section G entitled Task Order Process and Delivery. The type of work to be performed under such Task Orders is limited to the types of work incorporated by Section C entitled Statement of Objectives. The Contractor shall perform and/or deliver the following:

<u>Item</u>	<u>Description</u>	<u>Reference</u>	<u>Delivery Schedule</u>
1	Management Plan	Section C	Updates as required
2	Research Plan	Section C	Annual (15 November)
3	Task execution proposals including quality control plans	Section G	As Required in response to Task SOOs
4	Insurance Notification	Section I	30 days after award
5	Consent for Subcontract Approval 52.244-2	Section I	As Required
6	Small Business Subcontracting Plan 52.219-9	Section I	Semi-annually
7	Organizational Conflict of Interest Disclosure Report	Section G	Quarterly
8	Small Disadvantaged Business Participation Reporting 52.219-25	Section I	Contract Completion
9	Task and FFRDC Monthly Status Report (base effort and tasks) on schedule, finance, technical progress and issues	Section F	15 days after the end of the reporting month (aligned with invoice)
10	Travel Policy	Section G	30 days after award
11	Appointment of Security Officer	Section C	At contract award
12	Task Program Management Plans	Section G	15 days (draft) and 30 days (final) after task awards and modifications
13	Annual Government Property Report	Section F	Annual
14	Quarterly Progress Review (4 hour)	Section F	Quarterly
15	Report of Security Violations	DD254	Annually
16	"Need for Fee" report	Section J Sponsoring Agreement	Annually
17	Revalidation of SCI billets	DD254	Annual

18	FFRDC Parent Corporation Work for Others	Section J Sponsoring Agreement	Quarterly
19	Maintain copies of staff, sub-contractor, consultant NDAs and COIs for five years	Section J Sponsoring Agreement	NA
20	Organizational COI & Disposition	Section J Sponsoring Agreement	NA
21	Notice of Acquisition of Real Property	Section J Sponsoring Agreement	30 days advance notice
22	Notice of Material Increase in Employee Benefits Chargeable to the Contract	Section J Sponsoring Agreement	30 days advance notice
23	IT Security Plan	Section I	45 days after contract award
24	IT Security Accreditation report	Section I	6 months after contract award

To the extent any other deliverables are required by this contract, but not specifically referenced under this part, such requirements shall be considered as included.

(End of Section F)

SECTION G - CONTRACT ADMINISTRATION DATA

G.1 Accounting and Appropriation Data

Accounting and appropriation data for obligations under the contract will be set forth on individual task orders.

G.2 Points of Contact

The following subsections describe the roles and responsibility of individuals who will be the primary points of contact for the Government on matters regarding contract administration as well as other administrative information. The Government reserves the right to unilaterally change any of these individual assignments.

SAI Program Manager:

Name: Patrick Spahn
Address: Department of Homeland Security
Science and Technology Directorate
Operations Analysis Division
245 Murray Drive, Bldg 410
Washington, DC 20528
Email: patrick.spahn@dhs.gov

SAI Contracting Officer:

Name: Sharon Flowers
Address: Department of Homeland Security
Office of Procurement Operations
245 Murray Drive, Bldg 410
Washington, DC 20528
Email: sharon.flowers@hq.dhs.gov

SAI COTR:

Name: Deborah Russell
Address: Department of Homeland Security
Science and Technology Directorate
Operations Analysis Division
245 Murray Drive, Bldg 410
Washington, DC 20528
Email: deborah.russell@dhs.gov

Task Order Manager:

To be identified in each order

Written communications pertinent to SAI FFRDC program and/or any resulting TOs shall make reference to the TO Number and shall be mailed to the attention of the SAI PM, the COTR, and the CO at the above address.

G.2.1 Contracting Officer's Authority

The CO assigned to this contract has responsibility for ensuring the performance of all necessary actions for effective contracting, ensuring compliance with the terms of the contract and safeguarding the interests of the United States in its contractual relationships. The CO is the only individual who has the authority to enter into, administer, or terminate this contract and is the only person authorized to approve changes to any of the requirements under this contract, and notwithstanding any provision contained elsewhere in this contract, this authority remains solely with the CO.

It is the Contractor's responsibility to contact the CO immediately if there is even the appearance of any technical direction that is or may be outside the scope of the contract. The Government will not reimburse the Contractor for any work not authorized by the CO, including work outside the scope of the contract.

G.2.2 Contracting Officer's Technical Representative (HSAR 3052.242-72) (DEC 2003)

- (a) The CO may designate Government personnel to act as the COTR to perform functions under the contract such as review or inspection and acceptance of supplies, services, including construction, and other functions of a technical nature. The CO will provide a written notice of such designation to the Contractor within five (5) working days after contract award or for construction, not less than five (5) working days prior to giving the Contractor the notice to proceed. The designation letter will set forth the authorities and limitations of the COTR under the contract.
- (b) The CO cannot authorize the COTR or any other representative to sign documents, such as contracts, contract modifications, etc., that require the signature of the Contracting Officer.

G.2.3 Task Order Manager

Technical advice under the resulting TOs may be given to the Contractor by the Task Order Manager. Advice may also be received in coordination with the Task Order Manager by the COTR, DHS HSSAI FFRDC Program Manager, and DHS HSSAI FFRDC Executive Agent. Technical advice is defined as that process by which the Contractor receives instruction or contract clarification as it relates to an element of work solely within the existing requirements of the SOO. **The CO is the only individual who can authorize any changes to the terms and conditions of the TO in writing.** Costs incurred as the result of changes made to the terms and conditions without the CO's written approval may not be considered an allowable cost.

G.3 Task Order Process and Delivery

- (a) Only the CO may issue TOs to the Contractor including non-sponsors, providing specific authorization to perform work within the scope of the contract and as specified in the schedule. The Contractor may incur costs under this contract in performance of TOs and TO modifications issued in accordance with this clause. No other costs are authorized unless otherwise specified in the contract or expressly authorized by the CO.

(b) Prior to the CO issuing a TO, the DHS S&T PM will review the FFRDC Certification, the SOO, and the IGCE to make a suitability and appropriateness determination consistent with the FAR and DHS MD 143-4. This review will evaluate whether the proposed task objectives are consistent with the core capabilities of the FFRDC and whether or not the proposed objectives are more appropriate for competition in the domestic private sector.

(c) The CO has the right to issue tasks unilaterally and with no consultation with the Contractor. When tasks are issued unilaterally, the Contractor shall initiate performance and supply its proposal to the CO for evaluation unless the CO provides other instructions. The process described in paragraphs (c), (d), and (e) will apply absent the unilateral issuance of a task. Prior to issuing a TO, the CO will provide the Contractor with the following data:

- (1) A functional description of the work identifying the objectives or results desired from the contemplated TO;
- (2) Proposed performance standards to be used as criteria for determining whether the work requirements have been met; and
- (3) A request for a task plan from the Contractor to include the technical approach, period of performance, appropriate cost information, and any other information required to determine the reasonableness of the Contractor's proposal.

(d) Within three (3) calendar days, or a time specified that will accommodate the critical nature of the order, after receipt of the CO's request, the Contractor shall submit a task plan conforming to the request.

(e) After review and any necessary discussions, the CO may issue a task order to the Contractor containing, as a minimum, the following:

- (1) Date of the order.
- (2) Contract number and order number.
- (3) Functional description of the work identifying the objectives or results desired from the TO, including special instructions or other information necessary for performance of the task.
- (4) Performance standards, and where appropriate, quality assurance standards.
- (5) Maximum dollar amount authorized (cost and fee).
- (6) Any other resources (travel, materials, equipment, facilities, etc.) authorized.
- (7) Delivery/performance schedule, including start and end dates.
- (8) Accounting and appropriation data.

(f) The Contractor shall provide acknowledgment of receipt to the CO within one (1) calendar day after receipt of the TO.

(g) If time constraints do not permit issuance of a fully defined TO in accordance with the procedures described in paragraphs (a) through (d), a TO that includes a ceiling price may be issued. The TO shall be definitive at the earliest possible date.

(h) In the event of a conflict between the requirements of the TO and the Contractor's approved task plan, the TO shall prevail.

(i) If agreement cannot be reached on a Task Plan, the CO may unilaterally direct the Contractor to begin work on the TO in accordance with the Task Plan issued by the

Government. Failure to agree will constitute a dispute under the Disputes clause, FAR 52.233-1.

(j) Modification of Task Orders

The Ceiling Price or scope for each TO may not be changed except when authorized by a CO's modification to the TO.

No oral statement by any person and no written statement by anyone other than the CO or his/her authorized representative acting within the scope of his/her authority shall be interpreted as modifying or otherwise affecting the terms of this TO contract. All requests for interpretation or modification shall be made in writing to the CO.

(k) Procedures:

(1) Prior to issuance of a TO and upon definition of the Government requirement, the DHS S&T SAI PM will electronically issue to the Contractor a Statement of Objectives (SOO) or Performance Work Statement (PWS) that will designate a preferred TO type.

(2) After receipt of the SOO or PWS, the Contractor shall submit to the DHS S&T PM an electronic copy proposal (or Task Execution Plan (TEP)) that sets forth the Contractor's understanding of the requirements and objectives, desired impact, general approach, DHS sponsor and stakeholders, SAI Task Lead, assumptions and caveats, required Government furnished information or equipment, performance schedule and cost, staffing plan, milestones and deliverables, task security, and level of effort required. The technical proposal/TEP should also address other documentation required by the Government to perform the task or any specific issues raised in the RFP. The TEP shall be submitted by a mutually agreed upon date, which will be established for each individual TO. The TEP shall also include the cost proposal that sets forth all costs associated with furnishing the required services. The Contractor's technical proposal/TEP shall be consistent with Sections B and C.

If the Contractor anticipates the need for a longer period of time than originally agreed upon (to submit the proposal), the Contractor shall provide written justification to the DHS S&T PM electronically as soon as possible after receipt of a task assignment but no later than 45 days before the current end date of the task. If the PM concurs with the extension, the PM shall submit the request to the CO for approval.

(3) Upon receipt of the Contractor's proposal, the Government will evaluate the document, and negotiations will take place between the DHS S&T PM, acting on the Task Sponsor's behalf, and the Contractor.

(4) Following the conclusion of negotiations, the DHS S&T program office shall submit the negotiated TEP, cost data, and funding data to the CO, who will make a final determination. If acceptable, the CO will issue a fully executed TO containing all agreed-to terms and conditions and specifying the task to be performed, special reporting requirements and total estimated cost and fixed fee. The Contractor shall in no event exceed the total estimated cost of the TO (see FAR 52.232-20 and 52.232-22).

Whenever it appears to the Contractor that the actual cost to complete any task may exceed the estimated cost of such task, the Contractor shall immediately, and in no event later than the incurrence of 75% of the estimated task cost, notify the CO in writing

and furnish a revised estimate for the completion of the task. The Contractor shall not incur costs to perform work under any specific task in excess of the cost estimate authorized for the task until the CO notifies the Contractor in writing that such amount has been increased. Issuance of a TO is not authorization for the Contractor to incur costs in excess of the funds obligated to-date under the contract.

(5) In the event that the parties fail to agree on price, costs and/or fixed fee for any TO hereunder, the CO may render a unilateral written decision as to what level of price or costs and/or fee is reasonable under the circumstances for the services required pursuant to the TO and will subsequently unilaterally issue the TO in accordance with that decision. Said decision shall constitute a decision rendered concerning a question of fact within the meaning of and governed by the terms of FAR Clause 52.233-1 in Section I of this contract.

(6) Each TO shall be invoiced separately. Invoices shall include the following information: Task Title, Task Number, Budget (Planned), and must reference the appropriate section of the technical progress report. Incremental and/or optional follow on funding utilizing the same TO number must be identified separately on a TO break out sheet for invoicing purposes.

(7) SAI shall implement and manage the technical approach, organizational resources, and management controls to be employed to meet the cost, performance and schedule requirements throughout task order execution. A draft project management plan shall be submitted 15 days after a task order is received, with a final submittal reflecting Government input due 30 days after the TO is received. The project management plan shall provide a detailed schedule, including a critical path analysis, along with a narrative discussing the salient issues affecting task execution in terms of needed technical inputs and analysis to meet cost, schedule, and performance in the task execution.

G.4 Preparation of Payment Vouchers

(a) SF-1034, Public Voucher for Purchases and Services Other Than Personal, shall be prepared and submitted for payments under this contract, unless otherwise specified in the individual TO.

(1) Copy to the Finance Office:
DHS ICE
Burlington Finance Center
PO Box 1000
Williston, Vermont 05495-1000
Attn: S&T Division Research & Labs
SAT.Invoice.Consolidation@dhs.gov

(2) Copy to the TO COTR
(2) Copy to the CO

(b) All vouchers submitted to the Government shall delineate cost by:

(1) Contract and TO Number;

- (2) Funding document, including amount received, order billing item or contract line item number; and
- (3) Any additional information required by specific payment clauses.

G.5 Payment Information

Payments of invoices and vouchers shall be subject to the withholding provisions of this contract.

Payments under the contract will be made by wire transfer through the Treasury Financial Communications System. The bank account information required is as follows:

Wachovia National Bank
1970 Chain Bridge Road
McLean, VA 22102
American Bankers Association (ABA) identifier: 056007604

G.6 Travel

Travel must be pre-approved by the S&T COTR, usually through the Task Execution Plan proposal, and the Contractor will provide trip reports to the S&T COTR and task sponsor. Local travel will not be reimbursed. Other travel will be reimbursed in accordance with the *Federal Travel Regulation*. The S&T COTR may delegate travel approval to the sponsoring program offices, as required.

G.6.1 Travel Outside of the United States

- (a) Approval of Foreign Travel: The cost of foreign travel is allowable only when the specific written approval of the CO responsible for administration of the contract is obtained prior to commencing the trip. Approval must be requested at least 30 days before the scheduled departure date in order that all necessary clearances may be processed. Each individual trip must be approved separately even though it may have been included in a previously approved budget. Foreign travel is defined as any travel outside of the United States and its territories and possessions.
- (b) Travel shall take place in accordance with the Federal Travel Regulations (FTR) and will be considered reasonable and allowable to the extent permitted by FAR 31.205-46. Documentation will be available upon request to Defense Contract Audit Agency (DCAA).
- (c) The S&T Director, International Programs Division must approve all foreign travel in advance. The Contractor will notify the S&T COTR 45 days in advance to coordinate this approval. The Contractor must notify the S&T Director, International Programs Division 30 days (for unclassified visits) or 45 days (for classified visits) before arrival of visitors from foreign countries.

(End of Section G)

SECTION H – SPECIAL CONTRACTING REQUIREMENTS

H.1 Standard of Conduct at Government Installations

The Contractor shall be responsible for maintaining satisfactory standards of employee competency, conduct, appearance and integrity and shall be responsible for taking such disciplinary action with respect to employees as may be necessary. The Contractor is also responsible for ensuring that his employees do not disturb papers on desks, open desk drawers or cabinets, or use Government resources except as authorized by the Government.

H.2 Advertisements, Publicizing Awards and News Releases

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity news release or commercial advertising without first obtaining explicit written consent to do so from the SAI Program Manager and COTR. This restriction does not apply to marketing materials developed for presentation to potential Government customers of this contract vehicle.

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

H.3 Observance of Legal Holidays and Excused Absence

(a) The Government hereby provides notification that Government personnel observe the listed days as holidays: These holidays apply only to services performed within the United States, and the list is provided for informational purposes only.

- | | |
|-----------------------------------|----------------------|
| (1) New Year's Day | (6) Labor Day |
| (2) Martin Luther King's Birthday | (7) Columbus Day |
| (3) President's Day | (8) Veterans' Day |
| (4) Memorial Day | (9) Thanksgiving Day |
| (5) Independence Day | (10) Christmas Day |

(b) In addition to the days designated as holidays, the Government observes the following days:

- (1) Any other day designated by Federal Statute
- (2) Any other day designated by Executive Order
- (3) Any other day designated by the President's Proclamation

(c) It is understood and agreed between the Government and the Contractor that observance of such days by Government personnel shall not otherwise be a reason for an additional period of performance, or entitlement of compensation except as set forth within the contract. This provision does not preclude reimbursement for authorized overtime work if applicable to this contract.

(d) When the Federal and governmental entities grant excused absence to its employees, assigned Contractor personnel may also be dismissed. The Contractor agrees to continue to provide sufficient personnel to perform critical tasks already in operation or scheduled, and shall be guided by the instructions issued by the CO or the TO COTR.

(e) If Government personnel are furloughed, the Contractor shall contact the CO or the TO COTR to receive direction. It is the Government's decision as to whether the contract price will be affected. Generally, the following situations apply:

(1) Contractor personnel that are able to continue contract performance (either on-site or at a site other than their normal work station) shall continue to work and the contract price shall not be reduced or increased.

(2) Contractor personnel that are not able to continue contract performance (e.g., support functions) may be asked to cease their work effort.

(f) In those situations that furloughed Government personnel are reimbursed, the Contractor may not invoice for their employees working during the Government furlough until such time as the special legislation affecting Government personnel is signed into law by the President of the United States.

(g) Nothing in this clause abrogates the rights and responsibilities of the parties relating to stop work provisions as cited in other sections of this contract.

H.4 Insurance (HSAR 3052.228-70) (DEC 2003)

In accordance with the clause entitled "Insurance - Liability to Third Persons" in Section I, insurance of the following kinds and minimum amounts shall be furnished at any time at the request of the CO and maintained during the period of performance of this contract:

(a) Worker's compensation and employer's liability. The Contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(a).

(b) General liability. The Contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(b).

(c) Automobile liability. The Contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(c).

H.5 Information Technology Accessibility for Persons with Disabilities

All services and Electronic Information Technology (EIT) delivered as result of orders placed under this contract shall comply with accessibility standards in accordance with Federal Information Technology Accessibility as required by Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended. Information about the Section 508

Electronic and Information Technology Accessibility Standards may be obtained via the Web at the following URL: from www.Section508.gov.

H.6 Organizational Conflicts of Interest and Confidentiality

(a) Purpose. The purpose of this clause is to ensure that the contractor (1) is not biased because of its financial, contractual, organizational, or other interests that relate to the work under this contract, and (2) does not obtain any unfair competitive advantage over other parties by virtue of its performance of this contract.

(b) Scope. The restrictions described herein shall apply to performance or participation by the contractor and any of its affiliates or their successors in interest (hereinafter collectively referred to as “contractor”) in the activities covered by this clause as a prime contractor, subcontractor, cosponsor, joint venture, consultant, or in any similar capacity. For the purpose of this clause, affiliation occurs when a business concern is controlled by or has the power to control another or when a third party has the power to control both.

(1) Use of Contractor's Work Product. (i) The contractor shall be ineligible to participate in any capacity in Department of Homeland Security and component contracts, subcontracts, or proposals thereof (solicited and unsolicited) which stem directly from the contractor's performance of work under this contract for a period of two years after the completion of this contract. Furthermore, unless so directed in writing by the contracting officer, the Contractor shall not perform any systems engineering or development work under this contract on any of its products or services or the products or services of another firm if the contractor is or has been substantially involved in their development or marketing. Nothing in this subparagraph shall preclude the contractor from competing for a recompetition of this contract.

(ii) If, under this contract, the contractor prepares a complete or essentially complete statement of work or specifications to be used in competitive acquisitions, the contractor shall be ineligible to perform or participate in any capacity in any contractual effort which is based on such statement of work or specifications. The contractor shall not incorporate its products or services in such statement of work or specifications unless so directed in writing by the contracting officer, in which case the restriction in this subparagraph shall not apply.

(iii) Nothing in this paragraph shall preclude the contractor from offering or selling its standard and commercial items to the Government.

(2) Access to and use of information. (i) If the contractor, in the performance of this contract, obtains access to information, such as Department plans, policies, reports, studies, financial plans, internal data protected by the Privacy Act of 1974 (5 U.S.C. 552a), or data which has not been released or otherwise made available to the public, the contractor agrees that without prior written approval of the contracting officer it shall not:

(A) use such information for any private purpose unless the information has been released or otherwise made available to the public;

(B) compete for work for the Department based on such information for a period of six (6) months after either the completion of this contract or until such information is released or otherwise made available to the public, whichever is first;

(C) submit an unsolicited proposal to the Government which is based on such information until one year after such information is released or otherwise made available to the public; and

(D) release such information unless such information has previously been released or otherwise made available to the public by the Department.

(ii) In addition, the contractor agrees that to the extent it receives or is given access to proprietary data, data protected by the Privacy Act of 1974 (5 U.S.C. 552a), or other confidential or privileged technical, business, or financial information of third parties under this contract, it shall treat such information in accordance with any restrictions imposed on such information.

(c) Disclosure after award. (1) The contractor agrees that, if changes, including additions, to the facts disclosed by it prior to award of this contract, occur during the performance of this contract, it shall make an immediate and full disclosure of such changes in writing to the contracting officer.

(2) In addition, the Contractor shall provide the CO any disclosure of interests of itself or its affiliates that creates a real or potential organizational conflicts related to the performance of individual TOs.

(3) The disclosure may include a description of any action which the contractor has taken or proposes to take to avoid, neutralize, or mitigate any resulting conflict of interest. The Department may, however, terminate the contract or individual TO for convenience if it deems such termination to be in the best interest of the Government.

(4) In the event that the Contractor was aware of facts required to be disclosed or the existence of an actual or potential organizational conflict of interest and did not disclose such facts or such conflict of interest to the contracting officer, DHS may terminate this contract for default.

(d) Remedies. For breach of any of the above restrictions or for nondisclosure or misrepresentation of any facts required to be disclosed concerning this contract, including the existence of an actual or potential organizational conflict of interest at the time of or after award, the Government may terminate the contract for default, disqualify the contractor from subsequent related contractual efforts, and pursue such other remedies as may be permitted by law or this contract.

(e) Waiver. Requests for waiver under this clause shall be directed in writing to the contracting officer and shall include a full description of the requested waiver and the reasons in support thereof. If it is determined to be in the best interests of the Government, the CO may grant such a waiver in writing.

(f) Subcontracts. (1) The Contractor shall include a clause, substantially similar to this clause, including this paragraph (f), in subcontracts expected to exceed the simplified

acquisition threshold determined in accordance with FAR part 13 and involving the performance of advisory and assistance services as that term is defined at FAR 37.201. The terms “contract,” “contractor,” and “contracting officer” shall be appropriately modified to preserve the Government's rights.

(2) Prior to the award under this contract of any such subcontracts for advisory and assistance services, in fulfilling its obligations under this contract, the Contractor shall obtain from the proposed subcontractor or consultant the disclosure of facts relevant to the performance of the proposed subcontract and shall determine in writing whether the interests disclosed present an actual or significant potential for an organizational conflict of interest. Where an actual or significant potential organizational conflict of interest is identified, the contractor shall take actions to avoid, neutralize, or mitigate the organizational conflict to the satisfaction of the Contractor. If the conflict cannot be avoided or neutralized, the Contractor must obtain the approval of the DHS CO prior to entering into the subcontract.”

H.7 Tasks Performed for Federal Agencies Other Than the Sponsors

Projects performed by the contractor for Federal agencies other than the Sponsors shall be in strict accordance with this contract, DHS Management Directive 143-04 and will be processed in compliance with the Sponsoring Agreement. The work performed for others shall be included with any STE count limitation established in this contract.

H.8 Consultants

Prior to retention of any consultant(s) and sub-contractors, other than those, which may be included in the Offeror's proposal, for the work under this contract, the Contractor shall obtain advance written approval from the CO. Payments for the services of consultants shall not exceed the current maximum daily equivalent rate paid to a Level IV Executive Employee per day (exclusive of indirect cost, travel, per diem, clerical services, vacation, fringe benefits, and supplies) without the prior written approval of the CO. Total payments shall not exceed a total of ten (10) days per consultant during any one twelve month period without the prior written approval of the CO.

Requests by the Contractor for authorization to use consultants and sub-contractors shall contain the following information:

- 1 A biographical sketch including education and professional experience of the consultant;
- 2 The services the consultant will perform and the amount of time that will be spent;
- 3 Previous rates paid to the consultant by the Contractor for similar services for a like period;
- 4 Available information on rates charged by the consultant for similar services for a like period.

H.9 Investigating and Reporting Possible Scientific Misconduct

- a. "Misconduct" or "Misconduct in Science" is defined as fabrication, falsification, plagiarism, or other practices that seriously deviate from those that are commonly

- accepted within the scientific community for proposing, conducting or reporting research. It does not include honest error or honest differences in interpretations or judgments of data.
- b. Contractors shall foster a research environment that prevents misconduct in all research and that deals forthrightly with possible misconduct associated with research for which DHS funds have been provided or requested.
 - c. The Contractor agrees to:
 - (1) Establish and keep current an administrative process to review, investigate, and report allegations of misconduct in science in connection with research conducted by the contractor;
 - (2) Comply with its own administrative process;
 - (3) Inform its scientific and administrative staff of the policies and procedures and the importance of compliance with those policies and procedures;
 - (4) Take immediate and appropriate action as soon as misconduct on the part of employees or persons within the organization's control is suspected or alleged; and
 - (5) Report to the CO a decision to initiate an investigation into possible scientific misconduct.
 - d. The Contractor is responsible for notifying the CO of appropriate action taken if at any stage of an inquiry or investigation any of the following conditions exist:
 - (1) An immediate health hazard is involved;
 - (2) There is an immediate need to protect Federal funds or equipment;
 - (3) A probability exists that the alleged incident will be reported publicly; or
 - (4) There is a reasonable indication of possible criminal violation.

H.10 Security Requirements

As further described in Homeland Security Acquisition Regulation (HSAR) 3052.204-71, Contractor staff requiring recurring access to Government facilities, Contractor facilities operated on behalf of the Government, sensitive government information, or IT resources are required to have a favorably adjudicated Suitability background investigation prior to commencing work at the HSSAI FFRDC.

Work under this contract can be classified at *up to Top Secret, SCI*. S&T will provide specific security compliance guidance via DD Form 254. The Contractor will also adhere to the requirements in the *National Industrial Security Program Operations Manual (NISPOM)*.

The work to be performed under this contract will involve access to, handling of, and generation of classified information up to and including Top Secret (SCI). The Contractor shall appoint a Security Officer at contract award, who shall (i) be responsible for all security aspects of the work performed under this contract, (ii) ensure compliance with all Security Regulations of the US Government that apply to the DHS, and (iii) ensure compliance with any written instructions from the CO or Security Officers of DHS.

H.10.1 Top Secret, Sensitive Compartmented Information, (SCI) Personnel and Facility Clearance Requirement

The Contractor shall possess a facility clearance and safeguarding capability equal to the highest classification stated on the Contract Security Classification Specification (DD Form 254) attached to this contract and in accordance with Section H of this contract.

The Contractor shall:

- (a) Have appropriate number of key personnel having access to Sensitive Compartmented Information (SCI) that will be available for assignment to this effort immediately upon contract award. The Contractor identified in its technical proposal those cleared or clearable personnel by name and Social Security Account number that will be assigned to the program upon award.
- (b) Have an SCI certified vault facility or the ability to obtain access to such a shielded enclosure in the Washington, D.C. metropolitan area with the capability to support the anticipated work load as defined in the Contractor's proposal.
- (c) Have an SCI accredited and approved Automatic Data Processing System to run SCI information. The Contractor identified in its technical proposal the location and type of SCI accredited system that will be available to the program upon contract award.

H.10.2 General Security Requirements

The DHS has determined that performance of this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), have access to classified National Security Information (herein known as classified information). Classified information is Government information which requires protection in accordance with Executive Order 12958 as amended, Classified National Security Information, and supplementing directives.

Under provisions of U.S. Law, Title 18, U.S. Code section 499 and 701, the Contractor will abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the National Industrial Security Program Operating Manual (NISPOM) for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service (DSS). If the Contractor has access to classified information at a DHS or other Government Facility, it will abide by the requirements set by the agency.

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

Under provisions of U.S. Law, Title 18, U.S. Code section 499 and 701, the Contractor will return any expired DHS issued identification cards and building passes, Government owned property or those of terminated employees to the COTR. If an identification card or building pass is not available to be returned, a report must be submitted to the COTR, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card.

H.10.3 Employment Eligibility

The Contractor shall verify the employment eligibility of all employees and any consultants performing work under this contract using the E-Verify system within 33 calendar days of contract award and, for employees hired after contract award, within 3 business days. For E-Verify registration, see <https://www.vis-dhs.com/EmployerRegistration>.

The contractor shall include this clause in any subcontract exceeding \$2500.

H.10.4 Security Management

The COTR, DSS, and the DHS S&T Security Office shall have the right to inspect the procedures, methods, and facilities utilized by the Contractor in complying with the security requirements under this contract. Should the COTR determine that the Contractor is not complying with the security requirements of this contract, the Contractor will be informed in writing by the CO of the proper action to be taken in order to effect compliance with such requirements.

H.10.5 Information Technology Security Clearance

When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably Suitability adjudicated background investigations commensurate with the defined sensitivity level.

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

H.10.6 Information Technology Security Training and Oversight

All Contractor employees using DHS automated systems or processing DHS sensitive data will be required to receive Security Awareness Training. This training will be provided by the appropriate component agency of DHS.

Contractors who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the DHS shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. DHS contractors with significant security responsibilities shall receive specialized training specific to their security responsibilities annually. The

level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access DHS information systems will be continuously evaluated while performing these duties. The Contractor should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local DSS and DHS Security Office or Information System Security Officer (ISSO).

H.11 Conflict of Interest

The Contractor shall not employ any person who is an employee or a Contractor of the United States Government, if the employment of that person would create or appear as a conflict of interest.

H.12 Reporting Waste, Fraud, Abuse and Theft

The Contractor shall notify the CO and the COTR of any instances of suspected waste, fraud, abuse, loss, or theft of Contractor or Government-furnished property by employees or subcontractors.

H.13 Interface with Participating Associate Contractors (PAC)

The Contractor shall establish and maintain working relationships with associate contractors who can impact the performance of this contract.

H.14 Freedom of Information Act (FOIA) and Privacy Act (PA)

Any FOIA or PA request received by the Contractor shall be forwarded, no later than the next workday after receipt, to the CO and COTR. The COTR will deliver the request to the appropriate unit for processing action. The Contractor shall protect the privacy of all information reported by or about contract employees and shall protect against unauthorized disclosure. The Contractor shall ensure personal privacy data is protected to prevent unauthorized disclosure and ensure proper disposal of records subject to the act.

H.15 Handling of Data

(a) In the performance of this contract, it is anticipated that the Contractor may have access to, be furnished with or use the following categories of data (which may be technical data, computer software, administrative, management information, or financial, including cost or pricing):

(1) Data of third parties which the Government has agreed to handle under protective arrangements; and

(2) Government data, the use and dissemination of which the Government intends to control.

(b) In order to protect the interests of the Government and the owners, licensors and licensees of such data, the Contractor agrees, with respect to any such third party or Government data that is either marked with a restrictive legend specifically identified in this contract or otherwise identified in writing by the CO as being subject to this clause, to:

(1) Use, disclose, and reproduce such data only to the extent necessary to perform the work required under this contract;

(2) Allow access to such data only to those of its employees that require access for their performance under this contract;

(3) Preclude access and disclosure of such data outside the Contractor's organization; and

(4) Return or dispose of such data, as the CO may direct, when the data is no longer needed for contract performance.

(c) The Contractor agrees to inform and instruct its employees of its and their obligations under this clause and to appropriately bind its employees contractually to comply with the access, use, disclosure, and reproduction provisions of this clause.

(d) In the event that data includes a legend that the Contractor deems to be ambiguous or unauthorized, the Contractor may inform the CO of such condition. Notwithstanding such a legend, as long as such legend provides an indication that a restriction on use or disclosure was intended, the Contractor shall treat such data pursuant to the requirements of this clause unless otherwise directed, in writing, by the CO.

(e) Notwithstanding the above, the Contractor shall not be restricted in use, disclosure, and reproduction of any data that:

(1) Is or becomes, generally available or public knowledge without breach of this clause by the Contractor;

(2) Is known to be, in the possession of, or is developed by the Contractor independently of any disclosure of, or without reference to, proprietary, restricted, confidential, or otherwise protectable data under this clause;

(3) Is rightfully received by the Contractor from a third party without restriction;

(4) Or is required to be produced by the Contractor pursuant to a court order or other Government action.

If the Contractor believes that any of these events or conditions that remove restrictions on the use, disclosure, and reproduction of the data apply, the Contractor shall promptly notify the CO of such belief prior to acting on such belief, and, in any event, shall give notice to the CO prior to any unrestricted use, disclosure, or reproduction of such data.

H.16 Key Personnel or Facilities (HSAR 19 3052.215-70) (DEC 2003)

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

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

The Key Personnel or Facilities under this Contract:

Phil Anderson, Director

George Thompson, Deputy Director, Plans and Programs

Robert Tuohy, Deputy Director, Operations and Architecture

(End of clause)

H.17 Strikes or Picketing Affecting Access to a DHS Facility (HSAR 3052.222-71) (DEC 2003)

If the Contracting Officer notifies the Contractor in writing that a strike or picketing: (a) is directed at the Contractor or subcontractor or any employee of either; and (b) impedes or threatens to impede access by any person to a DHS facility where the site of the work is located, the Contractor shall take all appropriate action to end such strike or picketing, including, if necessary, the filing of a charge of unfair labor practice with the National Labor Relations Board or the use of other available judicial or administrative remedies.

H.18 DCAA

DCAA will have cognizance to negotiated provisional and final indirect rates.

(End of clause)

(End of Section H)

SECTION I - CONTRACT CLAUSES

I.1 General

The Ordering Activity may include additional contract clauses in orders, other than those enumerated in this section, such as (1) option FAR clauses, (2) activity clauses, (3) unmentioned FAR alternate clauses, and (4) order specific clauses.

I.2 Clauses Incorporated By Reference (FAR 52.252-2) (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these addresses: <http://farsite.hill.af.mil>;

<http://www.dhs.gov/xlibrary/assets/opnbiz/cpo-acquisition-regulation-0606.pdf>

(End of clause)

The following FAR and HSAR clauses are incorporated by reference into this contract:

52.202-1	Definitions	Jul 2004
52.203-3	Gratuities	Apr 1984
52.203-5	Covenant Against Contingent Fees	Apr 1984
52.203-7	Anti-Kickback Procedures	Jul 1995
52.203-13	Contractor Code of Business Ethics and Conduct	Dec 2007
52.203-8	Cancellation, Rescission and Recovery of Funds for Illegal or Improper Activity	Jan 1997
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity	Jan 1997
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	Jun 2003
52.204-4	Printed or Copied Double Sided on Recycled Paper	Aug 2000
52.204-7	Central Contractor Registration	Oct 2003
52.204-9	Personal Identity Verification of contractor Personnel	Sep 2007
52.209-6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment	Jan 2005
52.215-2	Audit and Records – Negotiation	Jun 1999
52.215-8	Order of Precedence – Uniform Contract Format	Oct 1997
52.215-10	Price Reduction for Defective Cost or Pricing Data	Oct 1997
52.215-12	Subcontractor Cost or Pricing Data	Oct 1997
52.215-14	Integrity of Unit Prices	Oct 1997

52.215-15	Pension Adjustments and Asset Reversions	Oct 2004
52.215-16	Facilities Capital Cost of Money	Oct 1997
52.215-18	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other Than Pensions	Oct 1997
52.215-21	Requirements for Cost or Pricing Data or Information Other Than Cost or Pricing Data – Modifications	Oct 1997
52.216-7	Allowable Cost and Payment	Dec 2002
52.216-8	Fixed Fee	Mar 1997
52.216-15	Predetermined Indirect Cost Rates	Apr 1998
52.219-9 Alt II	Small Business Subcontracting Plan - Alternate II	Apr 2008 Oct 2001
52.222-1	Notice to the Government of Labor Disputes	Feb 1997
52.222-2	Payment for Overtime Premiums (insert value)	Jul 1990
52.222-3	Convict Labor	Jun 2003
52.221-21	Prohibition of Segregated Facilities	Feb 1999
52.222-26	Equal Opportunity	Apr 2002
52.222-35	Equal Opportunity for Disabled Veterans, Veterans of the Vietnam Era and Other Eligible Veterans	Dec 2001
52.222-36	Affirmative Action for Workers with Disabilities	Jun 1998
52.222-37	Employment Reports on Special Disabled Veterans, Veterans of the Vietnam Era and Other Eligible Veterans	Dec 2001
52.223-3 Alt I	Hazardous Material Identification and Material Safety Data – Alternate I	Jan 1997, Jul 1995 (Alt I)
52.223-6	Drug Free Workplace	May 2001
52.223-7	Notice of Radioactive Materials	Jan 1997
52.223-14	Toxic Chemical Release Reporting	Aug 2003
52.225-13	Restrictions on Certain Foreign Purchases	Mar 2005
52.226-1	Utilization of Indian Organizations and Indian-Owned Economic Enterprises	Jun 2000
52.227-1	Authorization and Consent	Dec 2007
52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement	Dec 2007
52.227-11	Patent Rights Retention by Contractor, Short Form	Dec 2007
52.227-14 Alt II Alt III Alt V	Rights in Data – General	Dec 2007
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	Dec 2007
52.227-19	Commercial Computer Software – Restricted Rights (This clause is limited to off the shelf commercial computer software)	Dec 2007
52.227-16	Additional Data Rights	Dec 2007
52.228-7	Insurance – Liability to Third Persons	Mar 1996

52.230-2	Cost Accounting Standards	Apr 1998
52.230-6	Administration of Cost Accounting Standards	Nov 1999
52.232-9	Limitation on Withholding of Payments	Apr 1984
52.232-17	Interest	Jun 1996
52.232-20	Limitation of Cost	June 2007
52.232-22	Limitation of Funds	Apr 1984
52.232-23	Assignment of Claims	Jan 1986
52.232-25	Prompt Payment	Oct 2003
52.232-33	Payment by Electronic Funds Transfer – Central Contractor Registration	Oct 2003
52.233-1	Disputes	Jul 2002
52.233-3	Protest After Award (Aug 1996) – Alternate I	Jun 1985
52.233-4	Applicable Law for Breach of Contract Claim	Oct 2004
52.237-3	Continuity of Services	Jan 1991
52.242-1	Notice of Intent to Disallow Costs	Apr 1984
52.242-3	Penalties for Unallowable Costs	May 2001
52.242-4	Certification of Final Indirect Costs	Jan 1997
52.242-13	Bankruptcy	Jul 1995
52.243-2	Changes – Cost Reimbursement (Aug 1987) – Alternate V	Apr 1984
52.243-6	Change Order Accounting	Apr 1984
52.244-2	Subcontracts (Aug 1998) – Alternate II	Aug 1998
52.244-5	Competition in Subcontracting	Dec 1996
52.244-6	Subcontracts for Commercial Items	Dec 2004
52.245-1	Government Property	Jun 2007
52.247-1	Commercial Bill of Lading Notations	Apr 1984
52.247-63	Preference for U.S. Flag Air Carriers	Jun 2003
52.249-6	Termination (Cost Reimbursement)	Sep 1996
52.249-14	Excusable Delays	Apr 1984
52.251-1	Government Supply Sources	Apr 1984
52.253-1	Computer Generated Forms	Jan 1991
3052.204-71	Contractor Employee Access	Jun 2006

I.3 Security Requirements (FAR 52.204-2) (Aug 1996)

(a) This clause applies to the extent that this contract involves access to information classified “Confidential,” “Secret,” or “Top Secret.”

(b) The Contractor shall comply with—

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

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

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

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

(End of clause)

I.4 Notification of Ownership Changes (FAR 52.215-19) (OCT 1997)

- (a) The Contractor shall make the following notifications in writing:
- (1) When the Contractor becomes aware that a change in its ownership has occurred, or is certain to occur, that could result in changes in the valuation of its capitalized assets in the accounting records, the Contractor shall notify the Administrative Contracting Officer (ACO) within 30 days.
 - (2) The Contractor shall also notify the ACO within 30 days whenever changes to asset valuations or any other cost changes have occurred or are certain to occur as a result of a change in ownership.
- (b) The Contractor shall --
- (1) Maintain current, accurate, and complete inventory records of assets and their costs;
 - (2) Provide the ACO or designated representative ready access to the records upon request;
 - (3) Ensure that all individual and grouped assets, their capitalized values, accumulated depreciation or amortization, and remaining useful lives are identified accurately before and after each of the Contractor's ownership changes; and
 - (4) Retain and continue to maintain depreciation and amortization schedules based on the asset records maintained before each Contractor ownership change.
- (c) The Contractor shall include the substance of this clause in all subcontracts under this contract that meet the applicability requirement of FAR 15.408(k).

(End of Clause)

I.5 Ordering (FAR 52.216-18) (OCT 1995)

- (a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from the contract start date until 30 days prior to the expiration date.
- (b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this

contract, the contract shall control.

- (c) If mailed, a delivery order or task order is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

(End of clause)

I.6 Order Limitations (FAR 52.216-19) (OCT 1995)

- (a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than \$25,000 the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.
- (b) Maximum order. The Contractor is not obligated to honor:
 - (1) Any order for a single item in excess of \$5,000,000;
 - (2) Any order for a combination of items in excess of \$20,000,000; or
 - (3) A series of orders from the same ordering office within 365 days that together call for quantities exceeding the limitation in subparagraph (1) or (2) above.
- (c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) above.
- (d) Notwithstanding paragraphs (b) and (c) above, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within 5 days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of clause)

I.7 Indefinite Quantity (FAR 52.216-22) (OCT 1995)

- (a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.
- (b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the

Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum". The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum".

- (c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.
- (d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided that the Contractor shall not be required to make any deliveries under this contract after 30 days past the expiration date.

(End of clause)

I.8 Option to Extend Services (FAR 52.217-8) (NOV 1999)

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

(End of clause)

I.9 Option to Extend the Term of the Contract (FAR 52.217-9) (MAR 2000)

- (a) The Government may extend the term of this contract by written notice to the Contractor within 30 days prior to the expiration date; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.
- (b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
- (c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 5 years.

(End of clause)

I.10 Notification of Employees Rights Concerning Payment of Union Dues and Fees (FAR 52.222-39) (DEC 2004)

- (a) *Definition.* As used in this clause—
“United States” means the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands, and Wake Island.
- (b) *Except* as provided in paragraph (e) of this clause, during the term of this contract, the Contractor shall post a notice, in the form of a poster, informing employees of their rights concerning union membership and payment of union dues and fees, in conspicuous places in and about all its plants and offices, including all places where notices to employees are customarily posted. The notice shall include the following information (except that the information pertaining to National Labor Relations Board shall not be included in notices posted in the plants or offices of carriers subject to the Railway Labor Act, as amended (45 U.S.C. 151-188)).

Notice to Employees

Under Federal law, employees cannot be required to join a union or maintain membership in a union in order to retain their jobs. Under certain conditions, the law permits a union and an employer to enter into a union-security agreement requiring employees to pay uniform periodic dues and initiation fees. However, employees who are not union members can object to the use of their payments for certain purposes and can only be required to pay their share of union costs relating to collective bargaining, contract administration, and grievance adjustment.

If you do not want to pay that portion of dues or fees used to support activities not related to collective bargaining, contract administration, or grievance adjustment, you are entitled to an appropriate reduction in your payment. If you believe that you have been required to pay dues or fees used in part to support activities not related to collective bargaining, contract administration, or grievance adjustment, you may be entitled to a refund and to an appropriate reduction in future payments.

For further information concerning your rights, you may wish to contact the National Labor Relations Board (NLRB) either at one of its Regional offices or at the following address or toll free number:

National Labor Relations Board
Division of Information
1099 14th Street, N.W.
Washington, DC 20570
1-866-667-6572
1-866-316-6572 (TTY)

To locate the nearest NLRB office, see NLRB's website at <http://www.nlr.gov>.

- (c) The Contractor shall comply with all provisions of Executive Order 13201 of February 17, 2001, and related implementing regulations at 29 CFR Part 470, and orders of the Secretary of Labor.
- (d) In the event that the Contractor does not comply with any of the requirements set forth in paragraphs (b), (c), or (g), the Secretary may direct that this contract be cancelled, terminated, or suspended in whole or in part, and declare the Contractor ineligible for further Government contracts in accordance with procedures at 29 CFR Part 470, Subpart B—Compliance Evaluations, Complaint Investigations and Enforcement Procedures. Such other sanctions or remedies may be imposed as are provided by 29 CFR Part 470, which implements Executive Order 13201, or as are otherwise provided by law.
- (e) The requirement to post the employee notice in paragraph (b) does not apply to—
 - (1) Contractors and subcontractors that employ fewer than 15 persons;
 - (2) Contractor establishments or construction work sites where no union has been formally recognized by the Contractor or certified as the exclusive bargaining representative of the Contractor's employees;
 - (3) Contractor establishments or construction work sites located in a jurisdiction named in the definition of the United States in which the law of that jurisdiction forbids enforcement of union-security agreements;
 - (4) Contractor facilities where upon the written request of the Contractor, the Department of Labor Deputy Assistant Secretary for Labor-Management Programs has waived the posting requirements with respect to any of the Contractor's facilities if the Deputy Assistant Secretary finds that the Contractor has demonstrated that—
 - (i) The facility is in all respects separate and distinct from activities of the Contractor related to the performance of a contract; and
 - (ii) Such a waiver will not interfere with or impede the effectuation of the Executive order; or
 - (5) Work outside the United States that does not involve the recruitment or employment of workers within the United States.
- (f) The Department of Labor publishes the official employee notice in two variations; one for contractors covered by the Railway Labor Act and a second for all other contractors. The Contractor shall—
 - (1) Obtain the required employee notice poster from the Division of Interpretations and Standards, Office of Labor-Management Standards, U.S. Department of Labor, 200 Constitution Avenue, NW, Room N-5605, Washington, DC 20210, or from any field office of the Department's Office of Labor-Management Standards or Office of Federal Contract Compliance Programs;
 - (2) Download a copy of the poster from the Office of Labor-Management Standards website at <http://www.olms.dol.gov>; or
 - (3) Reproduce and use exact duplicate copies of the Department of Labor's official poster.
- (g) The Contractor shall include the substance of this clause in every subcontract or purchase order that exceeds the simplified acquisition threshold, entered into in connection with this contract, unless exempted by the Department of Labor Deputy Assistant Secretary for Labor-Management Programs on account of special circumstances in the national interest under authority of 29 CFR 470.3(c). For indefinite quantity subcontracts, the Contractor shall include the substance of this clause if the value of orders in any calendar year of the subcontract is

expected to exceed the simplified acquisition threshold. Pursuant to 29 CFR Part 470, Subpart B—Compliance Evaluations, Complaint Investigations and Enforcement Procedures, the Secretary of Labor may direct the Contractor to take such action in the enforcement of these regulations, including the imposition of sanctions for noncompliance with respect to any such subcontract or purchase order. If the Contractor becomes involved in litigation with a subcontractor or vendor, or is threatened with such involvement, as a result of such direction, the Contractor may request the United States, through the Secretary of Labor, to enter into such litigation to protect the interests of the United States.

(End of clause)

I.11 Rights to Proposal Data (Technical) (FAR 52.227-23) (JUN 1987)

It is agreed that as a condition of award of this contract, and notwithstanding the conditions of any notice appearing thereon, the Government shall have unlimited rights (as defined in the “Rights in Data—General” clause contained in this contract) in and to the technical data contained in the proposal dated Jan 2, 2009 , upon which this contract is based.

(End of clause)

I.12 Notification of Changes (FAR 52.243-7) (APR 1984)

- (h) *Definitions.* “Contracting Officer,” as used in this clause, does not include any representative of the CO. “Specifically Authorized Representative (SAR),” as used in this clause, means any person the CO has so designated by written notice (a copy of which shall be provided to the Contractor) which shall refer to this paragraph and shall be issued to the designated representative before the SAR exercises such authority.
- (i) *Notice.* The primary purpose of this clause is to obtain prompt reporting of Government conduct that the Contractor considers to constitute a change to this contract. Except for changes identified as such in writing and signed by the Contracting Officer, the Contractor shall notify the Administrative CO in writing promptly, within five (5) calendar days from the date that the Contractor identifies any Government conduct (including actions, inactions, and written or oral communications) that the Contractor regards as a change to the contract terms and conditions. On the basis of the most accurate information available to the Contractor, the notice shall state—
 - (1) The date, nature, and circumstances of the conduct regarded as a change;
 - (2) The name, function, and activity of each Government individual and Contractor official or employee involved in or knowledgeable about such conduct;
 - (3) The identification of any documents and the substance of any oral communication involved in such conduct;
 - (4) In the instance of alleged acceleration of scheduled performance or delivery, the basis upon which it arose;

- (5) The particular elements of contract performance for which the Contractor may seek an equitable adjustment under this clause, including—
 - (i) What contract line items have been or may be affected by the alleged change;
 - (ii) What labor or materials or both have been or may be added, deleted, or wasted by the alleged change;
 - (iii) To the extent practicable, what delay and disruption in the manner and sequence of performance and effect on continued performance have been or may be caused by the alleged change;
 - (iv) What adjustments to contract price, delivery schedule, and other provisions affected by the alleged change are estimated; and
- (6) The Contractor's estimate of the time by which the Government must respond to the Contractor's notice to minimize cost, delay or disruption of performance.
- (j) *Continued performance.* Following submission of the notice required by paragraph (b) of this clause, the Contractor shall diligently continue performance of this contract to the maximum extent possible in accordance with its terms and conditions as construed by the Contractor, unless the notice reports a direction of the Contracting Officer or a communication from a SAR of the Contracting Officer, in either of which events the Contractor shall continue performance; provided, however, that if the Contractor regards the direction or communication as a change as described in paragraph (b) of this clause, notice shall be given in the manner provided. All directions, communications, interpretations, orders and similar actions of the SAR shall be reduced to writing promptly and copies furnished to the Contractor and to the Contracting Officer. The Contracting Officer shall promptly countermand any action which exceeds the authority of the SAR.
- (k) *Government response.* The Contracting Officer shall promptly, within 15 calendar days after receipt of notice, respond to the notice in writing. In responding, the Contracting Officer shall either—
 - (1) Confirm that the conduct of which the Contractor gave notice constitutes a change and when necessary direct the mode of further performance;
 - (2) Countermand any communication regarded as a change;
 - (3) Deny that the conduct of which the Contractor gave notice constitutes a change and when necessary direct the mode of further performance; or
 - (4) In the event the Contractor's notice information is inadequate to make a decision under paragraphs (d)(1), (2), or (3) of this clause, advise the Contractor what additional information is required, and establish the date by which it should be furnished and the date thereafter by which the Government will respond.
- (l) *Equitable adjustments.*
 - (1) If the Contracting Officer confirms that Government conduct effected a change as alleged by the Contractor, and the conduct causes an increase or decrease in the Contractor's cost of, or the time required for, performance of any part of the work under this contract, whether changed or not changed by such conduct, an equitable adjustment shall be made—
 - (i) In the contract price or delivery schedule or both; and
 - (ii) In such other provisions of the contract as may be affected.
 - (2) The contract shall be modified in writing accordingly. In the case of drawings, designs or specifications which are defective and for which the Government is responsible, the equitable adjustment shall include the cost and time

extension for delay reasonably incurred by the Contractor in attempting to comply with the defective drawings, designs or specifications before the Contractor identified, or reasonably should have identified, such defect. When the cost of property made obsolete or excess as a result of a change confirmed by the Contracting Officer under this clause is included in the equitable adjustment, the Contracting Officer shall have the right to prescribe the manner of disposition of the property. The equitable adjustment shall not include increased costs or time extensions for delay resulting from the Contractor's failure to provide notice or to continue performance as provided, respectively, in paragraphs (b) and (c) of this clause.

(End of clause)

The following Homeland Security Acquisition Regulation (HSAR) clauses are provided in full text. All HSAR clauses shall flow down to all subcontractors on the contract and task order levels as applicable with emphasis given to H.6 and I.14.

I.13 Security Requirements for Unclassified Information Technology Resources (HSAR 3052.204-70) (Jun 2006)

- (a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.
- (b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.
 - (1) Within 45 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the Offeror's proposal. The plan, as approved by the contracting Officer, shall be incorporated into the contract as a compliance document.
 - (2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.
 - (3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance,

programming, and system administration of computer systems, networks, and telecommunications systems.

- (c) Examples of tasks that require security provisions include –
- (1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and
 - (2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).
- (d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Organizational elements shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.
- (3) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of Clause)

**I.14 Limitation of Future Contracting (HSAR 3052.209-73) (JUN 2006)
(Applicable at the Task Order Level)**

- (a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective Offerors is invited to FAR Subpart 9.5--Organizational Conflicts of Interest.
- (b) The nature of this conflict are: There are at least three forms of potential organizational conflicts of interest that may arise in the performance of this contract: (1) either the contractor or an affiliate's being able to compete when the contractor (a) had access to procurement sensitive information or (b) drafted specifications or statements of work or substantially complete statements of work; (2) the contractor's reviewing the work of itself or any affiliates, done on other DHS contracts; or (3) offering advice or planning in areas in which the contractor or any affiliates have financial interests tied to particular technologies.
- (c) The restrictions upon future contracting are as follows:

(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.

(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

(End of Clause)

I.15 The Small Business Subcontracting Program Reporting (HSAR 3052.219-70) (DEC 2003)

a) The Contractor shall submit Standard Form (SF) 295, Summary Subcontract Report electronically via the Electronic Subcontract Reporting System (eSRS). The report is due October 30th for the calendar period October 1 through September 30. In the event that the Electronic Subcontract Reporting System (eSRS) is not yet available for use, reports shall be submitted to the address identified in Section G.2.

b) The Contractor shall include this clause in all subcontracts that include the clause at (FAR) 48 CFR 52.219-9.

(End of Clause)

I.16 DHS Mentor-Protégé Program (HSAR 3052.219-71) (DEC 2003)

a) Large businesses are encouraged to participate in the DHS Mentor-Protégé program for the purpose of providing developmental assistance to eligible small business protégé entities to enhance their capabilities and increase their participation in DHS contracts.

b) The program consists of:

(1) Mentor firms, which are large prime contractors capable of providing developmental assistance;

(2) protégé firms, which are small businesses, veteran-owned small businesses, service-disabled veteran-owned small businesses, HUBZone small businesses,

small disadvantaged businesses, and women-owned small business concerns;
and

(3) Mentor-Protégé agreements, approved by the DHS OSDBU.

c) Mentor participation in the program means providing business developmental assistance to aid protégés in developing the requisite expertise to effectively compete for and successfully perform DHS contracts and subcontracts.

d) Large business prime contractors, serving as mentors in the DHS mentor-protégé program, are eligible for a post-award incentive for subcontracting plan credit by recognizing costs incurred by a mentor firm in providing assistance to a protégé firm and using this credit for purposes of determining whether the mentor firm attains a subcontracting plan participation goal applicable to the mentor firm under a DHS contract. The amount of credit given to a mentor firm for these protégé developmental assistance costs shall be calculated on a dollar for dollar basis and reported via the SF-295; for example, the mentor/large business prime contractor reports a \$10,000 subcontract to the protégé/small business subcontractor and \$5,000 of developmental assistance to the protégé/small business subcontractor as \$15,000 (\$10,000 traditional subcontract plus \$5,000 in developmental assistance for a total of \$15,000).

e) Contractors interested in participating in the program are encouraged to contact the DHS OSDBU for more information.

(End of Clause)

(End of Section I)

SECTION J – LIST OF ATTACHMENTS

- J-1 Sponsoring Agreement
- J-2 Monthly Contractor Financial Report
- J-3 Non-Disclosure Agreement, DHS Form 11000-6
- J-4 Contract Security Classification Specification, DD Form 254
- J-5 Small Business Concerns Subcontracting Plan
- J-6 DHS Certification and Accreditation Guide
- J-7 DHS Management Directive # 0143-04

J-1 SPONSORING AGREEMENT

J-2 MONTHLY CONTRACTOR FINANCIAL REPORT

J-3 NON-DISCLOSURE AGREEMENT, DHS FORM 11000-6

J-4 CONTRACT SECURITY CLASSIFICATION SPECIFICATION, DD FORM 254

*PLACEHOLDER – DD 254 FORTHCOMING AFTER AWARD

J-5 SMALL BUSINESS CONCERNS SUBCONTRACTING PLAN

J-6 DHS CERTIFICATION AND ACCREDITATION GUIDE

J-7 DHS MANAGEMENT DIRECTIVE # 0143-04

(End of Section J)

SECTION K – REPRESENTATIONS AND CERTIFICATIONS

The contractor's annual representations and certifications electronically filed at www.orca.gpn.gov are incorporated herein by reference and made a part of this contract.

(End of Section K)

SPONSORING AGREEMENT
Between
THE DEPARTMENT OF HOMELAND SECURITY
and
ANALYTIC SERVICES INC.
to Operate the
HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE (HSSAI)
FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTER (FFRDC)

1. PURPOSE OF THIS AGREEMENT

This Sponsoring Agreement (this Agreement) sets forth the policies and requirements for the operation of the Homeland Security Studies and Analysis Institute (HSSAI) Federally Funded Research and Development Center (FFRDC) by the **ANALYTIC SERVICES INC.**. The Homeland Security Studies and Analysis Institute (HSSAI) Federally Funded Research and Development Center (FFRDC) (hereafter referred to as the HSSAI FFRDC) shall be operated by **ANALYTIC SERVICES INC.** as an autonomous organization or as an identifiable separate operating unit of a parent organization in support of the Secretary of Homeland Security (DHS), the Under Secretary for Science and Technology (S&T), and the DHS Operating Elements. The Under Secretary for Science and Technology (S&T) is the Primary Sponsor of this Agreement.

This Agreement is in compliance with Federal Acquisition Regulation (FAR) Part 35.017. Additionally, the DHS Management Directive Number 143-04 "Establishing or Contracting with Federally Funded Research and Development Centers (FFRDCs) and National Laboratories" dated May 25, 2007, as amended, is hereby incorporated by this reference into and made a part of this Agreement.

This Agreement will be incorporated by reference into and made a part of the DHS contract with **ANALYTIC SERVICES INC.** for the operation of the HSSAI FFRDC (the Contract). If conflicts exist between this Agreement and the Contract, the Contract will take precedence and will control.

Portions of this Agreement are based on Federal government-wide and DHS policies, and future changes in these policies might necessitate changes to this Agreement. This Agreement may be amended, and its provisions may be modified or waived, by mutual written agreement of the parties. Capitalized terms used within this Agreement shall have the meanings ascribed to them herein or in the Contract.

2. BACKGROUND OF ANALYTIC SERVICES INC.

Analytic Services Inc. is a nonprofit corporation (under Section 501(c)(3) of the Internal Revenue Code) originally established in 1958 to provide scientific and technical analyses to the United States Air Force. The corporation today performs a broad spectrum of studies and analyses for clients throughout the National Security, Homeland Security, and Public Safety communities. Analytic Services Inc. has a wholly owned for-profit subsidiary, Program Solutions Incorporated, which also provides professional services to these same communities and operates in accordance with the Analytic Services Inc. conflict-of-interest policy. Analytic Services Inc. is governed by a Board of Trustees which includes members from business, academia, law, and defense communities. The Board of Trustees has established a separate committee to provide oversight for conflict of interest issues. Analytic Services Inc.'s corporate headquarters are located in Arlington, Virginia.

3. PURPOSE AND MISSION OF THE FFRDC

The purpose of this Homeland Security Studies and Analysis Institute (HSSAI FFRDC) is to provide special technical expertise to Department mission owners to transform mission-level goals into strategies, operational requirements, and performance metrics, constrained by cost and schedule. Through studies and analysis the Institute shall provide recommendations for policy and operational changes, as well as technology insertion concepts, throughout the federal, state, local, tribal, public and private sector organizations that make up the homeland security enterprise. The HSSAI FFRDC shall generally work on the most complex homeland security issues and problems. The HSSAI FFRDC will

promote fair and open competition for the development and delivery of homeland security enterprise capabilities by providing independent and objective technical expertise in: cross-cutting mission analysis, strategic studies and assessments, modeling of operational concepts and policy trade-offs within and across mission areas, system simulations and technical assessments to evaluate mission trade-offs, creation and evolution of high-level concepts of operation, development of top-level system and operational requirements and performance metrics, operational analysis across the homeland security enterprise, and analytic support for operational testing and evaluation in tandem with the Government's acquisition process. The HSSAI FFRDC shall ensure a logical optimization of mission and system-of-system tradeoffs from a long term perspective based on system/program lifecycle costs. Overtime, this FFRDC will help the Department develop a homeland security enterprise "system of systems" approach and thought leadership that will promote efficiencies and synergies across all missions. Through its long term relationship with the Department, the HSSAI FFRDC shall promote frameworks and strategies to enhance the general understanding of the trade-offs inherent in reducing our Nation's risk to terrorism and catastrophic incidents through, among other things, improved interoperability and information sharing across the homeland security enterprise.

4. SCOPE OF WORK

The Contractor shall be responsible for providing technical and integration expertise to Department of Homeland Security (DHS) senior leadership as a trusted agent, particularly in the evolution of the most complex and critical homeland security mission areas. The purpose of the HSSAI FFRDC is to help the Department address "what" must be accomplished, in a risk-informed manner, to meet and measure performance of homeland security mission goals and objectives with limited resources. The general goal is to maximize risk reduction across the gamut of terrorism and major disaster scenarios based on available funding and "dual-use" solution strategies. The HSSAI FFRDC will provide the government with the necessary expertise to conduct: cross-cutting mission analysis, strategic studies and assessments, development of models that baseline current capabilities, development of simulations and technical evaluations to evaluate mission trade-offs, creation and evolution of high-level operational and system concepts, development of top-level system and operational requirements and performance metrics, operational analysis across the homeland security enterprise, and analytic support for operational testing and evaluation in tandem with the government's acquisition process. The HSSAI FFRDC shall ensure a logical optimization of mission and system-of-system tradeoffs from a long term perspective based on system lifecycle costs. Overtime, this FFRDC will help the Department develop a homeland security enterprise "system of systems" approach that will promote efficiencies and synergies across all homeland security mission areas.

The FFRDC shall operate based on an annual research plan that will consist of "core" tasks funded by the S&T program office, and "task order" studies funded from sponsors across the Department. The "core" program is expected to be maintained at roughly 20% of the total Institute funding that is envisioned to enable the Institute to provide, among other things:

- Quick-response and strategic forward and field analysts where-ever and whenever required
- Thought leadership on cross-cutting and homeland security enterprise-wide critical and strategic issues
- Development of risk and other models and methods for understanding and comparing the mission requirements, performance metrics, and measures of effectiveness across the homeland security enterprise

Task order funding from the Department will address a variety of studies and analysis, including:

- Conduct strategic assessments of homeland security threats, vulnerabilities and consequences as well as national and international strategies for addressing the risk to the Nation
- Examine broad security topics such as countering vulnerabilities to critical infrastructures; proliferation of nuclear, chemical, and biological weapons; regional political, economic, military, and terrorist trends; and international terrorist cooperation and assess domestic and international implications of trade and technology cooperation, plans, and controls.
- Development of top level mission risk and risk reduction (threat, vulnerability, consequence) resource allocation models, component tradeoff simulations, and tools and metrics to evaluate mission tradeoffs and mission integration strategies

- Development of system and system-of-system concepts through analysis of alternatives to address the most strategic and critical needs of the homeland security enterprise
- Analyze the risk (threat, vulnerability, consequence) reduction potential of constrained resources by analyzing synergies obtained through common homeland security enterprise systems developments, interoperability, and common hardware/software interfaces and protocols
- Development of top-level program requirements and system performance and effectiveness metrics based on mission goals
- Develop and promote standardization of effective and efficient operational modeling, simulation, test and evaluation best practices for homeland security programs to provide independent and objective assessments based on mission and program goals
- Develop methods for identification, particularly within the various DHS Integrated Process Teams (IPTs), of critical capability gaps particularly in areas where policy, operations, and/or technology may be expected to contribute substantially to solutions; and develop trade-off studies and roadmaps for “filling the gap”
- Design and provide support for the conduct of homeland security-related exercises, games, and simulations, including the examination of past incidents, tabletop and operational exercises, and nominal operations to determine lessons learned and the implications for homeland security planning. A principal focus of these studies also will be on assessing national response and multi-agency collaboration and coordination; interoperability of federal with state and local personnel and systems; and logistics support.
- Provide assistance to the homeland security enterprise in establishing test-beds requirements to evaluate the effectiveness of technologies under development and assess the appropriateness of such technologies for deployment; and conduct assessments of technology feasibility, performance, producibility, demonstrations, and development risks.
- Conduct operational analysis, particularly at field activities for extended (months to 1-2 years) periods, to provide objective assessments, systems evaluations, and other technical and analytic support that promotes the identification and understanding of the interplay of operation elements, like: doctrine, organization, training, material, leadership, education, personnel, facilities, etc. in the need for identifying solutions to new and evolving mission requirements including the instantiation of capabilities to provide and promote security, privacy, and the protection of civil rights and civil liberties.
- Use economic (lifecycle) and policy analyses to assess the distributed costs and benefits of alternative approaches to enhancing security including leveraging of homeland security, particularly R&D, assets across the Nation and with international partners.
- Examine infrastructure and support activities, including issues related to major acquisitions and R&D planning; advanced manufacturing practices; the governmental and commercial technology base; mobilization and stockpiling of critical materials; the training establishment; logistics needs; and environmental technologies.
- Promote ethics in acquisition through an understanding of: the need for objective development of operational requirements and performance metrics, and operational test and evaluation planning and analysis independent from the development program; promotion of fair and open competition in acquisitions through high quality technical data packages and quality oversight, trusted agent relationships with the government task sponsors and the FFRDC program office, establishment of staff and organizational conflict or interest protocols.

Within and across these core areas, DHS sponsors’ specific needs are expected to evolve over time, and the HSSAI FFRDC capabilities and areas of concentration will evolve accordingly.

The HSSAI FFRDC will also implement a broad-based consultative strategy to extend beyond the in-house staff and include perspectives from experts in industry, academia, and the non-profit sector. The HSSAI FFRDC will also be expected to have broad access to facilities that can provide simulation and modeling in support of trade-off analysis studies, performance metric development, operational studies, and operational test and evaluation analysis across all areas of homeland security mission areas, including but not limited to (classified and unclassified): information technology and management, intelligence and information sharing, borders and maritime security (sensor and data networks), chemical and biological detection and protection, transportation system and critical infrastructure protection

and security, cyber security and protection, biometric identification, communications interoperability and security, and emergency planning and response.

Other Duties. In addition to those services described in this Section 4 (Scope of Work), DHS may require the HSSAI FFRDC to perform other services within the HSSAI FFRDC core competencies.

5. POLICY

a. The HSSAI FFRDC will maintain the capabilities (high-quality research staff, other management and technical capabilities, analytic tools, models and simulations, computing resources, knowledge of sponsor needs, etc.) necessary to address any issue consistent with the FFRDC's purpose, mission, and scope of work. The HSSAI FFRDC will work on many classified and highly sensitive projects and shall strictly comply with the provisions of the National Industrial Security Program – including the provisions dealing with foreign ownership, control or influence (FOCI) – as set forth in DOD Directive 5220.22-M as amended.

b. All DHS components and Operating Elements are potential sponsors of HSSAI FFRDC tasks.

c. HSSAI FFRDC tasks will be undertaken by mutual consent between the HSSAI FFRDC and the sponsor in accordance with procedures instituted by the Primary Sponsor or designee and the HSSAI FFRDC Advisory Group, as appropriate. All tasks must be approved by the HSSAI FFRDC program management office. (Prior to execution, tasks require signature approval of the HSSAI FFRDC Program Manager.) Funding for specific tasks may come from various program elements available to sponsoring offices.

d. Proposals for work to be undertaken by the HSSAI FFRDC may originate with any sponsoring office or with the HSSAI FFRDC itself. Tasks may be initiated at any time during a fiscal year, and may extend over several fiscal years in accordance with the funding appropriation. The HSSAI FFRDC, in conjunction with its Primary Sponsor (or the Primary Sponsor's designee), will prepare an annual research plan representing collectively the research agenda of the sponsoring community. Changes to the plan, consistent with the HSSAI FFRDC's core statement may be made throughout the year. These changes must be approved by the Executive Agent (as defined in Section 6(a)(6)).

e. The sponsoring community as represented by the HSSAI FFRDC Advisory Group will: (1) maintain and strengthen the "special relationship" between the HSSAI FFRDC and its sponsors; (2) serve as a link between the HSSAI FFRDC sponsor community and ANALYTIC SERVICES INC. management, providing feedback on DHS needs, interests, and priorities; and (3) assist and advise the Primary Sponsor in ensuring that the HSSAI FFRDC produces work consistent with this Agreement and the DHS Management Directive 143-04.

f. The Primary Sponsor will assure a reasonable continuity in the level of support to the HSSAI FFRDC, consistent with DHS needs and the terms of this Agreement, and contingent on available funding (as required by the FAR 35.017-2).

g. The HSSAI FFRDC may accept work from non-sponsoring agencies (i.e., organizations not specified in sections 5.b. above), including non-DHS Government entities, state and municipal governments, and public charities, provided that the work is: (1) determined to be consistent with the HSSAI FFRDC core statement; (2) approved by the Executive Agent (using the criteria set forth in Section 7 below and the DHS Management Directive Number 143-04 for determining the feasibility of and appropriateness of FFRDC work) and coordinated with the HSSAI FFRDC Program Manager and Contracting Officer's Technical Representative (COTR); and (3) does not interfere with the priority of the work that HSSAI FFRDC is performing for the sponsors (i.e., HSSAI FFRDC has adequate resources to perform work for non-sponsoring agencies and still meet the time frames for its deliverables to the HSSAI FFRDC DHS sponsors).

h. The HSSAI FFRDC's sponsors will provide access to classified and sensitive data, facilities, plans and related information, including proprietary data, as necessary to ensure that the HSSAI FFRDC's work takes full account of the best available information, including that which is not normally available to non-government organizations.

i. Subject to the requirements set forth in Section 5(j) below, the HSSAI FFRDC may augment its in-house research staff with other technical and analytic resources for work on sponsor problems the scope of which requires temporary access to specialized expertise that is not available within the organization. These resources if not included in the research plan will be coordinated with the Executive Agent and/or the Program Manager.

j. The HSSAI FFRDC may utilize subcontractors and consultants (including reach-back employees from the parent organization) for DHS related work subject to the following conditions: (i) HSSAI FFRDC has received the Executive Agent's approval prior to retaining a subcontractor or consultant for DHS related work; (ii) the Contracting Agent may require that HSSAI FFRDC terminate a subcontractor or consultant from performing DHS related work; and (iv) HSSAI FFRDC will require every subcontractor and consultant to sign nondisclosure agreements (containing the terms set forth in Section 9(g) below with the exception of Section 9(g)(2)) and conflict of interest agreements. Both agreements must have been approved by the DHS Office of the General Counsel prior to HSSAI FFRDC allowing a subcontractor or consultant to perform DHS-related work. HSSAI FFRDC will maintain signed copies of every non-disclosure and conflict of interest agreement for a period of at least five (5) years from the signature date on each document.

k. The HSSAI FFRDC's independent research program will be used primarily to assist in building and maintaining research capabilities in support of the HSSAI FFRDC's mission, purpose, and scope of work, consistent with DHS-wide guidelines for independent research and development activities.

l. No member of the ANALYTIC SERVICES INC. Board of Trustees who is also serving as a member of a Board of Directors, Trustees, or Overseers or any similar governance board for any other for-profit or non-profit entity that is engaged in providing professional services or research and development in the government services market shall be permitted to serve on panels or committees reasonably related to the HSSAI FFRDC or vote on decisions reasonably related to the HSSAI FFRDC unless such automatic recusal of the Board of Trustees member is waived by the DHS Executive Agent.

6. RESPONSIBILITIES AND OVERSIGHT

a. The ultimate sponsor of the HSSAI FFRDC is the Department of Homeland Security. The Under Secretary for Science and Technology acts for DHS as the Primary Sponsor of HSSAI FFRDC. The Primary Sponsor (U/S Science and Technology):

- (1) Ensures that the HSSAI FFRDC is used for its intended purposes.
- (2) Ensures that individual sponsors make appropriate use of the HSSAI FFRDC's work.
- (3) Ensures that the HSSAI FFRDC produces high-quality work of value to sponsors.
- (4) Ensures that the costs of services provided by HSSAI FFRDC are reasonable.
- (5) Determines whether to continue or terminate the sponsorship of the HSSAI FFRDC upon completion of each five-year comprehensive review.
- (6) Designates an Executive Agent (the Executive Agent) to provide DHS oversight of the HSSAI FFRDC, consistent with the terms of this Agreement, the HSSAI FFRDC contract, and any additional policies and procedures established for the HSSAI FFRDC.

b. The Executive Agent:

- (1) Designates membership and chairs the HSSAI FFRDC Advisory Group. Designates replacements for HSSAI FFRDC Advisory Group members.
- (2) Provides oversight through the HSSAI FFRDC program management office which includes the HSSAI FFRDC Program Manager and the Contracting Officer's Technical Representative

(3) Reviews and approves DHS-sponsored research plan.

(5) Reports to the Contracting Officer any organizational conflicts of interest associated with ANALYTIC SERVICES INC. performance under the contract as soon as conflicts are identified (or appear to be identified). The Executive Agent shall provide a recommended disposition of the conflict and solicit advice as needed from the Contracting Officer.

(6) Designates the Program Manager and replacements for such individual.

(7) Reviews and approves each non-DHS sponsored research task conducted by ANALYTIC SERVICES INC. (and any affiliate thereof) involving the same core work as the HSSAI FFRDC, as elaborated in Section 4 of this Agreement, subject to the following terms and conditions:

- a. All work to be performed by ANALYTIC SERVICES INC. for the Department of Homeland Security will be approved in advance by the Executive Agent. The Executive Agent will approve/disapprove all such work requests within four working days following being notified in writing by ANALYTIC SERVICES INC. of its intention to enter into a contract or bid on work with the Department of Homeland Security.
- b. All work performed by ANALYTIC SERVICES INC. for all other public sector entities and public charities will be reported on a quarterly basis to the Executive Agent. The first such report on non-FFRDC work by ANALYTIC SERVICES INC. will be due at the end of the first quarter following conclusion of this Agreement and each quarter thereafter.
- c. DHS reserves the right to require pre-approval of all new non-FFRDC work involving the same core work of the HSSAI FFRDC to be conducted by ANALYTIC SERVICES INC. under the notice and approval procedures set forth in subparagraph (a) of this Section 6(b)(7).

(8) Reviews and approves each non-DHS sponsored research task conducted by the HSSAI FFRDC.

(9) Reviews and approves the classification, publication, and distribution of HSSAI FFRDC publications prepared for DHS Operating Elements, non-DHS Government entities, state and municipal governments, and public charities.

(10) Oversees HSSAI FFRDC's use of subcontractors and consultants subject to the restrictions set forth in Section 5(j).

c. The Program Manager

(1) Administers the day-to-day HSSAI FFRDC relationship with the Government as approved by the Executive Agent.

(2) Ensures compliance with DHS and FFRDC policies.

(3) Coordinates and works with the staff points of contact for the HSSAI FFRDC Advisory Group members to implement Advisory Group decisions, and assists the Executive Agent in administering the HSSAI FFRDC strategic relationship as required.

(4) Establishes procedures for processing task orders.

(5) Reviews and approves DHS-sponsored tasks.

(6) Provides procurement liaison to the Contracting Officer for tasks placed under the contract for HSSAI FFRDC performance.

(7) Acts as the DHS focal point for contact with HSSAI FFRDC. Once tasks are approved, sponsors deal directly with the HSSAI FFRDC on specific technical matters related to HSSAI FFRDC research.

(8) Assists sponsoring offices in providing information on the HSSAI FFRDC research to other DHS offices and Government agencies.

(9) Ensures HSSAI FFRDC receives access to Government information needed to conduct approved research projects. Ordinarily, sponsors release classified, privileged, no-contractor, and other sensitive material directly to HSSAI FFRDC.

d. The HSSAI FFRDC Advisory Group:

(1) Ensures the proposed research program addresses senior management concerns and priorities.

(2) Identifies cross-cutting or other issues important to senior management for joint sponsorship and funding.

(3) Confirms that the research program is appropriate for an FFRDC and consistent with the HSSAI FFRDC's core statement.

(4) Identifies ways to strengthen the strategic relationship between DHS sponsors and the HSSAI FFRDC.

(5) Reviews the results of annual performance reviews and takes appropriate action to resolve problems.

(6) Provides feedback to ANALYTIC SERVICES INC. management on DHS' needs, interests, and priorities for the upcoming year and over the longer term.

e. Sponsoring Offices:

(1) Identify research and technical topics to be undertaken by HSSAI FFRDC, and formulate these topics into task orders, consulting as appropriate with the executive agent (or designee) and the HSSAI FFRDC.

(2) Identify project funding and provide documentation necessary to initiate the task, consistent with established procedures. These procedures require signature approval for each task from the HSSAI FFRDC Program Manager. Before a task can be placed on contract, a written justification showing that the work is appropriate for the HSSAI FFRDC (i.e., satisfies the criteria included in the core statement) must be prepared. This justification can be incorporated in the project's task order.

(3) Monitor the execution of research projects, including the quality and timeliness of the work, and its value to DHS.

(4) Participate as appropriate in meetings of the HSSAI FFRDC Advisory Group and related activities.

(5) Provide HSSAI FFRDC full access to the information necessary to carry out the research tasks.

f. ANALYTIC SERVICES INC. and HSSAI FFRDC Management:

(1) Manages the operations of the HSSAI FFRDC consistent with the provisions of the HSSAI FFRDC contract with the Government, this Agreement, and ANALYTIC SERVICES INC.'s corporate charter.

- (2) Develops and maintains research capabilities necessary to address any issue consistent with the FFRDC's purpose, mission, and scope of work; with sponsor needs; and with the availability of funds.
- (3) Develops, on occasion, proposals for research topics, particularly research on cross-cutting issues of interest to several HSSAI FFRDC sponsors. In conjunction with sponsors and the Executive Agent, prepares and presents an annual research plan to the HSSAI FFRDC Advisory Group.
- (4) Executes the research program, maintaining quality control over the research products.
- (5) Prepares other materials requested by the Advisory Group, and works with the sponsoring offices and the Advisory Group, if necessary, to resolve any problems related to the HSSAI FFRDC research program.
- (6) Maintains a written, rigorous, corporate-wide, organizational and staff conflict of interest regimen in accordance with a conflict of interest policy reviewed and approved in writing by DHS. Any changes made to an HSSAI FFRDC conflict of interest policy, or ANALYTIC SERVICES INC.'s conflict of interest policy regarding the HSSAI FFRDC, must be approved in writing by the DHS Executive Agent.
- (7) Reports any organizational conflicts of interest and their proposed disposition to the Contracting Officer and to the Executive Agent (and/or designee) as soon as such conflicts are identified.

7. DETERMINING SUITABILITY OF WORK FOR HSSAI FFRDC

The task sponsor and the Executive Agent have joint responsibility for determining that a proposed research task is appropriate for the HSSAI FFRDC. Consideration will be given to several criteria related to the nature of the specific project, and the special relationship that the HSSAI FFRDC maintains with its sponsors. The criteria include:

- a. Consistency with the HSSAI FFRDC's mission, purpose, and capabilities.
- b. Consistency with the HSSAI FFRDC's core competencies, as reflected in the core statement required by DHS' FFRDC Management Plan and summarized in the scope of work statement above. Changes in the details of the core statement can be made by agreement between HSSAI FFRDC and the Executive Agent.
- c. Consistency with the HSSAI FFRDC's special relationship with its sponsors, as evidenced by the need for one or more of the following:
 - (1) Effective performance of objective, high-quality work on subjects integral to the mission and operations of sponsoring offices.
 - (2) Freedom from real and perceived conflicts of interest caused by commercial or other involvement.
 - (3) Broad access to information, including sensitive Government information, proprietary data from industry, and other information not normally available outside the Government.
 - (4) Comprehensive knowledge of sponsor needs, problems, and issues.
 - (5) Responsiveness to emerging and evolving needs of sponsors.
 - (6) Long-term continuity of knowledge on issues and problems of enduring concern, including both maintaining corporate memory for sponsors when appropriate and responding to quick-response sponsor needs in areas of established expertise.

8. ANNUAL ASSESSMENT PROCEDURES

- a. The COTR will conduct an annual assessment (which will then be approved and forwarded by the Executive Agent) as specified in DHS' FFRDC Management Plan.
- b. For the annual assessment, a survey of project sponsors will be conducted. The survey will gather data on sponsors' perceptions of the various aspects of the HSSAI FFRDC work (e.g., technical quality, responsiveness, program value, and timeliness).
- c. The Program Manager will report the results of the annual assessment to the Advisory Group and to the HSSAI FFRDC. The Advisory Group will review the assessment with the HSSAI FFRDC, provide feedback, and assist in resolving any real or perceived problems.
- d. In addition, HSSAI FFRDC will describe for the Advisory Group steps taken to ensure cost-effective operations.
- e. HSSAI FFRDC, and its parent corporation, will provide an annual compliance statement in terms of organizational conflicts of interest and staff non-disclosure agreements and conflicts of interest.

9. OTHER CONSIDERATIONS AND GENERAL UNDERSTANDINGS

a. Limitations. The strategic relationship between the HSSAI FFRDC and its sponsors requires that the HSSAI FFRDC accept certain restrictions, namely, that the HSSAI FFRDC:

- (1) May only perform core work as defined in the core statement and in accordance with the guidelines specified in the DHS Management Directive 143-04.
- (2) May not compete with any non-FFRDC in response to a Federal request for proposals for other than the operation of an FFRDC.
- (3) May accept no work developing specific components or component prototypes, without written approval of the Executive Agent; who may approve the work when directly related to a specific critical system program development.
- (4) May accept no work from commercial firms or foreign governments.
- (5) Shall not, unless authorized by legislation and the contract, undertake quantity production or manufacturing.
- (6) And its parent corporation and affiliates, if any, shall not, because of the need to eliminate actual or potential conflicts of interest between the interrelated missions of the DHS FFRDCs, operate the National Biodefense Analysis and Countermeasures Center (NBACC), the Homeland Security Systems Engineering and Development Institute (SEDI), or any other future DHS FFRDC, or participate as a substantial partner or sub-contractor to another DHS FFRDC contractor. Employees of the HSSAI FFRDC contractor and its parent corporation and affiliates, if any, may participate as consultants on specific tasks conducted by other DHS FFRDCs providing the procedures for approving the consultants are followed.

b. The limitations enumerated in 9.a (1-5) apply to the HSSAI FFRDC, not **ANALYTIC SERVICES INC.** **ANALYTIC SERVICES INC.** may perform non-FFRDC work, if such work meets the following criteria specified in the DHS Management Directive 143-04 and any additional criteria mutually agreed to between **ANALYTIC SERVICES INC.** and the Primary Sponsor or designee:

- (1) Parent institutions operating DHS-sponsored FFRDC(s) may perform non-FFRDC work subject to US(S&T) or its designee review for compliance with established criteria mutually agreed upon by the US(S&T) and the parent institution.

(2) Non-FFRDC work by parent institutions should be in the national interest, such as addressing economic, social, or governmental issues.

(3) Non-FFRDC work shall not undermine the independence, objectivity, or credibility of the FFRDC by posing an actual or perceived conflict of interest, nor shall it detract from the performance of FFRDC work.

(4) Non-FFRDC work shall not be acquired by taking unfair advantage of the parent institution's operation of its FFRDC(s) or of information that is available to that parent institution only through its FFRDC(s).

(5) Non-FFRDC work may be done for public sector entities and not-for-profit organizations that operate in the public interest; e.g., public charities. Commercial work (i.e., work for for-profit entities) may only be accepted if the primary sponsor, or its designee, grants a specific exception in writing for the commercial work request at issue. If the sponsor grants an exception, such work may not exclusively benefit any individual for-profit entity to avoid the appearance that an FFRDC parent organization is endorsing a particular product, company, or industrial process.

c. Retained Earnings and Fees. The parties acknowledge that fees may be appropriate. They can provide the capital and financial flexibility required to sustain professional expertise, obtain necessary facilities, equipment, and special test equipment, and maintain operations capable of supporting requirements of sponsors of HSSAI FFRDC core tasks under the contract. The guidelines for FFRDC Fees included in the DHS Management Directive 143-04 will serve as the guiding document in determining "need-for-fee" and the amount of the fee.

(1) **ANALYTIC SERVICES INC.** will annually submit a fee justification.

(2) In reviewing the fee justification, the Contracting Officer will apply the methodology and considerations of the FAR and DHS Management Directive 143-04, as applicable. The Contracting Officer will consult, as appropriate, with DHS Contract Audit Personnel or DCAA, and the Executive Agent (or designee) for the HSSAI FFRDC.

(3) Fees received by **ANALYTIC SERVICES INC.** for the operation of the HSSAI FFRDC may be commingled with fees earned on other contracts and/or with other income. Similarly, so long as HSSAI FFRDC is operated within **ANALYTIC SERVICES INC.**, it may use fees received under contracts covered by this Agreement for the benefit of the corporation (e.g., for working capital or facilities acquisition).

d. Cost Elements Requiring Advance Notice. **ANALYTIC SERVICES INC.** will provide the Executive Agent and the Contracting Officer at least 30 days of advance notice prior to:

(1) The acquisition of real property either by purchase or long-term lease that is to be used primarily by the HSSAI FFRDC.

(2) Any material increase in employee benefits chargeable, directly or indirectly, to a contract or contracts covered by this Agreement (except to the extent such increase is mandated by law).

e. Reports. In addition to the reports described in this Agreement, the HSSAI FFRDC will provide the reports described in Appendix C of the DHS Management Directive 143-04 to DHS. An annual report will be provided to the Primary Sponsor on 01 July.

f. Technology Transfer. If the HSSAI FFRDC wishes to participate in a technology transfer program with private industry, HSSAI FFRDC shall adhere to the technology transfer policies established by S&T. Such policies will include adequate safeguards to ensure the HSSAI FFRDC remains free of organizational conflicts of interest and that the conditions for establishing and maintaining the HSSAI FFRDC are not compromised. S&T shall also review and approve any technology transfer work on a case-by-case basis.

g. Non Disclosure of Sensitive Information. The HSSAI FFRDC acknowledges that in the course of performing work for DHS, HSSAI FFRDC and its personnel (which includes dedicated staff, consultants, and subcontractors) may have access to proprietary and privileged information of DHS and other entities and may also produce information that is proprietary and privileged to DHS. Except as otherwise required by applicable law or

regulation or a final order of a court of competent jurisdiction (in which event written notice will be given to DHS prior to disclosure or use of the information in order to give DHS a reasonable opportunity to protect its interests), or as expressly authorized in writing by the DHS Executive Agent, the HSSAI FFRDC agrees on behalf of itself and its personnel, that the HSSAI FFRDC and its personnel will not (a) disclose any Privileged Information (as defined below) related to the work performed for or on behalf of DHS, or (b) use any Privileged Information for the benefit of the HSSAI FFRDC, any of the HSSAI FFRDC personnel, or any third party. HSSAI FFRDC will require all of its personnel to execute non-disclosure agreements approved by the DHS Executive Agent prior to performing work for DHS, and shall ensure that such personnel comply with the provisions of such agreements and this paragraph g.

(1) For purposes of this Agreement, "Privileged Information" means any and all information and data (1) relating to the work performed by the HSSAI FFRDC for or on behalf of DHS, including the products of such work and deliverables; or (2) provided by DHS, S&T, or any of the DHS Operating Elements to the HSSAI FFRDC; or (3) provided by corporate entities working on or advising on DHS matters. "Privileged Information" shall include, but not be limited to, all data, pricing information and cost data information, controlled unclassified information (e.g., Protective Critical Infrastructure Information, Sensitive Homeland Security Information, and Law Enforcement Sensitive Information), know-how, written materials, proposals, memoranda, notes, inventions, devices, technology, designs, copyrighted information, trade secrets, confidential business information, analyses, test and evaluation results, manuals, videotapes, contracts, letters, facsimile transmissions, electronic mail and other correspondence, financial information and projections, and business and marketing plans. "Privileged Information" shall not include any information or data that is in the public domain or becomes part of the public domain by any means other than a breach by HSSAI FFRDC or HSSAI FFRDC personnel of the obligations under this Agreement.

(2) The restrictions set forth in this Agreement with regard to Privileged Information are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958; 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 U.S.C. 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 U.S.C. 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. 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.

10. NON-RENEWAL, TERMINATION, OR DISSOLUTION

a. This Agreement and **ANALYTIC SERVICES INC.**'s operation of the HSSAI FFRDC are based on expectations of a long-term and continuing relationship between the parties. DHS will use its best efforts to inform **ANALYTIC SERVICES INC.** as far as possible in advance if it concludes that such a long-term relationship is no longer in the best interests of the Government.

b. In the event that the contract for the HSSAI FFRDC is terminated (as that term is defined in FAR Part 49) in whole or in part, termination, disposal of assets, and settlement of liabilities will be in accordance with the DHS contract with **ANALYTIC SERVICES INC.** and FAR 52.249-6. Nothing in this Agreement shall be construed as committing the U.S. Government to termination costs.

c. In the event of such termination or of the expiration or non-renewal of this Agreement and of contract(s) for the HSSAI FFRDC, all items that were furnished by the Government or purchased by **ANALYTIC SERVICES INC.** and charged directly to the contract are the property of the Government and will be managed/disposed of in accordance with FAR 52.245-1.

d. Except as otherwise provided in a contract or advance agreement, all other assets (including equipment and leases on real property) will be the property of **ANALYTIC SERVICES INC.** and all liabilities will be the responsibility of **ANALYTIC SERVICES INC.**

e. In the event of dissolution of **ANALYTIC SERVICES INC.**, the Members of the Corporation will designate the successor corporation or a charitable organization or organizations or the Federal Government or any or all of them to be recipients to which will be paid over any or all property or assets remaining after the winding up of **ANALYTIC SERVICES INC.**'s affairs, in accordance with the Corporation's Certificate of Incorporation and By-Laws.

11. TERM OF THIS AGREEMENT

This Agreement will be effective when executed by both parties and shall be made a part of and incorporated by this reference into the Contract. This Agreement will be in force for the duration of the Contract. Subject to a favorable "need determination" resulting from the Comprehensive Review (as described by the FAR Section 35.017 and the DHS Management Directive 143-04) and, if mutually agreed between the Primary Sponsor and **ANALYTIC SERVICES INC.**, this Agreement will continue to be in full force and effect for subsequent renewals of the Contract.

This Agreement obligates no appropriations, and creates no responsibility on the part of DHS to fund work at or provide funds to **ANALYTIC SERVICES INC.** Funds are obligated and work undertaken only and strictly in accordance with the terms and conditions of the Contract.

Ruth A. David
President and Chief Executive Officer
Analytic Services Inc.

Bradley Buswell
Acting Under Secretary for Science and Technology
Department of Homeland Security

(date)

(date)

INSTRUCTIONS FOR COMPETITION OF MONTHLY CONTRACTOR FINANCIAL MANAGEMENT REPORT

1. Report for Month Ending and Number of Working Days: enter the ending date of the contractor's accounting month and the number of working days for that accounting month.
2. Contractor: Enter the full name and address of the contractor, and, if applicable, the division performing the contract.
3. Contract Value: Enter the total definitized cost (a) and fee (b) of all currently authorized work to be performed under the contract. Include dollar amounts through the latest definitized modification a noted in item #5.
4. Contract Type: Cost plus fixed fee, cost reimbursement/cost share, etc.
5. Contract No. and Latest Definitized Modification No.: Enter complete letter or contract symbol, number, and number of latest definitized modification.
6. Fund Limitation: Enter the total funds obligated and latest corresponding contract modification number.
7. Scope of Work: Enter a brief description of the contract effort.
8. Authorized Contractor Representative (signature and date): The authorized contractor representative shall sign and date the summary page to reflect approval.
9. Billing:
 - a. Invoice Amounts Billed: Enter the total amount of invoices billed against the contract and latest invoice number.
 - b. Total Payments Received: Enter the total amount of payments received for the contract.
10. Reporting Category: enter the captions of the reporting categories specified in the contract.
11. Cost Incurred/Hours Worked: Cost and hour data will be reported in the categories specified in the contract.
 - a. Actual During Month: Enter the total actual cost incurred/hours worked for the accounting month being reported (item #1).
 - b. Planned: Enter the Contractor's planned cost/hours.
 - c. Actual Cum to Date: Enter the cumulative actual cost incurred/hours worked.
 - d. Planned: Enter the Contractor's planned cost/hours.
12. Estimated Cost/Hours to Complete: Enter the current estimates for performing authorized work included in the most recently executed contract modification, plus additional authorized work (directions to proceed) for which execution of modifications is pending. The estimates will be for planning purposes only and will not be binding on either the contractor or DHS.
13. Estimated Final Cost/Hours:
 - a. Contractor Estimate: Enter the total estimated cost/hours for completion of the contracted effort (this should equal the sum of columns 11c, 12a, and 12b).

b. Contract Value: Enter the distribution of contract value to the reporting categories. The total of this column shall agree with item #3. Significant differences between columns 13a and 13b shall be explained in the "Contractor Narrative Remarks."

C.5 – SUBCONTRACT MANAGEMENT PLAN

Analytic Services Inc. has developed an excellent network of external support consisting of over 200 private sector companies, academic institutions, DHS Centers of Excellence, think tanks, national laboratories, and “pre-vetted nationally recognized SMEs.” (DHS Comprehensive Review of Analytic Services, 2008.

Management of Subcontractors and Consultants

Under the DHS Contract No. W81XWH-04-D-0011, Analytic Services has operated the Homeland Security Institute FFRDC since 2004. In that capacity, Analytic Services has consulted “widely with representatives from industry, institutions of higher education, nonprofit institutions, other government agencies, and federally funded research and development centers” (Homeland Security Act of 2002, Sec. 312(d), 6 USC 192 2002). We have reached across the broadest possible front to build meaningful, collaborative relationships, creating a community-wide intellectual foundation for homeland security. Under the current HSI contract, we have established agreements with over 200 organizations and subject matter experts including the DHS Centers of Excellence, many private sector companies, academia, national laboratories, think tanks, and other FFRDCs.

Analytic Services has a long history as a prime contractor who subcontracts out work of a size and complexity that demonstrate our capabilities for managing subcontractors and consultants under the HS SAI contract. We routinely compete and manage subcontracted efforts using time tested procedures to reduce subcontractor risk. Our general policies for acquisition of subcontractors may be found in the section entitled, “Subcontracting Policies and Procedures for Analytic Services Inc.” set forth below.

Access to Subcontractors

Prior to submission of this proposal, Analytic Services entered into a teaming agreement with (b) (4) to provide additional, high-level expertise in analytical services (b) (4) is considered a major teaming partner. They will provide dedicated staff to HS SAI.

In addition, we have sought and obtained commitments from a number of subcontractors and consultants that we refer to, in the aggregate, as the Participating Associate Subcontractors (PAS). These subcontractors will be readily available to provide a variety of services to the HS SAI as the need arises from tasks authorized.

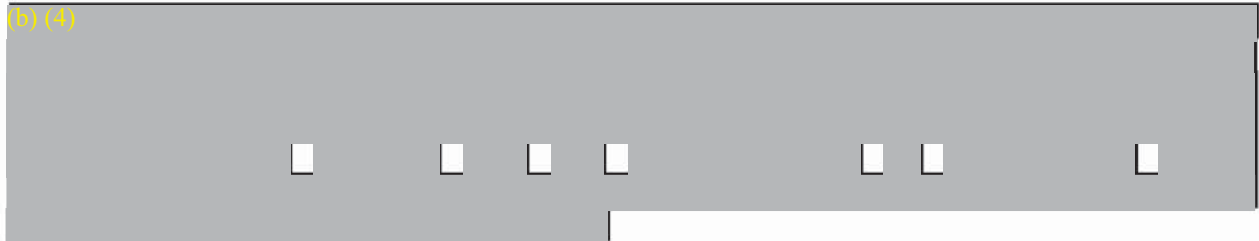
Overall, our method for addressing the availability of quality subcontractors beyond the dedicated staff is founded on our efforts to maintain a broad institutional network of potential subcontractors and consultants. Requests for possible subcontracting will emanate from the planning and organizing process associated with research plan development, thus ensuring direct traceability of subcontracted effort with HS SAI research objectives. Given these requests, we will initiate assessment of the availability of quality subcontractors by first looking at the capabilities of the PAS. If the need can be fulfilled by one of these subcontractors, then we will look no further.

However, if HS SAI has a need for a service or an expert which cannot be provided by one of the PAS, we will seek other subcontractors and consultants who will be able to meet the requirement. For that broader group, we have ready access to subcontractors and consultants who have performed work for Analytic Services’ current FFRDC, the Homeland Security

Institute. Since we have significant experience with that group of subcontractors, we will be able to verify capabilities, performance standards and costs quickly. Analytic Services will initiate assessment of the availability of such qualified subcontractors by searching our expanding and improving Subcontract and Consultant database. At present, a query of the database provides information on organizations or individuals who possess the subject matter expertise and/or skill necessary to meet specific requirements.

As necessary, we will expand our search for other providers through such mechanisms as the Small Business Administration's Dynamic Small Business Search function, and SUB-net, other electronic procurement services, and the outreach programs of the Office of Small and Disadvantaged Business Utilization at DHS. This program provides us with a broad reach across academia and a clear insight into their homeland security capabilities.

(b) (4)



In general, we determine the suitability of using a particular subcontractor by assessment of the subcontractor's past performance, availability of other quality providers to meet the requirements of the research plan, strict avoidance of conflict of interest issues and reasonable proposed costs.

We enable small business concerns to better compete for work awarded by the HS SAI by providing maximum practicable subcontracting opportunities to small business concerns (see Small Business Subcontracting Plan J-11) in accordance with the principles of Public Law 95-507.

Subcontractor Integration

(b) (4)



(b) (4)

Our subcontract management process begins with the selection of subcontractors. Once a subcontractor is selected and approved for work under HS SAI, all required HS SAI assurances and flow down clauses, as well as our management processes are compiled in the subcontract agreement document:

- Statement of Work
- Deliverable Requirements and Schedule
- Performance-Based Metrics
- Labor Category Schedule of Hours
- Labor Category Rates
- Other Direct Cost Estimates.

This information becomes an integral part of our task order response.

Inadequate Performance or Failure to Perform

HS SAI Task Monitoring, implemented by the HS SAI Quality Control program, allows for up-to-date task monitoring of subcontract performance. Subcontractor staff and subcontractor task leaders are integrated into the overall HS SAI task management process.

Performance issues identified in our monitoring and control function will be immediately addressed. Each subcontractor will assign a lead to serve as the focal point for coordination on all subcontractor matters including problem resolution. As an issue is raised concerning the possible performance of a subcontractor, the subcontractor lead will be informed and brought into the resolution process. As required, subcontractor leads will provide the HS SAI leadership with corrective action plans and will maintain a close follow-up to ensure that the issue was resolved. The HS SAI will provide written documentation to the subcontractor describing the problem, the corrective action plan, and the final resolution status. Persistent performance issues will be addressed by the Director with senior levels of the subcontractor's management. Ultimately, subcontractors whose performance is deemed inadequate or fail to perform in accordance with the terms and conditions of their subcontract will have their subcontracts terminated and they will be removed from the HS SAI activity.

No Organizational Conflict of Interest for Subcontractors

Under our current FFRDC contract (HSI) we have established DHS approved processes and forms for ensuring avoidance of conflict of interests. These include subcontractor and consultant certification of no conflicts of interests and non-disclosure agreements. Our in-place DHS approved process has been proven effective as evidenced by the DHS comprehensive review which states that the HSI "COI/NDA ... procedures are exemplary." We will continue to use this process with our subcontractors and consultants. Since we were awarded the original Homeland Security Institute FFRDC contract in 2004, Analytic Services has not tolerated any corporate employee, subcontractor or consultant providing even the appearance of a conflict of interest in their business dealings with DHS and the nation's homeland security enterprise.

(b) (4)

Subcontracting Policies and Procedures For Analytic Services Inc.

A. PURPOSE: To establish guidelines for the issuance, control and administration of subcontracts required under contracts held by Analytic Services Inc.

B. SCOPE: This policy and procedure applies to all contracts issued to Analytic Services Inc. by Federal Government (Federal) and Non-Federal agencies, as well as by subcontracts issued to Analytic Services Inc. by Federal Prime Contractors, which require subcontracting to accomplish the contract effort.

C. DEFINITION: The term "subcontracting" in this statement is defined as formal contractual agreements with participating organizations for the procurement of research, collaboration and/or technical services under a contract.

D. FEDERAL REQUIREMENTS: The terms and conditions of Federal and Non-Federal contracts may require prior approval for the subcontracting of certain types of work. In addition, the Contractor must select Subcontractors on a competitive basis to the maximum extent possible without unduly compromising the objectives and requirements of the contract. The guiding factors in selecting Subcontractors are price or cost, past performance and reputation for high quality and timely work. In any event, the competitive basis utilized should be chosen for its value to accomplish the objectives and meet the requirements of the prime contract. A record of negotiations, inquiries, factors in decisions, etc., must be maintained for audit purposes.

E. PREAWARD SUBCONTRACTING PROCEDURES: When a Subcontractor is proposed to be used for either a proposal or under an existing contract, the following information should be provided to the designated Contract Administrator by the Technical Manager (TM) responsible for the contract:

1. A detailed description of the services to be subcontracted sufficient to issue a Request for Proposal (RFP). This description shall include the contract number under which the subcontracted work will be performed.
2. A list of three (3) or more potential Subcontractors who might reasonably perform the subcontracted effort. If no potential Subcontractors are readily available, the TM shall suggest venues for finding such Subcontractors, if known.
3. If the TM has previously obtained information from one or more Subcontractors capable of performing the subcontracted effort, copies of any such proposals, cost estimates and/ or quotes should be provided.
4. If the proposed Subcontract is sole source, a Sole Source Justification should be prepared. The Technical Manager should prepare the Sole Source Justification and submit it to the designated Contract Administrator.
5. Once the Contract Administrator has the required information described above, the Contract Administrator shall prepare an RFP to obtain competitive proposals for the effort, unless a sole source justification has been approved.
6. For each potential Subcontractor, the Contract Administrator shall verify:
 - (a) that the Subcontractor has proposed in accordance with the Analytic Services' RFP, including acceptance of the type of subcontract to be awarded and the performance of the work specified in the RFP; and

- (b) that a detailed cost or price proposal signed by an official authorized to bind the Subcontractor has been provided.
7. After review of the potential Subcontractors' proposals, the TM and the Contract Administrator will determine an acceptable Subcontractor.
 8. Upon determination of the acceptable subcontractor, the Contract Administrator will seek appropriate approvals from the Federal or Non-Federal contracting personnel in accordance with the contract's terms and conditions. For Federal contracts, the following types of information are typically required:
 - (a) A description of the supplies or services to be subcontracted.
 - (b) Identification of the type of subcontract to be used.
 - (c) Identification of the proposed subcontractor.
 - (d) The proposed subcontract price.
 - (e) The subcontractor's current, complete, and accurate cost or pricing data and Certificate of Current Cost or Pricing Data, if required by other contract provisions.
 - (f) The subcontractor's Disclosure Statement or Certificate relating to Cost Accounting Standards when such data are required by other provisions of this contract.
 - (g) A negotiation memorandum reflecting—
 - (i) The principal elements of the subcontract price negotiations;
 - (ii) The most significant considerations controlling establishment of initial or revised prices;
 - (iii) The reason cost or pricing data were or were not required;
 - (iv) The extent, if any, to which the Contractor did not rely on the subcontractor's cost or pricing data in determining the price objective and in negotiating the final price;
 - (v) The extent to which it was recognized in the negotiation that the subcontractor's cost or pricing data were not accurate, complete, or current; the action taken by the Contractor and the subcontractor; and the effect of any such defective data on the total price negotiated;
 - (vi) The reasons for any significant difference between the Contractor's price objective and the price negotiated; and
 - (vii) A complete explanation of the incentive fee or profit plan when incentives are used. The explanation shall identify each critical performance element, management decisions used to quantify each incentive element, reasons for the incentives, and a summary of all trade-off possibilities considered.
 9. Subsequent to approval of the Subcontractor, the Contract Administrator will award a subcontract to the winning Subcontractor. The subcontract shall set forth appropriate Analytic Services' terms and conditions, along with those terms and conditions which should be flowed down to the Subcontractor from the prime contract document.

F. POSTAWARD SUBCONTRACTING PROCEDURES:

The TM and the Contract Administrator shall work together during the term of the Subcontract to assure that the Subcontractor is meeting the requirements of the subcontract. Such requirements shall include, at a minimum, timely and complete performance of work and provision of reports, as well as proper and timely submission of invoices. The Contract Administrator shall address any and all issues related to Subcontractor's failure to comply with the terms of the subcontract directly with the Subcontractor. If the Subcontractor fails to take appropriate and timely action to comply with the subcontract's requirements, then the TM, the Contract Administrator and appropriate management personnel within Analytic Services' shall consider the potential remedies for Subcontractor's failure to perform and take action based on the best remedy available for the issue and the circumstances.

Strategic Partnership

(b)
(4)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (4)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (4)

[Redacted]

- 1 [Redacted]

- 2 [Redacted]

- 3 [Redacted]

[Redacted]

Meet or Exceed Small Business Subcontracting Plan Goals

We have reviewed the Small Business subcontracting goals provided on page 77 of RFP HSHQDC-09-R-00016 and have every expectation of meeting or exceeding every goal within the first year of the contract. Our latest filing of SF-294/295, Summary of Subcontract Report and Subcontracting Report for Individual Contracts, documents the fact that we make every attempt to include every type of Small Business in our subcontract agreements (see SF-294/295 below).

SUBCONTRACTING REPORT FOR INDIVIDUAL CONTRACTS
(See Instructions on reverse)

OMB No.: 9000-0006
Expires: 11/30/2010

Public reporting burden for this collection of information is estimated to average 9 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the FAR Secretariat (MVR), Federal Acquisition Policy Division, GSA, Washington, DC 20405.

1. CORPORATION, COMPANY, OR SUBDIVISION COVERED			3. DATE SUBMITTED	
a. COMPANY NAME Analytic Services Inc.			October 30, 2008	
b. STREET ADDRESS 2900 South Quincy Street, Suite 800			4. REPORTING PERIOD FROM INCEPTION OF CONTRACT THRU:	
c. CITY Arlington			d. STATE VA	e. ZIP CODE 22206
2. CONTRACTOR IDENTIFICATION NUMBER DUNS: 07-781-5736			<input checked="" type="checkbox"/> REGULAR <input type="checkbox"/> FINAL <input type="checkbox"/> REVISED	
5. TYPE OF REPORT				

6. ADMINISTERING ACTIVITY (Please check applicable box)

<input type="checkbox"/> ARMY	<input type="checkbox"/> GSA	<input type="checkbox"/> NASA
<input type="checkbox"/> NAVY	<input type="checkbox"/> DOE	<input checked="" type="checkbox"/> OTHER FEDERAL AGENCY (Specify)
<input type="checkbox"/> AIR FORCE	<input type="checkbox"/> DEFENSE CONTRACT MANAGEMENT AGENCY	U.S. Department of Homeland Security

7. REPORT SUBMITTED AS (Check one and provide appropriate number)		8. AGENCY OR CONTRACTOR AWARDED CONTRACT		
<input checked="" type="checkbox"/> PRIME CONTRACTOR	PRIME CONTRACT NUMBER W81XWH-04-D-0011	a. AGENCY'S OR CONTRACTOR'S NAME U.S. Department of Homeland Security		
<input type="checkbox"/> SUBCONTRACTOR	SUBCONTRACT NUMBER	b. STREET ADDRESS 301 7th Street, SW		
9. DOLLARS AND PERCENTAGES IN THE FOLLOWING BLOCKS:		c. CITY	d. STATE	e. ZIP CODE
<input checked="" type="checkbox"/> DO INCLUDE INDIRECT COSTS	<input type="checkbox"/> DO NOT INCLUDE INDIRECT COSTS	Washington	DC	20407

TYPE	CURRENT GOAL		ACTUAL CUMULATIVE	
	WHOLE DOLLARS	PERCENT	WHOLE DOLLARS	PERCENT
10a. SMALL BUSINESS CONCERNS (Include SDB, WOSB, HBCU/MI, HUBZone SB, VOSB and Service Disabled VOSB) (Dollar Amount and Percent of 10c.)	\$ 7,301,579	41.0%	\$ 12,247,315	57.0%
10b. LARGE BUSINESS CONCERNS (Dollar Amount and Percent of 10c.)	\$ 10,704,420	59.0%	\$ 9,085,329	43.0%
10c. TOTAL (Sum of 10a and 10b.)	\$ 18,005,999	100.0%	\$ 21,332,644	100.0%
11. SMALL DISADVANTAGED (SDB) CONCERNS (Include HBCU/MI) (Dollar Amount and Percent of 10c.)	\$ 374,236	2.0%	\$ 1,369,770	11.2%
12. WOMEN-OWNED SMALL BUSINESS (WOSB) CONCERNS (Dollar Amount and Percent of 10c.)	\$ 519,100	3.0%	\$ 521,524	4.3%
13. HISTORICALLY BLACK COLLEGES AND UNIVERSITIES (HBCU) AND MINORITY INSTITUTIONS (MI) (If applicable) (Dollar Amount and Percent of 10c.)	\$ -	N/A	\$ -	N/A
14. HUBZONE SMALL BUSINESS (HUBZone SB) CONCERNS (Dollar Amount and Percent of 10c.)	\$ 374,236	3.0%	\$ 33,454	0.3%
15. VETERAN-OWNED SMALL BUSINESS CONCERNS (Including Service-Disabled Veteran-Owned SB) (Dollar Amount and Percent of 10c.)	\$ 374,236	2.0%	\$ 2,824,224	23.1%
16. SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS CONCERNS (Dollar Amount and Percent of 10c.)	\$ 97,489	0.5%	\$ 264,702	2.2%
17. Alaska Native Corporation (ANCs) and Indian Tribes that have not been certified by the Small Business Administration as Small Disadvantage Businesses (Dollar Amount) (See Specific Instructions)	N/A	N/A	N/A	N/A
18. Alaska Native Corporation (ANCs) and Indian Tribes that are not Small Businesses (Dollar Amount) (See Specific Instructions)	N/A	N/A	N/A	N/A

19. REMARKS
Analytic Services Inc. is seeking service-disabled veteran-owned and Hubzone small business concerns to provide services however the small business concerns marketed have not met the quality standards required.

19a. NAME OF INDIVIDUAL ADMINISTERING SUBCONTRACTING PLAN (b) (4)	19b. TELEPHONE NUMBER AREA CODE (b) (4) NUMBER (b) (4)
---	---

SUMMARY SUBCONTRACT REPORT
(See instructions on reverse)

OMB No.: 9000-0007
Expires: 2/28/2010

Public reporting burden for this collection of information is estimated to average 15.9 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the FAR Secretariat (MVR), Federal Acquisition Policy Division, GSA, Washington, DC 20405.

1. CORPORATION, COMPANY, OR SUBMISSION COVERED			3. DATE SUBMITTED	
a. COMPANY NAME Analytic Services Inc.			October 30, 2008	
b. STREET ADDRESS 2900 South Quincy St., Suite 800			4. REPORTING PERIOD:	
c. CITY Arlington			<input type="checkbox"/> OCT 1 - MAR 31	<input checked="" type="checkbox"/> OCT 1 - SEPT 30
d. STATE VA	e. ZIP CODE 22206	YEAR FY 2008		
2. CONTRACTOR IDENTIFICATION NUMBER DUNS: 07-781-5736			5. TYPE OF REPORT	
			<input checked="" type="checkbox"/> REGULAR <input type="checkbox"/> FINAL <input type="checkbox"/> REVISED	

6. ADMINISTERING ACTIVITY (Please check applicable box)

<input type="checkbox"/> ARMY	<input type="checkbox"/> DCMA	<input type="checkbox"/> DOE
<input type="checkbox"/> NAVY	<input type="checkbox"/> NASA	<input checked="" type="checkbox"/> OTHER FEDERAL AGENCY (Specify)
<input type="checkbox"/> AIR FORCE	<input type="checkbox"/> GSA	Department of Homeland Security

7. REPORT SUBMITTED AS (Check one)		8. TYPE OF PLAN	
<input checked="" type="checkbox"/> PRIME CONTRACTOR	<input type="checkbox"/> BOTH	<input checked="" type="checkbox"/> INDIVIDUAL	<input type="checkbox"/> COMMERCIAL PRODUCTS
<input type="checkbox"/> SUBCONTRACTOR		IF PLAN IS A COMMERCIAL PRODUCT PLAN, SPECIFY THE PERCENTAGE OF THE DOLLARS ON THIS REPORT ATTRIBUTABLE TO THIS AGENCY	

9. CONTRACTOR'S MAJOR PRODUCTS OR SERVICES LINES

a	Consulting and Analytic Services	b	
---	----------------------------------	---	--

CUMULATIVE FISCAL YEAR SUBCONTRACT AWARDS
(Report cumulative figures for reporting period in Block 4)

TYPE	WHOLE DOLLARS	PERCENT (To nearest tenth of a %)
10a. SMALL BUSINESS CONCERNS (Include SDB, WOSB, HBCU/MI, HUBZone SB) (Dollar Amount and Percent of 10c.)	\$ 4,257,084	62.50%
10b. LARGE BUSINESS CONCERNS (Dollar Amount and Percent of 10c.)	\$ 3,858,120	47.50%
10c. TOTAL (Sum of 10a and 10b.)	\$ 8,113,204	100.00%
11. SMALL DISADVANTAGED (SDB) CONCERNS (Include HBCU/MI) (Dollar Amount and Percent of 10c.)	\$ 262,158	3.23%
12. WOMEN-OWNED SMALL BUSINESS (WOSB) CONCERNS (Dollar Amount and Percent of 10c.)	\$ 184,267	2.27%
13. HISTORICALLY BLACK COLLEGES AND UNIVERSITIES (HBCU) AND MINORITY INSTITUTIONS (MI) (If applicable) (Dollar Amount and Percent of 10c.)	N/A	N/A
14. HUBZONE SMALL BUSINESS (HUBZone SB) CONCERNS (Dollar Amount and Percent of 10c.)	\$	0.00%
16. VETERAN-OWNED SMALL BUSINESS (VOSB) CONCERNS (Dollar Amount and Percent of 10c.)	\$ 723,038	8.91%
16. SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS CONCERNS (Dollar Amount and Percent of 10c.)	\$ 231,248	2.85%
17. Alaska Native Corporation (ANCs) and Indian Tribes that have not been certified by the Small Business Administration as Small Disadvantage Businesses (Dollar Amount) (See Specific Instructions)	N/A	N/A
18. Alaska Native Corporation (ANCs) and Indian Tribes that are not Small Businesses (Dollar Amount) (See Specific Instructions)	N/A	N/A

19. REMARKS
Analytic Services Inc. does not have a goal for HBCU, hence the N/A designation. We are working to identify other HUBZone and Service Disabled businesses.

20. CONTRACTOR'S OFFICIAL WHO ADMINISTERS SUBCONTRACTING PROGRAM

a. NAME (b) (4)	b. TITLE (b) (4)	c. TELEPHONE NUMBER	
		AREA CODE (b) (4)	NUMBER (b) (4)

21. CHIEF EXECUTIVE OFFICER

a. NAME Dr. Ruth David	c. SIGNATURE (b) (4)
b. TITLE President and CEO	d. DATE October 30, 2008

D

HS Mentor-Protégé Program

We already participate in the Federal government's Mentor-Protégé Program through the Department of Defense. We find the program to be very worthwhile and are in the process of filing an application with DHS to participate in the DHS Mentor-Protégé Program as well.



**Homeland
Security**

Certification and Accreditation Guide

October 1, 2008

Version 5.0

Document Change History

Version	Date	Description
1.0	1/30/2006	Internal draft
2.0	5/5/2006	First public release
3.0	7/31/2007	References to <i>FY 2006 C&A Remediation Plan</i> are deleted throughout. Additional requirements for Chief Financial Officer (CFO)-designated systems are summarized (page 9) Privacy section updated (Task 4) POA&M guidance updated (Task 13) Annual assessment screen shots are updated to include NIST SP 800-53 (pages 66 – 72).
4.0	10/1/2007	Accessibility Compliance Determination requirements added (new Task 5)
5.0	10/1/2008	Complete Revision. Contains a detailed set of processes and tasks for conducting C&A at the Departmental and Component levels.

Table of Contents

1. Introduction.....	1
1.1 Purpose.....	1
1.2 Background.....	1
1.3 Scope.....	2
1.4 Objectives	2
1.5 Audience	3
1.6 Assumptions and Constraints.....	3
1.7 DHS Security Organization	3
1.8 Certification and Accreditation Overview	4
1.8.1 DHS Enterprise Tools	5
1.8.2 Processes and Work Products	5
1.8.3 Roles & Responsibilities.....	6
1.9 C&A Document Repository.....	8
1.10 Governance of C&A Documents in the DHS SELC	9
2. System Identification Process	11
2.1 System Identification Purpose	11
2.2 System Identification Decision Making Factors.....	11
2.3 System Identification Input.....	12
2.4 System Identification Tasks.....	12
2.4.1 Define the System Boundary	13
2.4.2 Process an Inventory Change Request.....	13
2.5 System Identification Output	13
3. Security Characterization Process	17
3.1 Purpose.....	17
3.2 Decision Making Factors	17
3.3 System Security Characterization Tasks.....	18
3.4 FIPS 199 Categorization	18
3.4.1 FIPS 199 Categorization Input.....	18
3.4.2 FIPS 199 Categorization Subtasks.....	19

3.4.3 FIPS 199 Categorization Output.....	19
3.5 Privacy Threshold Analysis	19
3.5.1 PTA Input.....	19
3.5.2 PTA Subtasks.....	20
3.5.3 PTA Output.....	20
3.6 E-Authentication Level Determination.....	20
3.6.1 E-Authentication Input.....	20
3.6.2 E-Authentication Subtasks.....	21
3.6.3 E-Authentication Level Determination Output.....	21
3.7 CFO Designated Financial Systems Determination	21
3.7.1 CFO Designated Financial System Input.....	21
3.7.2 CFO Designated Financial System Subtasks	22
3.7.3 CFO Designated Financial Systems Output	22
3.8 DHS/NIST SP 800-37 Questionnaire in RMS.....	22
3.8.1 Questionnaire Input.....	22
3.8.2 Questionnaire Subtasks	23
3.8.3 Questionnaire Output	24
4. System Security Planning Process.....	27
4.1 System Security Planning Purpose	27
4.2 System Security Planning Decision Making Factors.....	27
4.3 Security Planning Input.....	28
4.4 System Security Planning Tasks	29
4.4.1 SSP Template.....	29
4.4.2 Security Controls Description.....	30
4.4.3 Rules of Behavior	33
4.4.4 Interconnection Security Agreements.....	33
4.5 Security Planning Output.....	34
5. Risk Assessment Process	35
5.1 Risk Assessment Purpose	35
5.2 Risk Assessment Decision Making Factors.....	35
5.3 Risk Assessment Input.....	36
5.4 Risk Assessment Tasks	37
5.4.1 Prepare for Risk Assessment	37

5.4.2	Threat Identification.....	37
5.4.3	Vulnerability Identification.....	37
5.4.4	Determine Susceptibility.....	37
5.4.5	Risk Definition.....	37
5.4.6	Security Control Analysis.....	38
5.4.7	Likelihood Determination.....	38
5.4.8	Impact Analysis	38
5.4.9	Risk Level Determination.....	38
5.4.10	Security Control Recommendations	38
5.4.11	Document the Risk Assessment.....	38
5.5	Risk Assessment Output	38
5.6	CFO Designated Financial Systems.....	39
6.	Contingency Planning Process.....	40
6.1	Contingency Plan Purpose	40
6.2	Contingency Plan Decision Making Factors.....	40
6.3	Contingency Plan Input.....	41
6.4	Contingency Plan Tasks.....	41
6.5	Contingency Plan Output.....	42
7.	Contingency Plan Testing Process.....	43
7.1	Contingency Plan Testing Purpose	43
7.2	Contingency Plan Test Decision Making Factors.....	44
7.3	Contingency Plan Testing Input.....	45
7.4	Contingency Plan Testing Tasks.....	45
7.4.1	Determine Test Exercise Type.....	45
7.4.2	Develop Contingency Plan Test Procedures.....	45
7.4.3	Arrange Test Resources	45
7.4.4	Training.....	45
7.4.5	Schedule CPT.....	46
7.4.6	Execute CPT	46
7.4.7	Test Reporting.....	46
7.5	Contingency Plan Testing Output.....	46
8.	Security Test & Evaluation Planning Process.....	47
8.1	ST&E Planning Purpose	47

8.2	ST&E Planning Decision Making Factors.....	47
8.3	ST&E Planning Process Input	47
8.4	ST&E Planning Tasks.....	47
8.5	ST&E Planning Output.....	48
9.	ST&E Execution Process.....	49
9.1	ST&E Execution Purpose	49
9.2	ST&E Execution Decision Making Factors.....	49
9.3	ST&E Execution Input.....	50
9.4	ST&E Execution Tasks.....	50
9.5	ST&E Execution Output.....	51
9.6	CFO Designated Financial Systems.....	51
10.	Security Assessment Process.....	52
10.1	Purpose.....	52
10.2	Decision Making Factors	52
10.3	Input	52
10.4	Tasks	52
10.4.1	Create the Security Assessment Report	52
10.5	Output	53
11.	Certification Documentation Process.....	54
11.1	Certification Documentation Purpose.....	54
11.2	Certification Documentation Decision Making Factors	54
11.3	Certification Documentation Input	54
11.4	Certification Documentation Tasks	54
11.5	Certification Documentation Output.....	55
11.6	Certification Requirements for CFO Designated Financial Systems	55
12.	Accreditation Process	56
12.1	Accreditation Purpose.....	56
12.2	Accreditation Decision Making Factors	56
12.3	Input	56
12.4	Accreditation Tasks	57
12.4.1	Final Risk Determination and Risk Acceptability	57
12.4.2	Accreditation Package Transmission.....	57
12.4.3	C&A Document Updates	57

12.5 Accreditation Output.....	57
12.6 CFO Designated Financial Systems.....	58
13. Continuous Monitoring and Annual Assessment Process.....	59
13.1 Purpose.....	59
13.2 Decision Making Factors	59
13.3 Input	60
13.4 Tasks	60
13.4.1 Conduct Annual Assessment	60
13.4.2 Annual ISA Review	60
13.4.3 Document System Changes	61
13.4.4 Operating System and Network Patch Management	61
13.4.5 Security Impact Analysis	61
13.4.6 Security Control Selection	62
13.4.7 Security Reporting and Documentation.....	62
13.5 Output	62
Appendix A. Information Assurance Compliance System	64
A.1 TrustedAgent FISMA	65
A.1.1 TAF Content	66
A.1.2 Accessing TAF.....	67
A.2 Risk Management System.....	67
A.2.1 C&A Package.....	67
A.2.2 Accessing RMS.....	68
A.3 DHS Compliance Help Desk	68
A.4 Getting TAF and RMS Accounts.....	68
Appendix B. Certification and Accreditation Document Quality Reviews.....	69
B.1 Component CISO C&A Package Approval.....	69
B.2 OIS Document Review Team	70
B.3 OIS POA&M Review Team	70
B.4 OIS Deep Dive C&A Reviews	70
B.5 DHS Privacy Office	71
Appendix C. List of Attachments.....	72
Acronyms.....	73
Glossary	76

References	78
-------------------------	-----------

List of Figures

Figure 1. DHS Office of Information Security Organization	4
Figure 2. DHS C&A Methodology Process Flow	5
Figure 3. Major Roles in the C&A Process	6
Figure 4. TrustedAgent FISMA: C&A Tab.....	9
Figure 5. DHS Inventory Change Form.....	16
Figure 6. Impact of FIPS 199 Security Categorization Level.....	17
Figure 7. Blank (Sample) C&A Package.....	23
Figure 8. Sample of Completed C&A Package	24
Figure 9. The NIST Risk Management Framework	28
Figure 10. Relationship of ST&E Results and Annual Assessments.....	50
Figure 11. IA Compliance System Policy Implementation	65
Figure 12. System View.....	66
Figure 13. DHS C&A Quality Review Process	69

List of Tables

Table 1. Summary of C&A Processes and Work Products	5
Table 2. Roles and Responsibilities for Major C&A Documents.....	7
Table 3. Roles and Responsibilities for Other C&A Activities	7
Table 4. Security in the DHS SELC	10
Table 5. System Identification Input.....	12
Table 6. Input for the FIPS 199 Categorization Task.....	18
Table 7. Input for the PTA Task	19
Table 8. Input for E-Authentication Task.....	21
Table 9. Input for the DHS/NIST 800-37 Questionnaire Task.....	22
Table 10. SRTM Field Definitions	25
Table 11. Security Planning Process Input	28
Table 12. Security Control Description Examples	31

Table 13. Risk Assessment Process Input.....	36
Table 14. Threat Source Examples	37
Table 15. Contingency Plan Process Input	41
Table 16. Contingency Plan Testing Process Input	45
Table 17. ST&E Planning Process Input	47
Table 18. ST&E Execution Process Input	50
Table 19. ST&E Results Documentation.....	51
Table 20. Security Assessment Process Input.....	52
Table 21. Certification Documentation Process Input.....	54
Table 22. Accreditation Package Process Input.....	56
Table 23. Input for the Continuous Monitoring Process.....	60
Table 24. TrustedAgent FISMA Tab Descriptions.....	66

1. Introduction

Under the authority of the Department of Homeland Security (DHS) Chief Information Officer (CIO), the Chief Information Security Officer (CISO) bears the primary responsibility to ensure compliance with Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB), and all applicable laws, directives, policies, and directed actions on a continuing basis. The organizational mechanism through which the CISO addresses this obligation is called Certification and Accreditation (C&A). This document sets forth the overall methodology for C&A of information systems operated within the Department.

1.1 Purpose

The intention of this *DHS Certification and Accreditation Guide* is to provide a set of enterprise processes used by the Department and its Components to certify and accredit information systems. Understanding these processes is critical to effective estimation and measurement of risk associated with department information systems, and so the Designated Accrediting Authority (DAA) can fully understand the risk to the enterprise prior to giving formal acceptance by granting an Authorization to Operate (ATO).

1.2 Background

Accurate, reliable, and trustworthy information contributes to every aspect of, and is fundamental to, meeting the strategic objectives of the Department. The successful performance of every DHS member's assignment depends upon the availability, correctness, and completeness of information and upon the information system providing that information when and where it is needed. Much of the information essential to the DHS mission also requires confidentiality and privacy protection.

Because of its extended geographic reach, and the large scope of departmental mission areas, DHS assigns the responsibility for assuring the implementation of Information Security and Privacy policies to the program officials who are directly involved with risk acceptance and mitigation decisions. DHS Headquarters and each Component have appointed a CISO to ensure that information security requirements are properly implemented, managed, and enforced and that Departmental and DHS Component information security programs are mutually supporting. Additionally, CISOs work in coordination with Departmental and Component Privacy Officials to leverage available information security mechanisms to support the accomplishment of privacy goals.

Departmental and Component CISOs and System Owners appoint an Information System Security Officer (ISSO) for each system for which the CISO is responsible. Many ISSOs do not report directly to a security organization or to the CISO and their ISSO role may be peripheral to their primary duties. Nevertheless, DHS geographic reach and breadth of mission needs a synergistic environment to operate an effective DHS Information Security Program. The ISSO works in conjunction with the System Owner to ensure that DHS and Component security controls are in place and operating as intended for their respective information systems.

Responsibility for information security across DHS is broadly shared within the security community. The ISSO is a security focal point that provides the links among owners, users, and stakeholders of a particular system. The ISSO proactively supports the correct, complete, and continuous implementation of DHS Security and Privacy policies applicable to Departmental and Component Information Technology (IT) resources and information. The ISSO serves as a liaison and coordinator, with system users and administrators, and numerous stakeholders and supporting personnel. The mission-space of the ISSO is complex and continuously demanding. To support the continuing success of the DHS Information Security Program, successful ISSOs will be constantly involved in directing and managing their system security policy compliance efforts over the complete system life cycle.

1.3 Scope

This DHS C&A Guide explains the processes and relationships among the major steps in the DHS C&A methodology from capturing the initial system concepts to a culminating milestone in achieving formal ATO. The various activities along the way include system identification and security characterization, risk assessment, security planning, security control evaluation, and contingency planning. This guide gives the ISSO helpful instructions for producing the various work products required by those activities. Although Continuous Monitoring is an important aspect of C&A, it is only briefly described in this guide. More detailed and practical guidance for conducting Continuous Monitoring is found in the *DHS ISSO Guide*.¹ The steady-state maintenance of accredited status is managed by the ISSO.

This guide is not intended to be procedural in nature, but rather a process-based method for performing C&A activities across DHS and its Components. However, process definitions are meant to be at a sufficiently low level to assure uniform execution of the various C&A tasks across the Components. This guide draws extensively from existing best practices contained in NIST Special Publication (SP) 800-37, and is intended to serve as a practical adjunct to the DHS *Sensitive Systems Policy Directive 4300A* and *DHS 4300A Sensitive Systems Handbook*. Furthermore, Components may institute and require additional C&A processes that must be followed to address Component-specific security requirements.

1.4 Objectives

The objectives for this guide are to:

- Define the elemental processes comprising C&A.
- Illustrate the relationships between those processes and other DHS enterprise information resource management functions.
- Give the ISSO helpful instruction for producing the work products required for successful C&A completion.
- Provide specific guidelines to help improve consistency of quality across the Components and contractors.
- Advance the level of sophistication in the DHS C&A methodology by including enhancements garnered through continuous improvement.

¹ The DHS ISSO Guide will be published in the first quarter of Fiscal Year 2009.

1.5 Audience

This guide is intended to be read by anyone with a need to understand the C&A process at DHS. The primary audience is the set of managers who have specific C&A duties and support roles detailed in DHS 4300A. Primary audience members include:

- Component CISO
- DAA
- Certifying Official (CO)
- ISSO
- System Owner

The secondary audience is comprised of DHS staff and others who support the efforts of the primary audience in the C&A of DHS systems such as certification agents, and/or certification teams contracted to conduct security testing. In addition, the secondary audience includes those parties responsible for activities within the DHS Systems Engineering Life Cycle (SELC).

1.6 Assumptions and Constraints

Assumptions

- The reader is assumed to have at least a basic level of knowledge in the subject areas of information technology and information security.

Constraints

- This guide pertains only to Sensitive But Unclassified (SBU) systems and does not address the special needs for certifying National Security Systems (NSS).
- This guide does not address the C&A requirements for pilot or developmental information systems.
- Tools are referenced in specific (rather than generic) terms throughout this guide, so as to prevent confusion about which tools are to be used for practical completion of C&A processing.
- Individual DHS Components will be referred to only when such clarity is required.

1.7 DHS Security Organization

Responsibilities for management of DHS Information Security policy are assigned to staff reporting to the CISO. The assignments of distributed responsibility are shown in Figure 1.

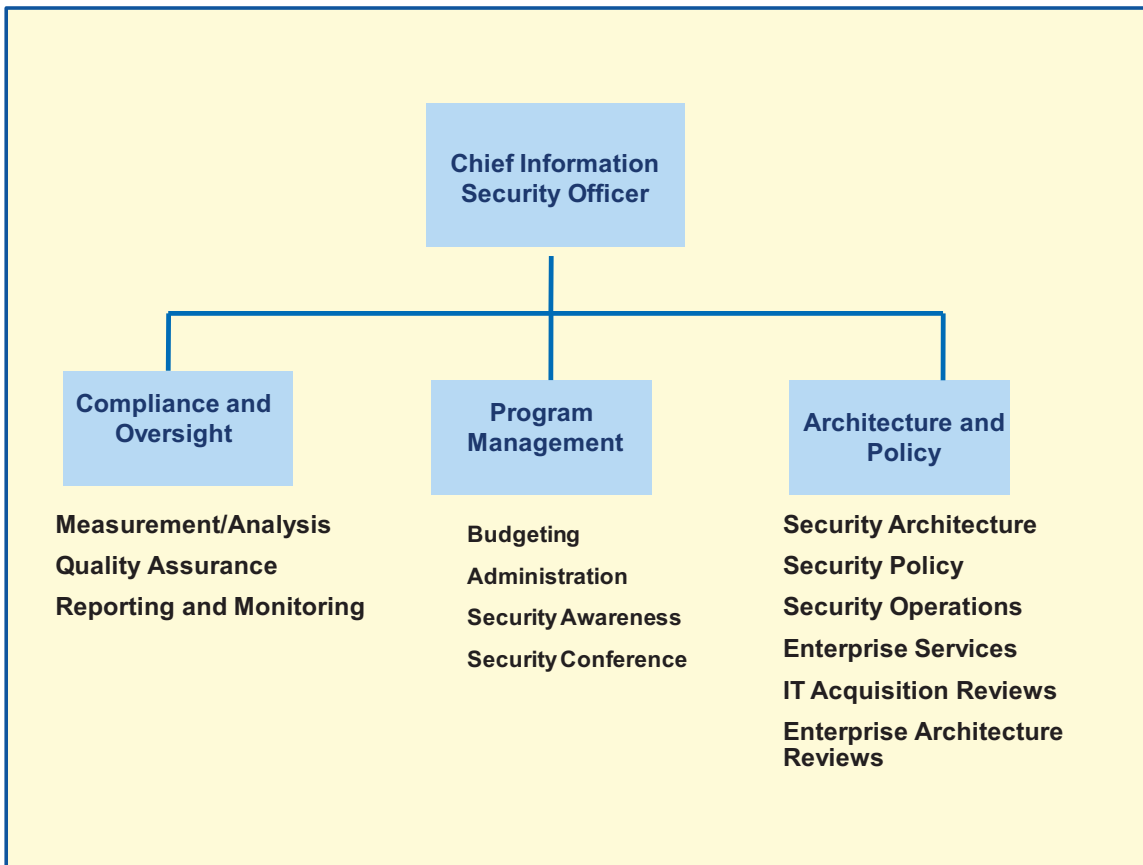


Figure 1. DHS Office of Information Security Organization

1.8 Certification and Accreditation Overview

The DHS C&A Guide includes these distinct processes:

- System Identification
- System Security Characterization
- System Security Planning
- Risk Assessment
- Contingency Planning
- Contingency Plan Testing
- Security Test and Evaluation (ST&E) Planning
- ST&E Execution
- Security Assessment
- Certification Documentation
- Accreditation

Figure 2 illustrates the flow of the DHS C&A processes.

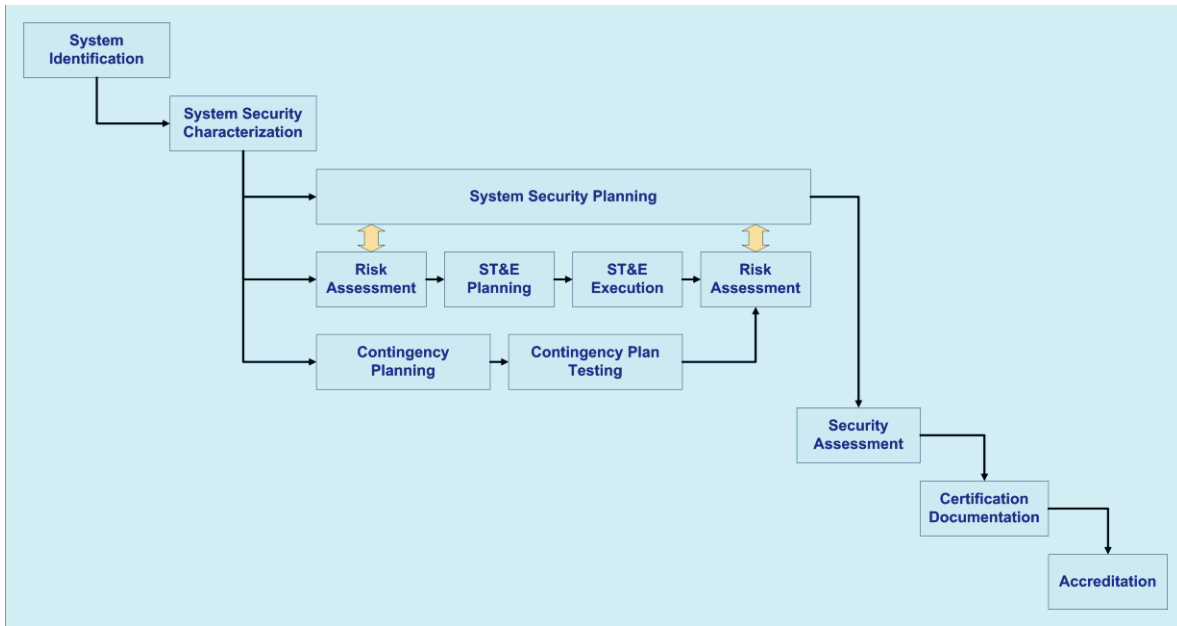


Figure 2. DHS C&A Methodology Process Flow

1.8.1 DHS Enterprise Tools

DHS mandates the use of its enterprise tools to develop and manage C&A documents (Section 3.9.1.1, *DHS Sensitive Systems Policy Directive 4300A*). These tools are TrustedAgent FISMA (TAF) and Risk Management System (RMS).

At a minimum, the Security Requirements Traceability Matrix (SRTM) must be generated using RMS and the RMS templates must be used for producing the C&A documents. TAF is used to track C&A documents for FISMA reporting and monthly scorecards developed by the CISO. Appendix A provides additional information about TAF and RMS.

It is intended that RMS be used for creating, updating, and managing C&A documents. In some cases, it may not be feasible to access the enterprise RMS tool and therefore manual download and subsequent upload of C&A documents may be necessary. However, this manual method is highly discouraged, as it reduces the ability of DHS to accurately reflect departmental adherence to FISMA across the enterprise.

1.8.2 Processes and Work Products

Table 1 provides a summary of the DHS C&A processes and work products.

Table 1. Summary of C&A Processes and Work Products

Process	Work Products
System Identification	<ul style="list-style-type: none"> • Certification boundary diagram • System designation as a General Support System (GSS) or Major Application (MA) • Unique System Number in the DHS IT System Inventory • List of interconnecting systems • List of subsystems and minor applications

Process	Work Products
System Security Characterization	<ul style="list-style-type: none"> • Determination of the Impact level (high, moderate, low) for the confidentiality, integrity, and availability security objectives for information systems and FIPS 199 Workbook • Determination by Privacy Officer whether the system is a Privacy Sensitive System and PTA • E-Authentication level determination and Workbook • Determination by the Chief Financial Officer (CFO) whether a system is a CFO Designated Financial System • DHS/NIST SP 800-37 Questionnaire in RMS • SRTM
System Security Planning	<ul style="list-style-type: none"> • Updated SRTM • System Security Plan (SSP) • Rules of Behavior (ROB) • User Access Request Forms & Procedures • Signed Interconnection Agreements, Memoranda of Understanding (MOU), Memoranda of Agreement (MOA) • Privacy Impact Assessment (PIA), if required
Risk Assessment	<ul style="list-style-type: none"> • Risk Assessment (RA)
Contingency Planning	<ul style="list-style-type: none"> • System Contingency Plan (CP) • CP Checklist • Plan of Action and Milestones (POA&M) updated for CP weaknesses
Contingency Plan Testing	<ul style="list-style-type: none"> • Contingency Plan Test (CPT) Results
Security Test and Evaluation Planning	<ul style="list-style-type: none"> • ST&E Plan
Security Test and Evaluation Execution	<ul style="list-style-type: none"> • ST&E Results
Security Assessment	<ul style="list-style-type: none"> • Security Assessment Report (SAR)
Certification Documentation	<ul style="list-style-type: none"> • Accreditation Package, including <ul style="list-style-type: none"> • SSP • SAR • POA&M • Accreditation Decision Letter – DRAFT
Accreditation	<ul style="list-style-type: none"> • Accreditation Decision Letter (ATO Letter)

1.8.3 Roles & Responsibilities

Figure 3 illustrates the major roles in the conduct of C&A.

FIGURE UNDER DEVELOPMENT

Figure 3. Major Roles in the C&A Process

These staff members (with potential contractor assistance as certification agents/certification teams) produce the primary C&A documents:

- Risk Assessment (RA)
- System Security Plan (SSP)
- ST&E Plan
- Security Assessment Report (SAR)
- Contingency Plan (CP)
- Contingency Plan Test (CPT) Results
- Plan of Action and Milestones (POA&M)
- Accreditation Decision Letter

These staff Create (C), Review (R), Update (U), Approve (A), and/or Approve and Sign (A/S) the documents as illustrated in Table 2.

Table 2. Roles and Responsibilities for Major C&A Documents

ROLE	RA	SSP	ST&E Plan	SAR	CP	CPT Results	POA&M*	ATO Letter
DAA	R	A/S	R	R	R	R	R	A/S
Component CFO (financial systems only)	R	R	R	R	R	R	R	A/S
Component CISO	R	A/S	R	R	R	R	R	R
ISSO	C/U	C/U	C/U	C/U	C	C	C	
System Owner	R	A/S	A	A	A	A	R	R
CO	R	R	A	A	A	A	R	C/U

Legend: C = Create
R = Review
U = Update
A = Approve
A/S = Approve and Sign

*Component CISO may be required to approve some POA&M items as required by the current *Information Security Performance Plan*.

In addition to the major C&A documents, there are other tasks needed to complete the DHS C&A process. The roles and responsibilities for other tasks in the DHS C&A Guide are summarized in Table 3.

Table 3. Roles and Responsibilities for Other C&A Activities

Role	System Boundary	FIPS 199	E-auth	CFO System	PTA	PIA	SORN
DAA	R	A	R	R	R	R	R
Inventory Team	A						
Component CISO	R	A	R	A	R	R	R
Component CFO				A/S			
Privacy Office			A		A/S	A/S	C
Component Privacy Officer					R/U	R/U	R
ISSO	C	C	C	C	C	C	R

Role	System Boundary	FIPS 199	E-auth	CFO System	PTA	PIA	SORN
System Owner	A	A	A	R	R	R	R
CO	R	R	R	R	R		

Legend: C = Create
R = Review
U = Update
A = Approve
A/S = Approve and Sign

1.9 C&A Document Repository

Upon completion and approval by the System Owner, CO, and DAA, as appropriate, the ISSO uploads all C&A documents to the C&A Tab in TAF. Figure 4 contains screen shots of the C&A Tab and the locations where C&A documents are to be uploaded.

In Figure 4, the blue boxes represent security documents related to the DHS C&A process and the green boxes represent documents under the purview of the DHS Privacy Officer.

C&A documents can be uploaded at any time. However, the Office of Information Security (OIS) Review Team (described in Appendix B) will only review complete C&A packages. The OIS Document Review Team will begin reviewing C&A security documents when the:

- Last C&A Date is updated in the TAF C&A Tab
- Component CISO approves all C&A documents in the TAF C&A Tab
- Next C&A Date is changed to equal the Current C&A Expiration in the System Development Life Cycle (SDLC) Status box in the TAF Identification Tab.

The screenshot displays the TrustedAgent FISMA: C&A Tab interface, which is organized into several sections, each with a form and a table of artifacts. The sections are:

- Annual Assessment:** Form with fields for Annual Assessment Status (Completed), Last Annual Assessment Date (12/21/2007), and Next Annual Assessment Date (12/21/2008). Table with 1 artifact: C&A Artifact, uploaded 10/03/2006.
- Certification and Accreditation:** Form with fields for C&A Status (ATO), Governing Policy (NIST 800-37), and C&A Initiation Date (03/09/2005). Table with 1 artifact: C&A Artifact, uploaded 10/03/2006.
- Risk Assessment:** Form with fields for RA Status (Completed), Last RA Date (10/03/2008), and RA Initiation Date (10/03/2009). Table with 1 artifact: Risk Assessment Artifact, uploaded 10/06/2006.
- System Security Plan:** Form with fields for SSP Status (Completed), Completion Date (03/09/2005), and SSP Initiation Date (10/03/2006). Table with 1 artifact: SSP Artifact, uploaded 10/06/2006.
- Contingency Plan:** Form with fields for CP Status (Tested), CP Initiation Date (03/09/2005), Last CP Completion Date (10/03/2006), and Next CP Revision Date (10/03/2009). Table with 3 artifacts: Contingency Plan Artifact (uploaded 10/06/2006), Tested Contingency Plan Artifact (uploaded 10/10/2006), and Security CONOPS (uploaded 10/10/2006).
- ST&E Plan:** Form with fields for ST&E Plan Status (Completed), ST&E Plan Initiation Date (10/03/2006), and ST&E Plan Completion Date (10/03/2009). Table with 2 artifacts: ST&E Test Plan (uploaded 10/06/2006) and Security Assessment Report (uploaded 10/06/2006).
- SAR:** Form with fields for SAR Status (Completed), SAR Initiation Date (10/03/2006), and SAR Completion Date (10/03/2009). Table with 1 artifact: SAR Artifact, uploaded 10/06/2006.
- SRTM:** Form with fields for SRTM Status (Completed), SRTM Initiation Date (10/03/2006), and SRTM Completion Date (10/03/2009). Table with 1 artifact: SRTM Artifact, uploaded 10/06/2006.
- E-Auth:** Form with fields for E-Auth Status (Completed), E-Auth Initiation Date (10/03/2006), and E-Auth Completion Date (05/06/2006). Table with 1 artifact: E-Authentication Artifact, uploaded 10/06/2006.
- PTA:** Form with fields for PTA Status (Completed), PTA Initiation Date (07/06/2006), and PTA Completion Date (09/07/2006). Table with 1 artifact: PTA Artifact, uploaded 09/07/2006.
- PIA:** Form with fields for PIA Status (Not Applicable), PIA Initiation Date (TBD), and PIA Completion Date (TBD). Table with 1 artifact: PIA Artifact, uploaded 10/06/2006.
- SORN:** Form with fields for SORN Status (Completed), SORN Initiation Date (12/29/2006), and SORN Completion Date (DHS /ALL-004). Table with 1 artifact: System of Records Notice, uploaded 08/22/2007.
- FIPS 199:** Form with fields for FIPS 199 Status (Yes), FIPS 199 Initiation Date (10/03/2006), and FIPS 199 Completion Date (10/03/2006). Table with 2 artifacts: FIPS 199 (uploaded 10/06/2006) and ISSO Letter (uploaded 05/11/2008).
- ISSO Letter:** Form with fields for ISSO Letter Status (Completed), ISSO Letter Initiation Date (10/03/2006), and ISSO Letter Completion Date (10/03/2006). Table with 1 artifact: ISSO Letter, uploaded 10/06/2006.

Figure 4. TrustedAgent FISMA: C&A Tab

1.10 Governance of C&A Documents in the DHS SELC

Ideally, the C&A documents are produced in the early stages of the DHS SELC. However, if the C&A documents are not initiated early in the SELC, it is likely that the documents will be more costly to produce. Table 4 shows where and when C&A documents should be created, updated, and finalized throughout the DHS SELC.

Table 4. Security in the DHS SELC

SELC Artifact	Governing Authority	Planning	Requirements Definition	Design	Development	Integration & Test	Implementation	Operations & Maintenance	Disposition
Privacy Threshold Analysis (PTA)	DHS Privacy Office	C/F							
SRTM	DHS CISO		C	U	F				
POA&M	DHS CISO		C	U		U	F		
SSP	DHS CISO		C	U	U	U	F		
CP	DHS CISO		C	U		F			
RA	DHS CISO		C	U		F			
ST&E Plan	DHS CISO		C		F				
Interconnection Security Agreement (ISA)	DHS CISO			C/F					
SAR	DHS CISO					C/F			
Accreditation Package	DHS CISO					C/F			
Accreditation Decision Letter	DHS CISO						C/F		
C&A Updates (every three years or when major change is made)	DHS CISO							U	U

Legend: C = Create
 U = Update
 F = Finalize

2. System Identification Process

System Identification is the first process of the DHS C&A Guide. It establishes a well defined information system boundary and an understanding of the mission and/or business functions of the information system. DHS implements a centralized system inventory process to facilitate consistent and repeatable interpretation of federal guidance related to system boundary definition and system identification. The DHS inventory process is managed by the DHS Inventory Management Team under the direction of the CISO.

Each DHS organization has an official system inventory that is maintained in TAF. In order to add a system to a Component's official inventory, the Inventory Change Management process is implemented. The System Identification Process should occur in the early stages of the system life cycle. However, its completion is mandatory for systems in the Development stage of the system life cycle.

2.1 System Identification Purpose

The purpose of the System Identification Process is to focus security engineering and the C&A process on a specific set of information system assets to ensure that the principles of the DHS Information Security Program are achieved. These principles are:

- Account for all information system assets as part of a General Support System (GSS) or Major Application (MA).
- Account for all interconnections to an information system.
- Ensure that all DHS systems are certified and accredited and that a DAA weighs mission requirements against operational risk.
- Document life-cycle system security in the SSP and assign responsibility for active management of the SSP to the system's ISSO:
 - The System Owner must be identified and named.
 - An ISSO must be named for every system.
 - An ISSO may be a Government employee or contractor.
 - An ISSO must report directly to a System Owner and indirectly to a Component CISO.
 - For DHS CFO Designated Financial Systems, ISSO duties shall be assigned to a dedicated ISSO, and no other significant collateral duties shall be assigned to them.
- All DHS systems must be associated with a specific IT investment or funding source.

2.2 System Identification Decision Making Factors

Accreditation boundaries that are unnecessarily expansive (i.e., including too many hardware, software, and firmware components) make the security C&A process unwieldy and complex. Boundaries that are unnecessarily limited (i.e., including too few hardware, software, and firmware components) increase the number of C&As that must be conducted and thus drive up the total cost of security for the Component.

2.3 System Identification Input

System identification depends on many sources of information as shown in Table 5. Titles of formal documentation are italicized.

Table 5. System Identification Input

Input	Source
System Name and Title	System design documents
System Description	System design documents
Organization Responsible for the System	System design documents
Organization providing Funding for the System	System design documents
System Points of Contact (e.g., System Owner, ISSO)	System design documents
High Level System Design Information	System design documents
System Network Diagrams	System design documents
Definition of System Users and Administrators (location, access types, clearances)	System design documents
Operational Status of the System	System design documents
Hardware/Software List	System design documents
OMB 300/53 Unique Project Identifier Code (if applicable)	System design documents
DHS Investment Name (if applicable)	System design documents
System Interconnections	System design documents
<i>DHS FISMA Inventory Methodology</i>	DHSONline/Components/Management/CIO/CISO FISMA.inventory@dhs.gov
<i>Inventory Change Request Form</i>	FISMA.inventory@dhs.gov

2.4 System Identification Tasks

Identifying system boundaries in an accurate and consistent manner is critical to the integrity of the DHS C&A process. DHS considers a system to be a composite of people, procedures, materials, tools, equipment, hardware, and software operating in a specific environment to achieve a specific mission requirement. The ultimate objective is to group system elements in a consistent manner throughout the Department, while enhancing security, facilitating risk management, and taking into account mission, budgetary and business requirements.

An information system can be defined by its support of Departmental or Component mission objectives, interfaces, networks, security categorization, functional requirements, and operating environment. The system may be simple, very complex with many subsystems, or reside in several locations with similar operating environments. Defining a system boundary should be a Component-level activity including careful negotiation among all key participants, taking into account the mission/business requirements of the agency, technical considerations with respect to information security, and the programmatic costs to the agency.

The System Identification Process consists of the tasks described below.

2.4.1 Define the System Boundary

The Inventory Management Team publishes and maintains a methodology document, *DHS FISMA Inventory Methodology* which is located on the DHS CISO web site. The methodology outlines the guidelines for identifying systems and system boundaries along with several case studies. The System Owner, CISO, and ISSO work with the DHS Inventory team to define the system boundary. The following characteristics are used to determine the system boundary.

The assets comprising the system:

1. are under the same direct management control;
2. support the same mission function, including the sites at which the assets are deployed;
3. have a common set of operational characteristics and security needs;
4. reside in a common operating environment.

In situations where it is difficult to determine whether system elements have the same management control and function/mission objective, budgetary control will be the deciding factor in determining accreditation boundaries. For an elaboration of this brief summary, refer to the *DHS FISMA Inventory Methodology*.

2.4.2 Process an Inventory Change Request

The second task is to complete an Inventory Change Request Form, which is found in the *DHS FISMA Inventory Methodology*. A copy of the DHS Inventory Change Request Form is provided in Figure 5.

Submission of an Inventory Change Request is an important part of the System Identification Process and the DHS C&A methodology. If the system is not part of the official inventory, unknown risks to the confidentiality, integrity, and availability of DHS information cannot be managed by the system owner and the Component CISO.

NOTE: An Inventory Change Request Form should be submitted whenever there is a change in the system's SELC status. However, it is crucial to submit a Change Request Form when the system goes into Operational status (See Table 4).

2.5 System Identification Output

The following are output from the System Identification process:

- Accreditation boundary diagram
- System designation as a GSS or MA
- List of interconnecting systems
- List of subsystems and minor applications
- A unique System Number in TAF

The System Number also identifies the Component and the system type (Major Application, General Support System, Type Accredited System, Minor Application, and Subsystem). The System Number includes a **System ID**, a unique, five digit number which is assigned to a system when it is added to the inventory. The five digit number is never reused, that is, when a system is placed in disposal, the System ID number is retired.

DHS FISMA System Inventory Change Request Form

Requestor Information

Name		Title		DHS Component	
Email		Telephone			

Change Type

<input type="checkbox"/> System	<input type="checkbox"/> Program	<input type="checkbox"/> Responsible Org	<input type="checkbox"/> Site
<input type="checkbox"/> Modify Existing	<input type="checkbox"/> Add New*	<input type="checkbox"/> Delete Existing**	

System Information

System Name*		System ID	
System Purpose/General Description*			

Change Request (DHS HQ Approval Required)

	Change		Reason For change
Component*			
System Classification*	<input type="checkbox"/> GSS	<input type="checkbox"/> Minor App	
	<input type="checkbox"/> MA	<input type="checkbox"/> Subsystem	
Major Information System*	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
SELC Status*	<input type="checkbox"/> Initiation	<input type="checkbox"/> Operational	
	<input type="checkbox"/> Development	<input type="checkbox"/> Modification	
	<input type="checkbox"/> Implementation	<input type="checkbox"/> Disposal	
Inventory System*	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
National Security System*	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Contractor Operation/Facility*	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Program*			
Responsible Org*			
System Classification*	<input type="checkbox"/> Unclassified	<input type="checkbox"/> Confidential	
	<input type="checkbox"/> SBU	<input type="checkbox"/> Secret	
		<input type="checkbox"/> Top Secret	
Financial System*	<input type="checkbox"/> Non-Financial		
	<input type="checkbox"/> Financial		
	<input type="checkbox"/> Financial- Mixed		
Number of Users			

*All asterisked fields are required for new systems.

**Deletion of Operational Systems Requires Letter of Disposal signed by DAA

UPI Code*		
Capital Planning Information	Investment Name:	
	Investment Portfolio:	

System Location*
<p>Please list physical locations, such as a datacenter or field office, where the system resides and physical security controls are implemented. Please indicate whether the site is Contractor Owned Contractor Operated, Government Owned Contractor Operated or Government Owned Government Operated.</p> <ul style="list-style-type: none"> •

System Interconnection Data*
<p>Please identify all interconnections between the information system and all other systems or networks, including those not operated by or under the control of DHS or the Component. For DHS Owned Systems: Please indicate the system name, unique ID For Non-DHS Owned Systems: Please indicate the system name, organization name, and point of contact</p> <ul style="list-style-type: none"> •

Internet Connectivity*
<p>Please identify all important connections: Types (like DSL, T1, DS3, PPP)</p> <ul style="list-style-type: none"> •

*All asterisked fields are required for new systems.

**Deletion of Operational Systems Requires Letter of Disposal signed by DAA

Subsystems (Please list any subsystems requiring subsequent modification)			
Name	System ID	Location	Description

Notes
<ul style="list-style-type: none">

*All asterisked fields are required for new systems.

**Deletion of Operational Systems Requires Letter of Disposal signed by DAA

Figure 5. DHS Inventory Change Form

3. Security Characterization Process

The second process in the DHS C&A methodology is to conduct a thorough analysis of the system mission and the types of information processed, stored, and transmitted by the information system,

3.1 Purpose

The purpose of this process is to characterize the type of information that will be processed, stored, and transmitted by the information system so that the appropriate security controls to be selected, tested, and implemented are identified.

3.2 Decision Making Factors

The categorization steps described in the *DHS Sensitive Policy Directive 4300A* should be followed. Errors in the initial categorization process can result in either an over-specification or under-specification of the security controls. Over-specification of security controls means that the organization is expending more effort and resources on information security than is actually necessary and potentially taking resources away from other mission/business areas with greater protection needs. Under-specification of security controls means that selected mission/business processes may be at greater risk due to potentially insufficient protection measures allocated for the information systems supporting those processes.² Figure 6 illustrates the impact of the Federal Information Processing Standards (FIPS) 199 Categorization on the number of NIST SP 800-53 controls and enhancements that need to be included in the SSP.

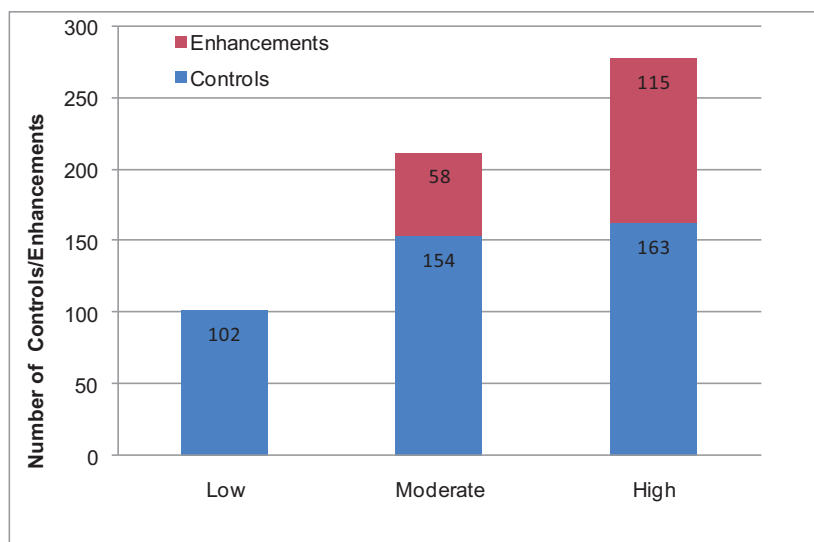


Figure 6. Impact of FIPS 199 Security Categorization Level

Ideally, the security categorization results for an individual system should be compared with similar Component systems to gain confidence in their accuracy. The comparison should be

² NIST SP 800-39, *Managing Risk From Information Systems: An Organizational Perspective*, Second Public Draft, April 2008.

completed at the Component-level and conducted by the Component CISO, System Owners, and DAAs.

3.3 System Security Characterization Tasks

To identify the full spectrum of the characteristics of the information processed by a system, the DHS security categorization process consists of five tasks. The first four tasks are not sequential and can be completed in any order:

- FIPS 199 Categorization
- Privacy Threshold Analysis (PTA)
- E-Authentication Level Determination
- CFO Designated Financial System Determination
- DHS/NIST SP 800-37 Questionnaire in RMS

The following sections describe the input, subtasks, and output for each of the System Security Characterization Process tasks.

3.4 FIPS 199 Categorization

In the FIPS 199 Categorization task, the impact levels (low, moderate, or high) for the information system security objectives (confidentiality, integrity, and availability) are determined. DHS has tailored the FIPS 199 “high water mark” approach to assign, different impact levels to each security objective. This means, for example, that for a system with low impact rating for availability, a high impact rating for integrity, and low impact rating for confidentiality it is not required to implement all high controls across the board. Rather the controls should be implemented according to their respective impact ratings (i.e., implemented at the high level for integrity controls and implemented at the low level for the confidentiality and availability controls).

3.4.1 FIPS 199 Categorization Input

Table 6 summarizes the input for the FIPS 199 Categorization task.

Table 6. Input for the FIPS 199 Categorization Task

Input	Source
<i>DHS Information Security Categorization Guide</i>	DHSOnline/Components/Management/CIO/CISO dhsinfosechelpdesk@dhs.gov
<i>DHS FIPS 199 Workbook</i>	DHSOnline/Components/Management/CIO/CISO dhsinfosechelpdesk@dhs.gov
Data Processed by the System System Requirements System/Security Concept of Operations Definition of System Users and Administrators (location, access types, clearances)	System acquisition planning documents System design documents System Owner

The DHS FIPS 199 Workbook is used to complete this task. The Workbook tailors federal-level guidance to the DHS environment. The recommended impact levels contained in the workbook are extracted from *Guide for Mapping Types of Information and Information Systems to Security Categories*, NIST SP 800-60, to correlate with the DHS Business Reference Model (BRM) elements.

3.4.2 FIPS 199 Categorization Subtasks

The subtasks are:

1. Following the instructions in the *DHS Information Security Categorization Guide*, complete the *DHS FIPS 199 Workbook* based on the types of information processed by the information system.
2. Obtain consensus on the *DHS FIPS 199 Workbook* from the System Owner and the DAA to prevent rework.

3.4.3 FIPS 199 Categorization Output

The following are output from the FIPS 199 Categorization task:

- Impact levels (high, moderate, low) for the confidentiality, integrity, and availability security objectives for the information system
- FIPS 199 document (workbook or summary sheet) uploaded to TAF

3.5 Privacy Threshold Analysis

The PTA determines if an information system involves the collection, maintenance, or dissemination of Personally Identifiable Information (PII). PTA is conducted as part of new information system development or whenever an existing system is significantly modified (*DHS Sensitive Systems Policy 4300A*, Section 3.14.2). PII is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the U.S.

3.5.1 PTA Input

Table 7 identifies the required input for the PTA task.

Table 7. Input for the PTA Task

Input	Source
PTA Template	www.dhs.gov/privacy pia@dhs.gov
Type of Project	System design documents
Description of Project and Purpose	System design documents
If the project is related to infrastructure, description of the communications log communication logs maintained	System design documents
Type of information collected about individuals	System design documents
Whether the system can be remotely accessed	System design documents
Whether PII can be physically transported outside	System design documents

Input	Source
the Department's physical perimeter	

3.5.2 PTA Subtasks

The DHS Privacy Office owns the overall privacy determination and assessment process. The DHS Privacy Office is responsible for designating Privacy Sensitive Systems. The Privacy Office uses the PTA Template to determine if a system processes PII and if a Privacy Impact Assessment (PIA) is required. The subtasks are:

1. ISSO completes the PTA template with the assistance of the Component Privacy Point of Contact (PPOC).
2. System Owner reviews and approves the PTA.
3. PTA is uploaded into TAF.
4. DHS Privacy Office (www.dhs.gov/privacy or pia@dhs.gov) determines whether a system is a Privacy Sensitive System.
5. DHS Privacy Office uploads approved PTA into TAF.

3.5.3 PTA Output

The following are output from the PTA task:

- Determination by the DHS Privacy Office that a system is a Privacy Sensitive System.
- PTA uploaded by the DHS Privacy Officer to TAF.
- If the DHS Privacy Office determines the system processes PII:
 - The confidentiality security objective for the system must be assigned an impact level of at least moderate (*DHS Sensitive Systems Policy 4300A*, Section 3.14).
 - Additional security controls are automatically generated for the SSP by RMS. (These controls are identified in *DHS 4300A Sensitive Systems Handbook*, Attachment S, *Compliance Framework NIST SP 800-53 Controls for Privacy Systems*.)
 - A PIA must be completed and approved by the Privacy Office.

3.6 E-Authentication Level Determination

E-Authentication Level Determination provides secure on-line transactions, eliminating the need for separate processes for the verification of identity and electronic signatures. Understanding the E-Authentication requirements provides information for the Risk Assessment process and assists with the identification of certain security controls for the system.

3.6.1 E-Authentication Input

Table 8 identifies the input for the E-Authentication task.

Table 8. Input for E-Authentication Task

Input	Source
<i>E-Authentication Workbook</i>	DHSONline/Components/Management/CIO/CISO dhsinfosechelpdesk@dhs.gov
<i>DHS Information Security Categorization Guide</i>	DHSONline/Components/Management/CIO/CISO dhsinfosechelpdesk@dhs.gov
System Description System Purpose Data processed by the information system	System Owner System design documents

3.6.2 E-Authentication Subtasks

The subtasks are:

1. Following the guidance in the DHS Information Security Categorization Guide, complete the *E-Authentication Workbook*.
2. Forward the *E-Authentication Workbook* to the System Owner for approval.
3. As part or reauthorization, the e-authentication status must be reviewed and updated.

3.6.3 E-Authentication Level Determination Output

The following are output from the E-authentication Level Determination:

- Completed *E-Authentication Workbook* is uploaded to TAF.
- The correct authentication level is updated in TAF.
- The technologies supporting the e-authentication level must be concisely described in the NIST SP 800-53 IA-2 control, User Identification and Authentication, in the SSP.
- Technical requirements described in NIST SP 800-63, *Electronic Authentication Guideline*, are implemented at the appropriate assurance level for those systems for which e-authentication requirements apply.

3.7 CFO Designated Financial Systems Determination

DHS systems designated by the CFO as Financial Systems must comply with the Office of Management and Budget (OMB) Circular A-123, Management’s Responsibility for Internal Control, Appendix A.

3.7.1 CFO Designated Financial System Input

The DHS CFO makes the final determination as to whether a system is a financial system using the following criteria from OMB Circular A-123, Appendix A:

- A **financial system** is an information system, comprised of one or more applications, that is used for any of the following:
 - Collecting, processing, maintaining, transmitting, and reporting data about financial events
 - Supporting financial planning or budgeting activities

- Accumulating and reporting cost information
- Supporting the preparation of financial statements,
- A **mixed financial system** is a system that supports both financial and non-financial functions of an organization.

3.7.2 CFO Designated Financial System Subtasks

The subtasks are:

1. The Component ISSO identifies systems as financial systems or mixed financial systems using the criteria identified in Section 3.7.1.
2. The Component CISO approves the systems categorization as financial of mixed financial systems.
3. The Component CISO submits the list of financial systems and mixed financial systems to the CFO.
4. The CFO reviews the Component submittals.
5. The CFO publishes the list of CFO Designated Financial Systems during the fourth quarter of every fiscal year.
6. The CFO provides the list of CFO Designated Financial Systems to the Component CISOs and the Inventory Team.

3.7.3 CFO Designated Financial Systems Output

If the CFO designates a system as a financial system, the ISSO must ensure that:

- All categorization controls for the system are designated as at least “moderate”. If warranted by a risk based assessment, all security objectives should be elevated to “high.”
- Requirements specified in *DHS Sensitive Systems Policy Directive 4300A*, Section 3.5, are implemented.
- Requirements specified *DHS 4300A Sensitive System Handbook*, Attachment R, *Compliance Framework for CFO Designated Financial Systems*, are implemented.

3.8 DHS/NIST SP 800-37 Questionnaire in RMS

Once the system boundary is defined and the other Security Categorization Process tasks are completed, RMS must be accessed to run the DHS/NIST 800-37 Questionnaire: Phase 1.

3.8.1 Questionnaire Input

Table 9 identifies the input for the DHS/NIST SP 800-37 Questionnaire task.

Table 9. Input for the DHS/NIST 800-37 Questionnaire Task

Input	Source
RMS Account	Component CISO must request accounts through dhsinfosechelpdesk@dhs.gov
RMS Users Guide	RMS Log-In Page

Input	Source
Inventory Information	System Inventory Change Request Form
Security Categorization Results	DHS FIPS 199 Workbook DHS Chief Privacy Officer (CPO) Privacy System designation E-Authentication Workbook CFO Financial System Designation
Technology included in System Boundary (e.g., PBX switch, Voice Over Data Network, Voice Over IP Facsimile equipment, Video Teleconferencing equipment, Wireless, PEDs, workstations, laptops, PKI, RFID)	System Owner System design documents
Network security issues (i.e., remote access, network monitoring, external connections, boundary protection, Internet usage, e-mail, vulnerability scanning)	System Owner System design documents
DHS Security Configuration Guides requirements (Windows 2000 Windows Vista, HP-UX, Windows 2003/XP, Linux, Solaris, SQL) ³	System Owner System design documents
Contractors and/or Outsourced Operations	System Owner System design documents

3.8.2 Questionnaire Subtasks

Following the guidance in the RMS Users Guide, the questionnaire should be completed and the C&A Package for the system generated. (Guidance for filling out the templates is contained in the appendices to this document).

1. Create folder. A blank C&A Package is illustrated in Figure 7.

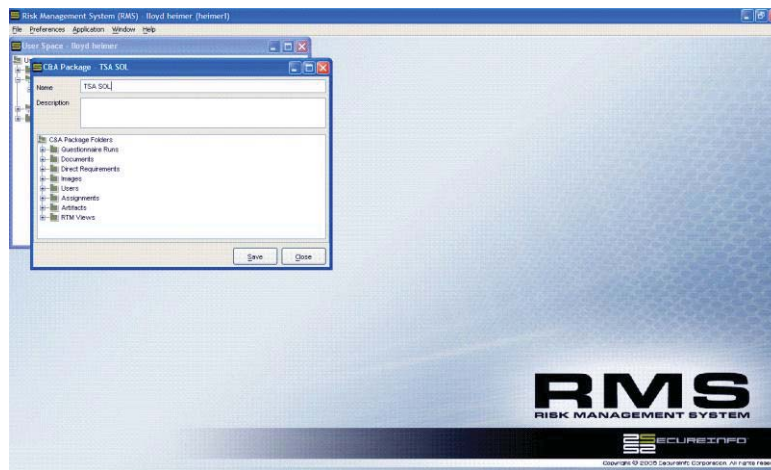


Figure 7. Blank (Sample) C&A Package

³ DHS Security Configuration Guides are located at [DHSOnline/Components/Management/CIO/CISO](https://dhs.gov/online/components/management/cio/ciso)

2. Run the Questionnaire.
3. Complete questionnaire using the information specified in the Questionnaire Input table above.
 - Select NIST SP 800-37 all documents (Phase I-IV).
 - A pop-up stating “Finish Questionnaire Run Options” appears.
 - Choose “Save and Generate C&A Package Documents.”

Figure 8 illustrates the contents of a completed C&A Package in RMS.

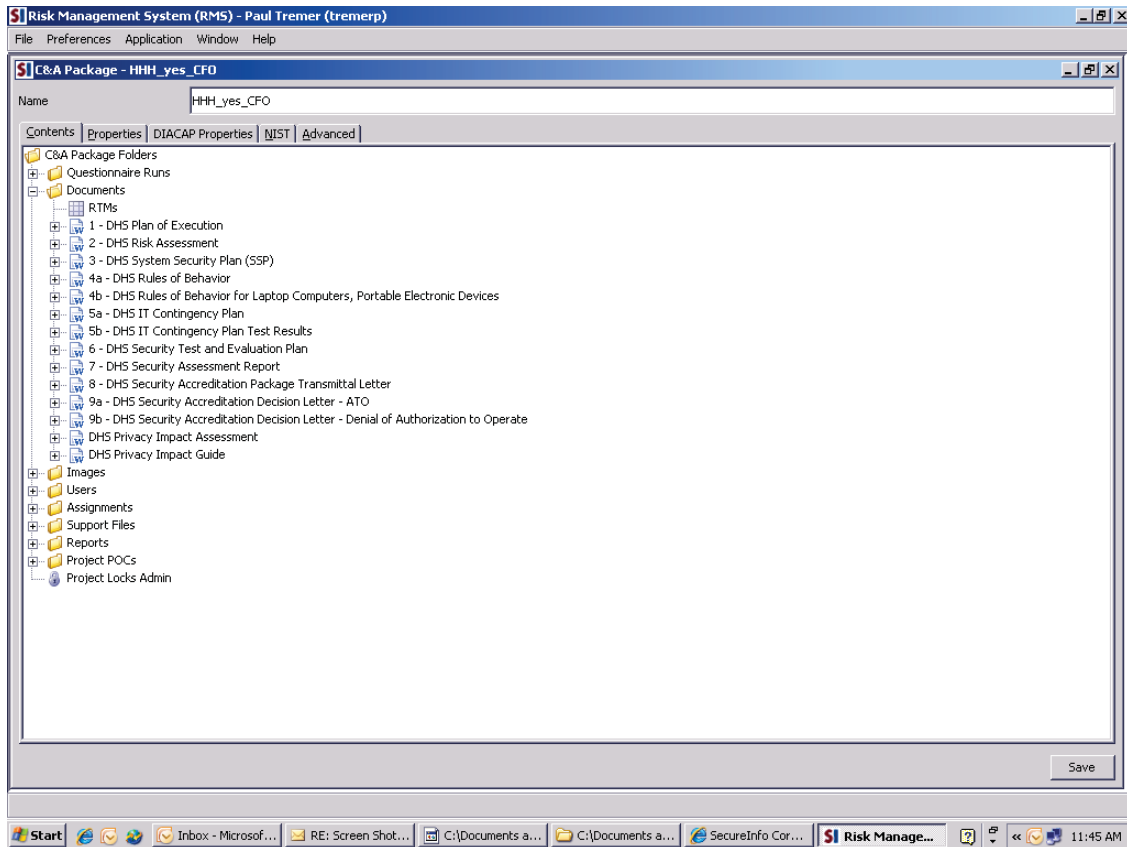


Figure 8. Sample of Completed C&A Package

3.8.3 Questionnaire Output

The C&A Package will contain the following documents:

- Set of blank DHS templates for completing key C&A documents. These documents are also included as attachments to this guide:
 - Risk Assessment (RA)
 - System Security Plan (SSP)
 - ST&E Plan
 - Contingency Plan (CP)
 - Contingency Plan Test (CPT) Results

- Security Assessment Report (SAR)
 - Accreditation Decision Letter
 - SRTM with applicable DHS policy, security requirements, and test requirements
- Table 10 shows the field definitions for fields in the SRTM.

Table 10. SRTM Field Definitions

SRTM Field	Field Definition
Requirement Type	Identifies Security Requirement Control Type: Management, Operational, or Technical
Requirement Sub Type	NIST or DHS Family Security Requirement Sub-class Type: Access Control, Audit & Accountability, Awareness & Training, C&A and Assessment, Configuration Management (CM), Contingency Planning, Emissions Security, Identification & Authentication, Incident Response, Maintenance, Media Protection, Personnel Security, Physical & Environmental Protection, Planning, Risk Assessment, Systems & Communications Protection, Systems & Information Integrity, Systems & Services Acquisition
Document Name	Source Document containing security requirement information: DHS SSP
Section	Section of document containing security requirement information
Reference	Source Reference for security requirement: DHS 4300A (version) System Security Handbook (SSH), NIST SP 800-53 (Rev 1)
Reference Date	Reference Date for security requirement
Requirement Name	Name of Security Requirement: example – AC-01 Control H (High) - Access Control Policy and Procedures
Requirement Description	Description of Security Requirement
Assessment Name	Provides more detail of security requirement & class type/sub-type: example – AC-01.1 H, AC-02 p1 CFO (relating to CFO data)
Methods Interview Examine Test	Specifies type(s) of evaluation method: Interview, Examine, Test
Objective	Test Objective to evaluate security requirement adherence: example - Determine if: (i) the organization manages IS accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts; (ii) the organization defines the frequency of Information System (IS) account reviews; (iii) the organization reviews IS accounts at least annually; and (iv) the organization initiates required actions on IS accounts based on the review. Examine:(DEPTH:

SRTM Field	Field Definition
	Detailed, COVERAGE: Comprehensive): Access control policy; procedures addressing account management; IS security plan; list of active system accounts along with the name of the individual associated with each account; lists of recently transferred, separated, or terminated employees; list of recently disabled IS accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records.
Preparation	Provides detail associated with Test Preparation activities/requirements
Procedures	Test Procedures to evaluate security requirement adherence: example - 1. Examine organizational records or documents to determine if the organization establishes, activates, modifies, reviews, disables, and removes IS accounts in accordance with documented account management procedures. 2. Examine organizational records or documents to determine if the organization conducts IS account reviews annually and any required actions as a result of the reviews have occurred in accordance with established procedures. 3. Examine selected active user accounts to determine if the organization followed procedures to establish and activate the user accounts and completed any organization-required documentation. 4. Examine a list of recently disabled IS accounts and compare to selected system-generated records with user IDs and last login date for each account to determine if the last log-in date is beyond the date that the account is disabled.
Expected Results	Specifies the expected results of testing activities: example - 1. The organization establishes, activates, modifies, reviews, disables, and removes IS accounts in accordance with documented account management procedures. 2. The organization conducts IS account reviews annually and any required actions as a result of the reviews have occurred in accordance with established procedures. 3. The organization followed procedures to establish and activate the user accounts and completed any organization-required documentation. 4. The last log-in date is beyond the date that the account is disabled.
Results	Identifies actual test results/findings
Status	Provides test status information: example –not started, passed, exception, not applicable
Severity Level	Identifies severity level of security requirement testing: example – Not set, Critical, High, Low, Medium
Completion Date	Specifies testing completion date
POC (Point of Contact)	Identifies Point(s) of Contact / Owner / Stakeholder Information

4. System Security Planning Process

System Security Planning is a crucial process for providing protection for DHS information systems as illustrated in Figure 2. It describes the controls to be used to provide protection for an information system.

Processes that occur earlier in the DHS C&A Guide define the security controls that are documented in the SSP. The SSP describes how the security controls are implemented. The SSP is also the basis for continuous monitoring to ensure the security of the information system throughout its lifecycle.

4.1 System Security Planning Purpose

The purpose of the SSP is to provide an overview of the security requirements of an information system and describe the controls in place or planned for meeting those requirements. It also includes a complete description of the information system, including purposes and functions, system boundaries, architecture, user groups, interconnections, hardware, software, encryption techniques, transmissions, and network configuration. In addition, the SSP delineates the responsibilities and expected behavior of all individuals who access the system. It should reflect input from the System Owner, information owners, Component CISO, ISSO, CO, and the DAA.

4.2 System Security Planning Decision Making Factors

The System Security Planning process at DHS is risk-based, ideally begins at the Requirements Definition lifecycle stage, and is conducted in parallel with the RA process. The SSP focuses on developing and recording a set of security controls that meet all security requirements of the system. It requires diligence to maintain the consistency of the SSP, as its development and maintenance continue throughout the system lifecycle. The minimum set of security controls for a system is identified in the SRTM generated during the System Security Characterization Process. However, the System Owner and ISSO can tailor the SRTM to address additional concerns identified in the RA and other system-specific requirements.

The SSP is the definitive reference document for security information pertaining to a specific information system. As a result, the SSP is a living document and needs to be updated, at least annually, as changes in the system or its environment will occur throughout the system life cycle.

Each of the primary C&A documents is referred to within the NIST Risk Management Framework as illustrated in Figure 9.

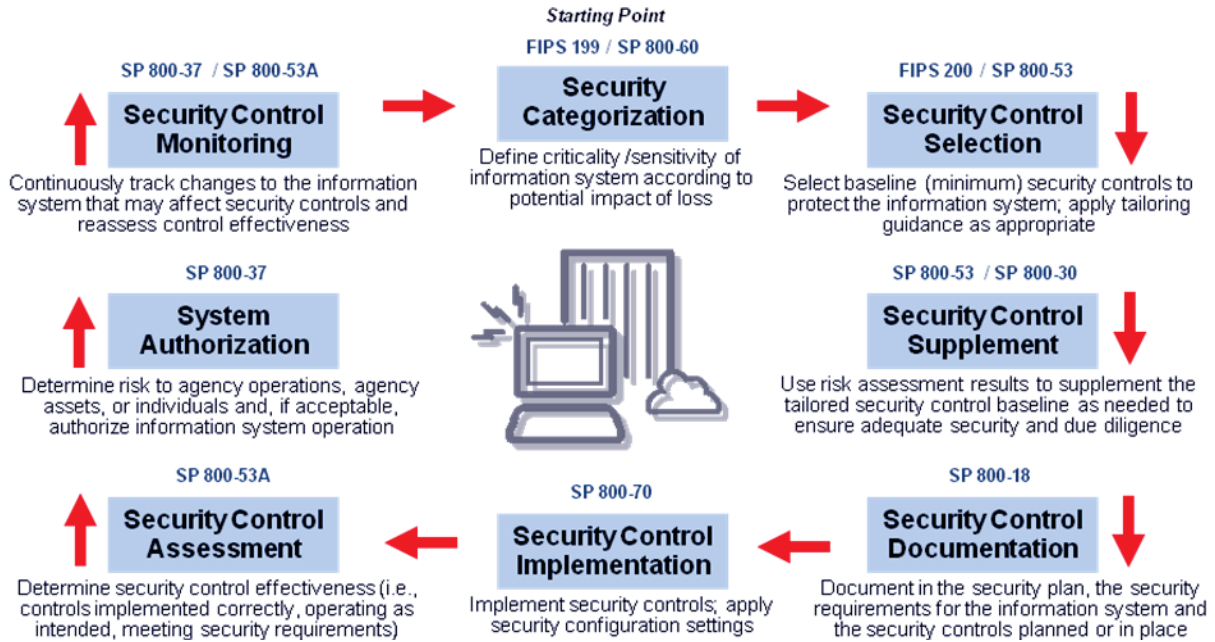


Figure 9. The NIST Risk Management Framework

For an understanding of how the primary C&A documents relate to Risk Management across the security life Cycle, refer to NIST 800-39, *Managing Risk from Information Systems: An Organizational Perspective*.

4.3 Security Planning Input

Table 11 identifies the required input for the Security Planning Process.

Table 11. Security Planning Process Input

Input	Source
System Description	Current RA and the system design
Accreditation Boundary Diagram	System Design Documents; current Risk Assessment information
System Points of Contact (e.g., System Owner, ISSO, and DAA)	Current RA
System Risks	Current RA
Current and Planned Security Controls	<ul style="list-style-type: none"> • SRTM • RA • Acquisition documents w/special requirements • Applicable Standards
Configuration Management (CM) Policy or Plan	Component CM Policy or Plan; Prior System CM Plan
Interconnectivity information	MOUs, MOAs, or ISAs; network or data models

4.4 System Security Planning Tasks

Analysis, design, and implementation descriptions of security controls are completed and recorded in the SSP. The following tasks are required for SSP development:

1. Review the SRTM for completeness.
2. Review the most current RA document to identify any additions to the controls listed in the SRTM.
3. Review Component policies to identify any modifications to the controls listed in the SRTM.
4. Document any planned compensating controls and track compensating controls into the ST&E Plan so that the compensating controls are tested as satisfying requirements. (See Section 8).
5. Review acquisition documents to identify any modifications to the controls listed in the SRTM.
6. Draft the SSP (Section 5.4.1), using the SSP template in RMS.
7. Draft Rules of Behavior (Section 5.4.3).
8. Draft Interconnection Security Agreements (ISA) (Section 5.4.2).
9. If required, together with the DHS Privacy Office, complete a PIA. See the section on System Security Characterization Process
10. Conduct SSP review and obtain approval by the System Owner, Component CISO, and DAA.

4.4.1 SSP Template

The DHS SSP Template is included as Attachment B of this guide. The current template is comprised of three major sections:

- 1.0 System Identification
- 2.0 Security Controls
- 3.0 Plan Approval

Information to assist in completing each of the key sections of the SSP is given below:

System Identification: Identifies the System Number, Name, and Abbreviation. These must be the same as the System Identification information recorded in TAF.

Roles and Responsibilities: Identifies the roles and responsibilities associated with the system and identifies the individuals assigned. The name, title, office, major organization, address, and contact information for the individuals responsible for the system mission, development, and security are provided.

System Operational Status: Indicates the operational status of the system.

General Description/Purpose: Provides a brief description of the system and its purpose. The following information topics may be provided, as appropriate, to describe the system:

- Capabilities
- Accreditation Boundary
- Firmware
- Encryption/Public Key Infrastructure

(PKI)

- System Users
- Related Major Applications
- Subsystems
- Hardware
- Software
- Network Topology
- Network Configuration
- Network Connection Rules
- Related interconnected systems
- Firmware

System Environment: Describes in a general fashion the technical implementation of the system (e.g., physical location(s), backup sites). The data included in this section is system-dependent and should include environmental or technical factors that raise special security concerns, such as use of Personal Digital Assistants, wireless technology..

System Interconnection/Information Sharing: Describes *all* external connections to the information system. Identifies external connections that have Memoranda of Understanding (MOU) and/or ISAs.

Applicable Laws/Regulations: Identifies DHS policies and procedures applicable to the system and other Component-specific or system-specific requirements that affect security control implementation.

Information Sensitivity: Gives the impact levels for confidentiality, integrity, and availability as defined in the Security Categorization process. In addition, this section indicates whether the system is a CFO Designated Financial System or a Privacy Sensitive System as defined in the Security Categorization Process. Finally, the security classification of the system is identified.

Security Controls: Describes the security controls implemented or planned for the system. The security controls are listed in alphabetical order and include NIST SP 800-53 controls as well as required DHS controls.

Plan Approval: Includes signatures of the System Owner, Component CISO, and DAA.

4.4.2 Security Controls Description

Each security control description must include the implementation status. That is, the description should clearly state whether or not the control is currently implemented, or is designed and planned for future implementation, and if not, describe what mechanism is in place or planned to compensate. Justification for non-applicable controls should be provided.

The description of each control should include:

- What (is being implemented)
- Who (is responsible [roles or organization] for implementing the control)
- Where (distributed or local, the scope, how many)
- When (the status of the control implementation)
- How (how is the control implemented)

The field labeled 'Status' in the SRTM is used to reflect the test results. The dropdown has the following options:

- Not Started
- In Progress
- Exception
- Passed
- Not Applicable

Table 12 provides examples of poor quality and good quality descriptions of security controls.

Table 12. Security Control Description Examples

Control	Poor Description	Good Description
AC-1	<p>The DHS Sensitive Systems Handbook, v 6.0 documents the DHS access control policies and procedures.</p>	<p>Security Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.</p> <p>Status: In Progress</p> <p>Implementation: The DHS Sensitive Systems Handbook addresses access control policies for all DHS systems. The handbook includes a discussion of purpose, scope, roles, responsibilities, management commitment, coordination, and compliance. DHS Headquarters is responsible for developing, disseminating, and updating the content of the handbook – currently the handbook is reviewed and republished quarterly.</p> <p>The ISSO is in the process of developing formal documented procedures for implementing the policies outline in the handbook and their associated controls. The procedures will be outlined in the system’s ‘Operations Manual’. The manual will describe specific procedures enacted by the system or performed by system staff to meet the requirements of applicable Access Control security controls.</p> <p>Development and maintenance of the Operations Manual is the responsibility of the system’s ISSO.</p> <p>The manual will be reviewed and updated at least annually. Applicable policy changes will be reflected in the operations manual within 60 days of their publication.</p> <p>The manual is distributed to all system administration personnel with security responsibilities. Security staff will use the manual as their set of procedures for performing security</p>

Control	Poor Description	Good Description
SC-7	<p>The system does not perform boundary protection. This control is handled by a GSS and is not applicable to this system.</p>	<p>related functions on the system.</p> <p>Security Control: The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.</p> <p>Status: Passed</p> <p>Implementation: The system inherits boundary protection controls from the GSS <System ID> the details of which can be found in the <System ID> SSP. The GSS's SSP identifies this system as a supported application with control inheritance responsibilities.</p> <p>The GSS employs <brand> firewalls to defend the network from other external information systems including the internet by only allowing data carried on required ports and protocols to transverse the system boundary. Further, GSS switches segregate traffic for this system to a dedicated Virtual Local Area Network (VLAN). The GSS firewalls only allow ports: 80, 443, and 5125 to access this system's VLAN and only accept port 80 egress requests from the VLAN.</p> <p>The GSS ISSO alerts this system's ISSO if any anomalous events are detected by the GSS's boundary protections.</p> <p>This system's ISSO is required to ensure that boundary controls are implemented and performing as expected. The ISSO will review logs and configurations at least quarterly.</p> <p>This system's ISSO may request access to log files or switch/firewall configurations with a 48 hour Service Level Agreement (SLA).</p>
AC-19	<p>The system does not allow the use of portable or mobile devices.</p>	<p>Security Control: The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.</p> <p>Status: Passed</p> <p>Implementation: The system is not capable of controlling the access of portable or mobile devices. Remote access to the system is not capable of filtering based on device authenticators and as such users can access the system from unapproved laptops.</p> <p>To compensate for this risk the system requires users with remote access permissions to sign</p>

Control	Poor Description	Good Description
		<p>remote access rules of behavior. Users are informed, and agree, to only access system data from approved Government Furnished Equipment (GFE) laptops. Users sign the Rules of Behavior (ROB) prior to being granted remote access and are required to reaffirm their understanding and agreement annually.</p> <p>The system ISSO is required to ensure that all remote access capable users have current remote access ROB on file. Monthly, the lead system administrator generates a list of active remote users that the ISSO uses to audit the list of signed ROB.</p>

4.4.3 Rules of Behavior

DHS 4300A Sensitive Systems Handbook, Attachment G, Rules of Behavior, contains a template for rules of behavior that apply to all DHS employees and support contractors who use DHS systems and IT resources, such as laptop computers and portable electronic devices to access, store, receive, or transmit sensitive information. Attachment G also provides guidance Components can use for tailoring the Rules of Behavior for a specific system. The rules of behavior are summarized in the SSP for the Planning security control PL-4, Rules of Behavior. Every user must sign the system Rules of Behavior prior to being granted access to a DHS system.

4.4.4 Interconnection Security Agreements

An ISA is required whenever the FIPS 199 categorizations of the interconnected systems are not identical and the systems are not accredited by the same DAA. The ISA documents the security protections that must operate on interconnected systems to ensure that transmissions between systems accredited at different security levels permit only allowable transactions and that shared data is protected at a level commensurate with each system’s Confidentiality, Integrity, and Availability security objectives. (See *DHS 4300A Sensitive Systems Handbook, Attachment N, Preparation of Interconnection Security Agreements*). Three other documents support the ISA:

- MOU or Memorandum of Agreement (MOA) define the responsibilities for both parties in interconnecting, operating, and securing the two systems. These brief nontechnical documents provide the authorization for detailed planning of an interconnection, leading to an ISA.
- The System Interconnection Implementation Plan (SIIP) provides the technical detail needed to guide the development and establishment of an interconnection and thus to help both organizations confirm that all details have been covered. An SIIP supplements the associated MOU, MOA, and ISA with administrative rather than technical content.

DHS 4300A Sensitive Systems Handbook, Attachment N, Preparation of Interconnection Security Agreements, contains guidance for completing ISAs and an outline for the SIIP. Templates for the ISA, MOA, and MOU are provided in RMS and are included as Attachments H through J of this *C&A Guide*.

4.5 Security Planning Output

The following are outputs from the Security Planning Activities:

- SRTM
- SSP
- Signed ROBs
- Signed ISAs, MOU, MOA, and SIIP
- PIA, if required

5. Risk Assessment Process

Statutory requirements of the FISMA Act of 2002 require periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

DHS uses a risk-based approach to information system security and relies on an accurate RA that is performed early in the certification process. The information gained from the System Identification process establishes an inventory of assets and serves as the basis for identifying vulnerabilities, assessing risks, and for selecting security controls (requirements). RA is conducted periodically during the system lifecycle and the frequency is defined by the organization as stipulated by NIST SP 800-53 Security Control RA-4.

The DHS C&A Guide employs recommendations for risk assessment as described in NIST SP 800-30, *Risk Management Guide for IT Systems*.

5.1 Risk Assessment Purpose

The Risk Assessment process is concerned with risk identification, determining the likelihood of occurrence, the resulting consequences, and the safeguards that can be used to mitigate risks. Risk Assessment sets the stage for planning and conducting the ST&E and provides the basis for all other downstream C&A activities. The objective of the Risk Assessment process is to produce an accurate understanding of the risks in the system and the security controls (planned or implemented) to mitigate those risks. Some of those controls may be preventive, designed to inhibit conditions that violate security policy, or detective, designed to warn of conditions that violate security policy. Most importantly, Risk Assessment provides a foundation for preparing a statement of operational risk from which a DAA or other certifying official can make informed operational decisions. Operational risk is the risk contained in a system under operational status: it is the risk that a DAA accepts when granting an ATO. Risks identified during the Risk Assessment process are included in the SAR.

Prioritization of risk mitigation activities is addressed in the POA&M, where corrective actions for each weakness are scheduled, estimated, and tracked to completion. The risk mitigation plans are documented in the TAF POA&Ms tab. The entire POA&M management and maintenance process is defined in *DHS 4300A Sensitive Systems Handbook*, Attachment H, *POA&M Process Guide*.

5.2 Risk Assessment Decision Making Factors

The Risk Assessment must present a realistic and concise picture of the information system assets needing protection, which events and conditions that may threaten those assets, and the vulnerabilities of the system. Decisions in the risk assessment process are based upon an accurate inventory of system assets and a complete understanding of the system security profile developed during the System Security Characterization process. Those decisions go beyond

hardware and software considerations and attempt to ascertain risks from all perspectives. Factors that should be addressed when assessing risks include, but are not limited to:

- Environmental systems (fire detection/suppression, temperature/humidity controls, drainage systems)
- Facilities security
- Intangibles (credibility, reputation, trust)
- Personnel with physical and logical access
- Physical security systems (badge systems, access control systems, closed-circuit TV)

Where risks cannot be mitigated satisfactorily by employing available controls, compensating controls can be devised to reduce the risk. Compensating controls are used to overcome existing or potential control deficiencies. For example, a detective control may be used to compensate for the deficiency of a preventive control. When devising compensating controls, cost and control effectiveness should be evaluated and a preferred implementation strategy should be considered.

5.3 Risk Assessment Input

Table 13 identifies the required input for the Risk Assessment Process.

Table 13. Risk Assessment Process Input

Input	Source
System description	System Identification process
FIPS 199 Categorization	System Security Characterization process
PTA	System Security Characterization process
E-Authentication Level Determination	System Security Characterization process
CFO-Designated Financial System Determination	System Security Characterization process
System Points of Contact	System design documents SSP
History of system attack	Department incident reports; Findings from the Office of the Inspector General (OIG), Federal Computer Incident Reporting Center (FedCIRC) Vendor-published software vulnerabilities
Audit findings	Government Accountability Office (GAO), OIG Audit Reports or Recommendations
Security requirements	SRTM
Prior risk assessments	RMS
Current and Planned Controls	SRTM, Acquisition documents w/special requirements, standards or obligations
Interconnectivity information	MOUs, MOAs, ISAs, Network diagrams

5.4 Risk Assessment Tasks

The Risk Assessment process must validate the applicability of the minimum set of security controls chosen for the system to determine whether they are appropriate. Results could substantiate the need for additional controls, alternative controls, or fewer controls.

5.4.1 Prepare for Risk Assessment

Prior to ST&E

Use the SRTM and the RA template previously generated by RMS.

After ST&E

Obtain the RA document that was prepared prior to ST&E.

5.4.2 Threat Identification

Identify specific threats for each threat source - Natural, Environmental, and Human. Examples are shown in Table 14.

Table 14. Threat Source Examples

Source	Threat	Impact of Exploit
Natural	Flood	System Unavailability Damage to hardware, cables and facility
Environmental	Power failure	System Unavailability
Human	Data corruption	Modify system data

5.4.3 Vulnerability Identification

Vulnerability is a weakness in an information system, system security procedures, internal controls, or an implementation that could be exploited to cause damage or a loss.⁴

Vulnerabilities are factors that have a negative impact on the security objectives of confidentiality, integrity, and availability; and may include security controls that are not implemented or not functioning as intended. Perform a Vulnerability Assessment, following the guidance contained in Attachment O, *Vulnerability Management Program, DHS 4300A Sensitive Systems Handbook* to identify vulnerabilities in the system.

5.4.4 Determine Susceptibility

Determine susceptibility to risk - i.e., the system is susceptible to risk wherever matches between threats and vulnerabilities exist. If susceptibility is confirmed, then a Risk Statement must be prepared. See Risk Definition in this section.

5.4.5 Risk Definition

Create a Risk Statement for all risks. All Risk Statements should use the IF/THEN format.

For example,

⁴ CNSI 4009, *Glossary of IA Terms*.

IF a flood occurs, THEN the system may be unavailable.

5.4.6 Security Control Analysis

Select security controls that are to be implemented to mitigate risks. Devise compensating controls when risks cannot be mitigated by implementation of internal controls.

5.4.7 Likelihood Determination

“Likelihood” is the expectation that a capable threat will exploit a system vulnerability to cause damage or a loss. This likelihood considers the preventive and deterrent properties of available security controls and system features that make exploitation difficult. Determine the likelihood that each identified risk will occur.

5.4.8 Impact Analysis

Determine impact rating (consequences and magnitude of harm) of the successful exploitation of each identified vulnerability. The overall impact determination for the system was accomplished as a result of the FIPS 199 categorization process. The determination of impact for all vulnerabilities should confirm the original categorization.

5.4.9 Risk Level Determination

Following guidance in the RA template, assign a Risk Level of LOW, MODERATE, or HIGH to all risks. Supplemental guidance is also provided by NIST SP 800-30.

5.4.10 Security Control Recommendations

Before ST&E, declare that the set of Security Controls already planned or implemented is adequate or recommend changes to it.

After ST&E Results are analyzed, declare that the set of Security Controls already planned or implemented is adequate or recommend changes to it.

5.4.11 Document the Risk Assessment

Document the analysis, decisions, and recommendations of the Risk Assessment Process in the RA. After ST&E, update the Risk Table in the RA.

5.5 Risk Assessment Output

The output from the Risk Assessment Process is the RA. The RA contains:

- Threat Identification
- Vulnerability Identification and susceptibility of vulnerabilities to exploitation
- List of Current and Planned Controls in the SRTM
- Impact Rating, Likelihood, and Risk Levels
- Recommended Security Controls
- POA&M

5.6 CFO Designated Financial Systems

System owners are responsible for ensuring that risk assessments for all CFO Designated Financial Systems are updated annually before or by the end of the 4th quarter.

6. Contingency Planning Process

Contingency planning is crucial to maintaining data availability during times of adverse interruptions to normal system operations. All DHS system owners are required to plan for emergencies and interruptions to system operations. A system-level Contingency Plan (CP) is required for each DHS system.

One should plan thoroughly, considering a broad spectrum of realistic disruptive scenarios but keeping the CP general enough to allow tailoring to the requirements of the system it protects. At the same time, directions should be concise, clear, and unambiguous so that assigned staff will understand their tasks easily.

As an important element of C&A for DHS information systems, Contingency Planning is guided by the CP control family described in NIST SP 800-53. Selected Contingency Planning controls should be defined in both the SSP and in the ST&E Plan.

6.1 Contingency Plan Purpose

The purpose of IT contingency planning is to ensure the availability of critical IT assets under adverse circumstances. DHS Components are required to develop, test, and maintain IT CPs to ensure adequate information system assets are available to sustain essential services and support functions in accordance with the requirements for the FIPS 199 impact level for the availability security objective.

Contingency planning is an integral part of the DHS Continuity Planning for Critical DHS Assets Program and supplements DHS Continuity of Operations Planning (COOP) policy. IT Contingency Plans are IT oriented and therefore focus on sustaining the systems (major applications and general support systems) that provide essential services and supporting office functions. Coordinate with the appropriate Departmental and Component Contingency Planning Program Office. The content of the CP focuses on what needs to be done to recover those systems.

6.2 Contingency Plan Decision Making Factors

The unavailability of critical IT assets potentially threatens the success of Departmental and Component programs unless asset owners and administrators are prepared for prompt recovery and reconstitution following disruptive events. A system's security categorization determines the level of rigor to be employed during Contingency Planning.

IT contingency planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency and includes identification of procedures and capabilities for recovering major applications and general support systems.

An understanding of the relationship of the CP with other DHS and Component business continuity plans is critical for coordinated recovery actions.

6.3 Contingency Plan Input

Table 15 identifies the input for the CP Process.

Table 15. Contingency Plan Process Input

Input	Source
System Identification and Characterization Information	System design documents ; inventory data; system metrics or other performance-related reports
All Personnel, roles and prioritized responsibilities or "line of succession" information	System design documents; system administration procedural documents; other DHS-related continuity plans; Current POC lists
Downtime thresholds	<i>DHS 4300A Sensitive Systems Handbook</i> , Attachment K, IT CP Template
Current and Planned Controls	<ul style="list-style-type: none"> • SSP and SRTM • Results of ST&E (SAR) • Acquisition documents w/special requirements, standards or obligations
Interconnectivity information	SLAs, MOUs, MOAs, ISAs, Network diagrams, data models

6.4 Contingency Plan Tasks

The Contingency Planning process must validate the minimum set of required recovery controls. The high-level sequence of activities (NIST SP 800-34, 2002) for developing a CP is:

1. **Develop the contingency planning policy statement.** Document formal departmental or component policy in the CP for the system. This formal policy provides the authority and guidance necessary to develop an effective CP. Policy statements should comply with *DHS Sensitive Systems Policy Directive 4300A*.
2. **Develop recovery strategies.** Formulate comprehensive recovery strategies that ensure effective and timely system recovery following a disruption. Develop these strategies to address disruption impacts and allowable outage times identified by the System Owner. Consider alternatives when developing the strategy, including cost, allowable outage time, security, and integration with larger, organization-level contingency plans. Coordinate the strategies with appropriate business customers and stakeholders.
3. **Develop the IT contingency plan** - in the plan, include detailed guidance and procedures for restoring the degraded system or a system whose operation has been stopped by a disruptive event. The plan should be organized in four sequential phases plus detailed appendices:
 - a. Supporting Information
 - b. Notification/Activation, including a Call Tree that is to be maintained as current
 - c. Recovery
 - d. Reconstitution.
4. **Train appropriate staff.** Ensure that all staff members assigned a contingency management or support role or responsibility receive formal training upon initial assignment of the role or responsibility and refresher training at scheduled intervals. The

system IT CP should be a basic course book for the training. To the extent possible, cross-train staff to attain broadened recovery and reconstitution capabilities following emergencies that arise when some key support staff may be unavailable. Exercise the Call Tree as a part of the essential training, which should also include a contingency for Call Tree members, who may be unreachable at the time of testing.

5. **Plan maintenance.** The IT CP is a living document. Update the plan regularly so that it remains current with the supported IT system and its operating environment, which may change. DHS policy suggests updating the Plan at least annually or when major changes occur and after testing if necessary.
6. **Plan distribution.** Distribute the CP and subsequent changes to all staff members assigned a contingency management or support role or responsibility.

6.5 Contingency Plan Output

The following are output from the Contingency Planning Activities:

- System CP
- CP Checklist
- POA&M updated in TAF for CP weaknesses

7. Contingency Plan Testing Process

Contingency Plan Testing (CPT) is required at least annually for all DHS information systems.⁵ This includes the DHS financial systems that must comply with Federal Information System Controls Audit Manual (FISCAM) domain key controls SP-1, *Periodically Assess Risks*, SC-3.2 *Arrangements have been made for Alternate Data Processing and Telecommunications Facilities*, and SC-4.1. As with the CP, the CPT objectives are limited to the certification boundary as identified in the SSP.

Test complexity varies according to the system availability impact level, CP resources, and system sensitivity. Testing the CP is dependent upon whether a standalone test is planned versus one that has been incorporated into another, higher-level, more comprehensive exercise by including other organizations. Contingency planning experts may choose to conduct a tabletop exercise or a full-blown simulation when testing the CP.

The test must challenge the elements of the Plan. In other words, the test is holistic and is not considered complete unless the whole plan is challenged and the results recorded and reported. For example, simple data retrieval is not sufficient to meet a readiness test of the CP. Or, if it is determined that some risks exist that would prevent operating from the primary location, then testing only from the primary location would be insufficient. Rather, an alternative location must be identified and tested.

Sometimes it is more reasonable and cost-efficient to test as a part of a larger exercise. An example might be that a Component-wide exercise is already planned that would include steps to validate a single system CP as one part of the larger exercise. Another possibility is conducting annual CP testing when a change to the system is also being tested. In these cases, the CP can be successfully verified, but it is very important to have prearranged for DHS requirements to be included in testing the CP and that documentation of results will meet the DHS verification standards. Additional guidance is provided in the DHS *Sensitive Systems Policy Directive 4300A*. If it is still unclear whether the planned test meets compliance guidelines, the Compliance Director at DHS Office of the CISO can provide more direction.

7.1 Contingency Plan Testing Purpose

Testing the CP periodically is essential to assuring that data can be recovered. According to DHS Policy, the following areas must be addressed in a test of the CP:

- System recovery
- Data recovery from backup
- Coordination among recovery teams
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations
- Notification procedures

⁵ NIST SO 800-53, Revision 2, extends contingency plan testing requirements to low impact availability systems.

A fundamental purpose of the CPT is to answer the question: “In an emergency, will we have timely, secure access to our data?”

7.2 Contingency Plan Test Decision Making Factors

Characteristics of the test plan should follow the same discipline used in best-practice test procedures – i.e. the test should be designed to challenge specific elements spelled out in the CP thoroughly and objectively; results should be recorded clearly and succinctly for each test objective; and solutions for remediation of deficient areas should be recommended. DHS policy and NIST guidelines also suggest including description of test scope, scenarios, logistics, scheduling and time frames for each test and participant. The test scenarios should mimic reality as closely as possible. Section 9.8 in the *DHS 4300A Sensitive Systems Handbook* provides detailed guidance on testing requirements for high, moderate, and low systems. See Attachment F, CP Planning Template, for further guidance.

There are two basic exercise formats:

- **Tabletop Exercises.** Participants in tabletop exercises, simulate recovery procedures – i.e. without any actual recovery operations occurring. Tabletop exercises are the most basic and least costly of the two types of exercises and should be conducted before performing a functional exercise. Actual contact information should be used and tested.
- **Functional Exercises.** Functional exercises are more extensive than tabletop exercises, requiring the event to be simulated. Functional exercises include simulations and war games. Often, scripts are written out for staff pretending to be external organization contacts, or there may be actual interagency and vendor participation. A functional exercise might include actual relocation to the alternate site and/or system cutover.

Test preparations will include arranging for meeting or exercise facilities and resources. Related or ancillary organizations may be notified so they know that a test is being conducted, and affecting operations during testing should be avoided.

Once test results are analyzed and reported, lessons learned should be validated and recorded. Any weakness in the test may need to have items recorded in the POA&M.

Training for personnel with contingency plan responsibilities should complement testing. Training should be provided at least annually; new hires who will have plan responsibilities should receive training shortly after they are hired. Ultimately, contingency plan personnel should be trained to the extent that they are able to execute their respective recovery procedures without aid of the actual document. This is an important goal in the event that paper or electronic versions of the plan are unavailable for the first few hours resulting from the extent of the disaster. Recovery personnel should be trained on the following plan elements:

- Purpose of the CP Test plan
- Cross-team coordination and communication
- Reporting procedures
- Security requirements

- Team-specific processes (Notification/Activation, Recovery, and Reconstitution Phases)
- Individual responsibilities (Notification/Activation, Recovery, and Reconstitution Phases)

7.3 Contingency Plan Testing Input

Table 16 identifies the required input for the Contingency Plan Testing Process.

Table 16. Contingency Plan Testing Process Input

Input	Source
CP	RMS
ISAs	RMS
DHS requirements to meet federal and Department requirements	<i>DHS Sensitive Systems Policy Directive 4300A</i> <i>DHS 4300A Sensitive Systems Handbook</i>

7.4 Contingency Plan Testing Tasks

Preparation for CPT is commensurate with the complexity of the CP. This varies from arranging a meeting room and assembling the tabletop exercise team for a simple scenario walkthrough for a small system to arranging a live full-scale failover to a “warm” or “hot” backup site. At a high level, these are the tasks associated with any CPT:

7.4.1 Determine Test Exercise Type

Evaluate the need for a tabletop or functional simulation exercise and schedule the event. Analyze the system’s CP objectives and consider the resources required such as cost, personnel, and locale.

7.4.2 Develop Contingency Plan Test Procedures

Determine topics and scope; identify objectives and participants, including a facilitator and who will execute the test. The design should test CP effectiveness in the areas of system recovery on an alternative platform from backup media; coordination among recovery teams; internal and external connectivity; system performance using the alternative equipment; restoration of normal operations; and notification procedures.

7.4.3 Arrange Test Resources

Obtain permissions and authority required for facility and/or alternative equipment use, inter-organizational coordination and participation of personnel needed for the test.

7.4.4 Training

Train the test team participants so they will be familiar with test objectives and be able to conduct their recovery activity without access to the CP document.

7.4.5 Schedule CPT

Announce and notify participants and affected organizations ahead of the actual date, so that participants can prepare for the test and adjust their work schedule appropriately.

7.4.6 Execute CPT

Conduct the test and capture results in post-test reviews attended by test participants. Add lessons learned results to the CP.

7.4.7 Test Reporting

Report Test results to management and system stakeholders. Consider including communication to other Component personnel who are responsible for contingency planning.

7.5 Contingency Plan Testing Output

The following are output from the CPT Process:

- CPT Results uploaded to TAF
- Documented Lessons Learned
- CPT deficiencies recorded in the POA&M

8. Security Test & Evaluation Planning Process

8.1 ST&E Planning Purpose

The purpose of ST&E planning is to identify system security controls, establish procedures and resources for verifying their effectiveness, and scheduling the verification activities. The Security Test and Evaluation (ST&E) Plan outlines the plan, the process, and the procedures necessary to verify that the controls identified in the SSP are in place and are operating as intended. The ST&E Plan template (Attachment C) is the starting point for ensuring that there is a plan and procedures for verifying that the appropriate security controls are in place.

8.2 ST&E Planning Decision Making Factors

The SRTM generated when a C&A package is initiated is pre-populated with sample test procedures and expected results. However, the procedures and results should be tailored to the particular system, risks, and system environment, and they may need to be supplemented with detailed technical methods and procedures. In addition, compensating controls identified in the RA and the SSP must be added to the SRTM.

8.3 ST&E Planning Process Input

The ST&E Plan template and the SRTM (spread sheet and .rtf format) are generated automatically from the C&A Package created in RMS. The SRTM contains the required DHS and NIST SP 800-53 controls for the information system and DHS configuration requirements for operating systems and platforms used in the system. The SRTM also identifies the method(s) used for conducting the test, the test objectives, and the test procedures. Table 17 identifies the required input for the ST&E Planning Process.

Table 17. ST&E Planning Process Input

Input	Source
ST&E Plan Template	RMS
SRTM	RMS
RA	RMS
SSP	RMS
POA&M	RMS
System requirements documents	System Owner
System design documents	System Owner
Previous assessments of the System to include Inspector General (IG) audits	System Owner

8.4 ST&E Planning Tasks

The following ST&E planning tasks should be performed.

1. Create the ST&E Plan, including Rules of Engagement.
2. Review the controls in the SRTM to determine completeness.
3. Review the adequacy of the testing procedures in the SRTM and update the procedures as required.
4. Identify script requirements and develop scripts, if applicable.
5. Select and configure vulnerability assessment tools.
6. Create ST&E schedule.
7. Coordinate with System Owner and facility manager.
8. Arrange for physical access to the system.
9. Arrange work space for test team.
10. Identify test team personnel (develop acquisition documents if testing is to be outsourced).
11. Plan for storage of test results data.
12. Provide all staff supporting the ST&E with copies of the ST&E Plan and the SSP.
13. Conduct staff review of ST&E Plan - Supporting staff must be familiar with the system, test plan, and test procedures.
14. Schedule the ST&E.
15. Obtain approval of Rules of Engagement.

8.5 ST&E Planning Output

Output of the ST&E Planning Process is:

- ST&E Plan, including the test schedule uploaded to TAF
- SRTM
- Written instructions for participating staff regarding:
 - Schedule
 - Tasks
 - Test procedures
 - Tools description
 - Configuration Management (CM) of test materials, the test environment, and media

9. ST&E Execution Process

9.1 ST&E Execution Purpose

The purpose of ST&E Execution is to verify that the system security controls are implemented correctly and producing the desired outcome. ST&E is crucial to deciding whether a system should be granted an ATO.

9.2 ST&E Execution Decision Making Factors

For moderate and high impact systems, NIST SP 800-53 (CA-4) requires that an independent certifying official conduct the ST&E to ensure that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system. Independent security certification services can be obtained from other organizations within the Component or can be contracted to a public or private sector organization. Contracted certification services are considered independent if the system owner is not directly involved in the contracting process or cannot unduly influence the independence of the certifying official conducting the assessment. The DAA decides on the level of independence based on the criticality and sensitivity of the information system and the ultimate risk to the system and the Component.

The ST&E meets the annual assessment requirements for the system in the year that the ST&E is conducted. As illustrated in Figure 10, a separate annual assessment is not required to be conducted in the same fiscal year that the ST&E is conducted. However, the results from the ST&E must be incorporated into the Annual Assessment Tab in TAF.

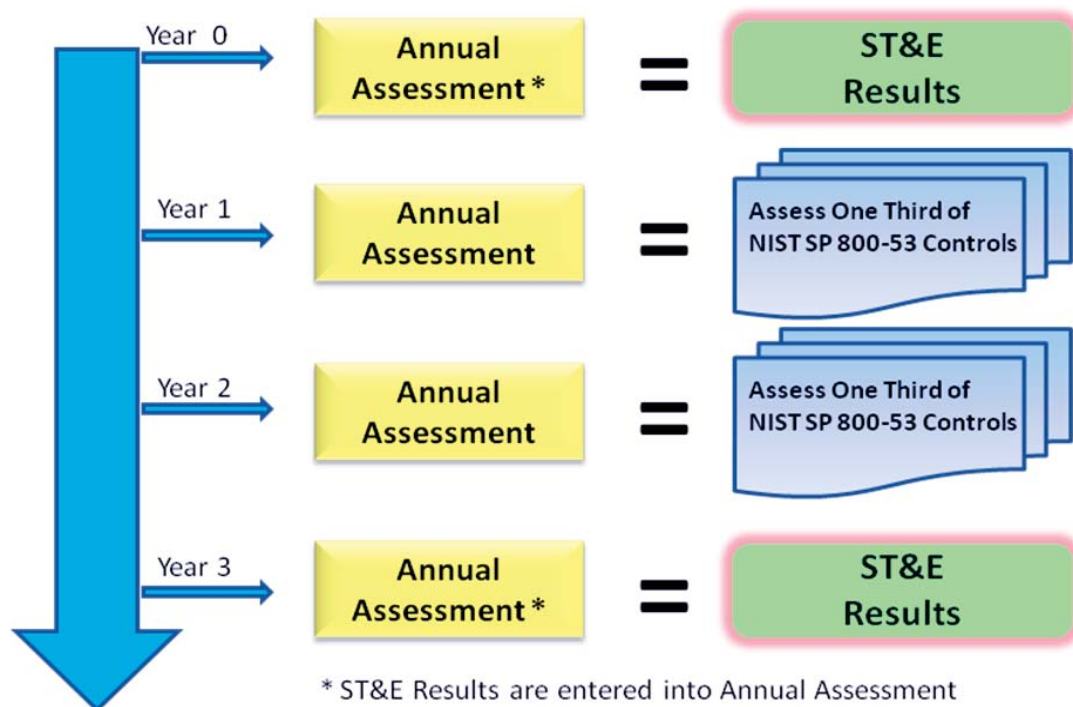


Figure 10. Relationship of ST&E Results and Annual Assessments

9.3 ST&E Execution Input

Table 18 identifies the input for the ST&E Execution Process.

Table 18. ST&E Execution Process Input

Input	Source
System ST&E Plan	RMS
System SRTM	RMS
POA&M	TAF
Audit Logs	ISSO
Configuration Guides	RMS DHSONline/Components/Management/CIO/CISO
Test Scripts (if applicable)	CO
Vulnerability Assessment Tools	CO
Test Team Instructions	CO

9.4 ST&E Execution Tasks

The following ST&E Execution tasks should be performed sequentially:

1. Conduct ST&E Execution kick-off meeting.

2. Arrange site visit and access requests as needed.
3. Execute ST&E.
4. Document the ST&E Results in the SRTM.
5. Review the ST&E Results contained in the SRTM with the System Owner and CO.
6. Collect and securely store all ST&E materials and media per Component document retention policy and procedures.
7. Upload completed SRTM into TAF.

9.5 ST&E Execution Output

ST&E Results for each requirement are documented in the SRTM using the columns shown in Table 19.

Table 19. ST&E Results Documentation

Column	Purpose
Results	Document the results of the test.
Status	Status has 5 options: <ul style="list-style-type: none"> • Not Started • In Progress • Exception • Passed • Not Applicable
Severity Level	Severity Level is used to classify the severity of an exception.
Completion Date	Date on which the test was performed.

9.6 CFO Designated Financial Systems

As specified in Section 3.15(a), *DHS Sensitive Systems Policy Directive 4300A*, ST&E plans and tests of key security controls for CFO Designated Financial Systems must be completed annually. The tests are to be performed during the first quarter of each fiscal year.

10. Security Assessment Process

10.1 Purpose

The purpose of the Security Assessment process is to document how the system is secured after ST&E and CPT have occurred. The objectives of the Security Assessment process are:

- Provide the CO a solid foundation for making a recommendation to the DAA to understand the risks of operating the system.
- Produce an accurate understanding of the risks in the system and the security controls (planned or implemented) to mitigate those risks.

10.2 Decision Making Factors

During the Security Assessment Process, it is necessary to analyze the effectiveness of the established security controls (planned or implemented) in mitigating risks identified during the Risk Assessment Process. Effectiveness is defined as a balance between the operational and economic costs of implementing a given control versus the gains in information security and mission capability achieved by implementing the given control.

In some cases, not all of the risk can be mitigated and there remains some residual risk. At the time of accreditation, these risks constitute the operational risk. The CO must have an accurate understanding of the full scope of operational risk as they make a recommendation to accredit the system. The SAR is meant to be an executive-level summary of the preceding C&A activities and a summary of those items that constitute operational risk.

10.3 Input

Table 20 identifies the input for the Security Assessment Process.

Table 20. Security Assessment Process Input

Input	Source
SSP	RMS
ST&E Results in SRTM	RMS
CPT Results	RMS
RA	RMS

10.4 Tasks

10.4.1 Create the Security Assessment Report

Make recommendations against currently implemented or planned security controls, or for adding new controls in the POA&M.

The SAR template is included as Attachment D of this guide. The template is comprised of three major sections:

- 1.0 Introduction

- 2.0 Security Assessment Results
- 3.0 Conclusion

The following discussion provides information helpful for completing the SAR.

Section 1 provides a context for the document. It includes:

- Purpose of the document
- Scope of the assessment (i.e., system description, summary of systems elements assessed, the FIPS 199 Security Categorization, Assessment Team composition, assumptions and constraints, and the risk rating scale)

Section 2 provides a quantitative summary of the ST&E results. This includes the number of controls implemented correctly, controls not implemented correctly, controls not evaluated, and controls not applicable for a system. For controls not implemented, the number of controls at high, moderate, and low risk are identified.

Section 3 includes detailed discussions of *all* the information system security weaknesses (not just those discovered in the ST&E Results) in order to provide the DAA with a complete picture of the security status of the system. Three tables require completion:

- Weaknesses that must be Remediated or receive an Exception/Waiver prior to ATO
- Weaknesses recommended to be remediated with the POA&M
- Weaknesses recommended as acceptable risks

These tables must include the following information:

- Link to the appropriate DHS or NIST SP 800-53 control identifier
- Brief description of the weaknesses
- System element affected by the weakness
- Risk Level (High, Moderate, Low)
- Recommended Resolution or Countermeasure

Finally, Section 3.0 contains the statement of operational risk and the Recommendation of the CO.

10.5 Output

The output of the Security Assessment Process is:

- SAR
- POA&M

11. Certification Documentation Process

The Certification Documentation Process ensures that documentation of all C&A activity has been prepared and supports the CO as they prepare to make a recommendation to accredit the system.

11.1 Certification Documentation Purpose

The purpose of the Certification Documentation Process is to compile work products and key C&A artifacts necessary for the CO to prepare the Accreditation Package.

11.2 Certification Documentation Decision Making Factors

- The **System Owner** should initiate the mitigation or elimination of exploitable information system vulnerabilities identified during ST&E but prior to the assembly and compilation of the accreditation package and its submission to the DAA. This can be accomplished by implementing corrective actions recommended by the CO.
- The **CO** should assess the effectiveness of the security controls modified or added to mitigate or eliminate exploitable vulnerabilities identified during ST&E.

11.3 Certification Documentation Input

Table 21 identifies the required input for the Certification Documentation Process.

Table 21. Certification Documentation Process Input

Input	Source
SAR	RMS
RA	RMS
SSP	RMS
POA&M	TAF

11.4 Certification Documentation Tasks

Perform the following certification documentation tasks:

1. Draft the Accreditation Decision Letter.
2. Assemble the Accreditation Package. The following documents are included in the Accreditation Package:
 - SSP
 - SAR
 - POA&M
 - Draft Accreditation Decision Letter.
3. Upload the Accreditation Decision Letter and Accreditation Package into TAF.

At the request of the DAA, additional documents may be included in the Accreditation Package such as the RA, completed SRTM, and ST&E Plan.

11.5 Certification Documentation Output

Output of the Certification Documentation Process is the Accreditation Package.

11.6 Certification Requirements for CFO Designated Financial Systems

The C&A process for CFO Designated Financial Systems is the same as that for other DHS information systems except that the accreditation must be signed jointly by the DAA and by the Component CFO.

12. Accreditation Process

Accreditation is a decision that the risks to agency operations, agency assets, or individuals that result from the operation of an information system are acceptable.

12.1 Accreditation Purpose

The purpose of the Accreditation Process is first to determine the operational risk and secondly for the DAA to make a decision to formally accept the operational risk.

12.2 Accreditation Decision Making Factors

The DAA must understand the risk that exists in the information system (after the implementation of an agreed-upon set of security controls) and whether those risks pose an acceptable level of risk to agency operations, agency assets, or individuals.

Authorizing officials (DAAs) must be able to determine the risk to operations, assets, or individuals and the acceptability of such risk given the mission and business needs of their Components.

The ISSO and CO should support the DAA in the evaluation of appropriate factors needed for deciding to accept or reject the risk to their respective Component. The following questions should be answered during the Accreditation Process to help ensure that the DAA makes informed, risk-based decisions:

- Is the potential risk to agency operations, agency assets, or individuals described in the system security plan (or risk assessment) prior to security certification correct and complete, and if so, would this risk be acceptable?
- Do security controls provide an appropriate level of protection for the system characterization?
- What specific actions have been taken or are planned to correct any deficiencies in the security controls for the information system to reduce or mitigate known vulnerabilities? Have resources been allocated to accomplish those actions?
- Are the results of security certification commensurate with Component-level risk and is the operational risk acceptable?

The Accreditation decision is explicitly based on the understanding and acceptance of the operational risk in the system after security certification is conducted.

12.3 Input

Table 22 identifies the input for the Accreditation Package Process.

Table 22. Accreditation Package Process Input

Input	Source
Accreditation Decision Letter	System Owner or CO (electronic or paper copy)
SAR	RMS

Input	Source
SSP	RMS
POA&M	TAF

12.4 Accreditation Tasks

12.4.1 Final Risk Determination and Risk Acceptability

The DAA determines whether the operational risk to DHS/Component operations, DHS/Component assets, or individuals is acceptable. The DAA then signs the final Accreditation Decision Letter. The DAA must judge which vulnerabilities are of greatest concern and determine how remaining exploitable vulnerabilities translate into operational risk. The DAA must also consider the ISSO's plan to handle the risks as declared in the POA&M and any planned or completed corrective actions to reduce or eliminate the risk.

The duration of an ATO must be at least six (6) months and can be no longer than three (3) years.

12.4.2 Accreditation Package Transmission

- Provide copies of the final Accreditation Package, including the Accreditation Decision Letter in either paper or electronic form to the System Owner and any other agency officials having an interest (i.e., need to know) in the security of the information system.
- DAA signs the Accreditation Decision Letter.
- Upload Accreditation Package to TAF.

12.4.3 C&A Document Updates

The following subtasks are required to complete the C&A documentation updates:

- Update the SSP based on the final determination of risk to DHS/Component operations, DHS/Component assets, or individuals.
- Develop POA&M items for all risks that are to be mitigated to include funding sources, funding levels, and schedule milestones. Requirements for POA&M development are specified in *DHS 4300 Sensitive Systems Handbook*, Attachment H, *POAM Process Guide*.

12.5 Accreditation Output

The output of the Accreditation Process is

- The Accreditation Decision Letter

The accreditation decisions that can be rendered by the DAA are:

- **Authorization to Operate (ATO):** If, after assessing the results of the security certification, the DAA accepts risk to agency operations or assets, an authorization to operate is issued for the information system. The information system can be

accredited without any significant restrictions or limitations on its operation or conditions on the ATO may be imposed.

- **Denial of Authorization to Operate:** If, after assessing the results of the security certification, the DAA finds that the risk to agency operations or assets is unacceptable, the authorization to operate the information system is denied. The information system is not accredited and must be removed from operation (or not be placed into operation).

12.6 CFO Designated Financial Systems

As specified in Section 3.15 (e), *DHS Sensitive Systems Policy Directive 4300A*, all accreditations for CFO Designated Financial Systems must be approved and signed by the DAA and by the Component CFO.

13. Continuous Monitoring and Annual Assessment Process

Continuous Monitoring consists of tasks that provide on-going monitoring of the internal security controls implemented for DHS information systems, and communicate to key personnel involved in the C&A process any changes to DHS information systems that may impact security and/or the current system authorization status. Continuous Monitoring is a proven technique to address the security impacts on information systems resulting from changes to the hardware, software, firmware, or operational environment. An effective Continuous Monitoring program requires:

- CM and change control processes for the information system
- Security impact analyses on changes to the information system
- Assessment of selected security controls in the information system and security status reporting to appropriate agency officials

The objective of Continuous Monitoring is to ensure that risk is kept within an acceptable level for all DHS information systems. DHS requires periodic testing and evaluation of the security controls in an information system to ensure that the controls are effective in their application. Security control monitoring (i.e., verifying the continued effectiveness of those controls over time) and reporting the security status of the information system to appropriate agency officials are essential activities of a comprehensive information security program. This C&A Guide contains a brief overview of activities needed for Continuous Monitoring and conducting annual assessments, whereas a complete description of those activities is contained in the ISSO Guide.

The ongoing monitoring of security control effectiveness can be accomplished in a variety of ways including security reviews, self-assessments, security testing and evaluation, or audits. Components should consult NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems*.

13.1 Purpose

The purpose of the Continuous Monitoring Phase is to provide oversight and monitoring of security controls and to inform the DAA or designated representative when changes occur that may impact the security of the information system. Effective information security programs should include an aggressive Continuous Monitoring program to check the status of the security controls in the information system on an ongoing basis. Continuous Monitoring ensures that C&A is not a one-time event within DHS.

It is necessary to identify any significant changes to the system configuration or to the operational/threat environment that might affect system security. DHS must re-accredit its information systems every 3 years or whenever a major change occurs, whichever occurs first.

13.2 Decision Making Factors

Overall, change control should concern itself with whether information assurance objectives will be met whenever changes are implemented. Once a need for change has been established, the

impact of the change must be assessed. System changes may affect dataflow requirements, communication with other systems or applications, and operational support functions.

The timing of related SELC activities must be understood when scheduling the implementation, testing, and validation of changes.

The ability to test proposed changes and the ability to validate the impact to system security profile after actual changes have been implemented are important factors.

13.3 Input

Table 23 identifies the input for the Continuous Monitoring Process.

Table 23. Input for the Continuous Monitoring Process

Input	Source
CM Plan	System Owner
SSP	RMS
POA&M	TAF
SRTM	RMS
RA	RMS

13.4 Tasks

13.4.1 Conduct Annual Assessment

Security Controls shall be assessed annually as part of the Continuous Monitoring Process. Standard evaluation procedures and techniques, similar to the ST&E procedures and techniques, shall be employed to determine the effectiveness of the security controls. It is important to

- Identify a sub-set of the security controls that should be evaluated to determine the continued effectiveness of those controls in providing an appropriate level of protection.
- Evaluate the agreed-upon sub-set of security controls.

These procedures are defined in TAF in the Security Controls Tab. DHS uses the annual assessment to perform the security control validation. The annual assessment results are recorded in TAF. In the years that ST&E is performed, it is not necessary to conduct a separate Annual Assessment. Please refer to Figure 10 Relationship of ST&E Results and Annual Assessments above. However, the ST&E Results must be entered into TAF on the Security Controls tab.

13.4.2 Annual ISA Review

ISAs are to be reviewed and updated as needed as a part of the Annual Assessment.

Components shall document all interconnections to the DHS OneNetwork (OneNet) with an ISA, signed by the OneNet DAA and by each applicable DAA.

- Ensure that ISAs are maintained for all connections that do not share the same security policy.

- Ensure completion of MOUs, MOAs, and ISAs for CFO Designated Financial System interconnections with any system not owned by DHS; ensure that they include appropriate security clauses; and monitor service provider for compliance with MOUs, MOAs, and ISAs.
- Ensure that the interconnected system has a current ATO.
- Ensure that the interconnected system has no PO&AM items affecting the interconnection. If a POA&M item affects the interconnection, then it must be recorded in the primary system POA&M, so that the risk associated with it can become known to the DAA via the Continuous Monitoring status reporting mechanism.

13.4.3 Document System Changes

- Document and record any relevant information about proposed or actual changes to the system hardware, firmware, or software, in accordance with DHS Component CM practices and the DHS Acquisition Management policies.
- Document any changes to the operating environment, including modifications to the physical environment.
- Provide formal documentation of system changes to the ISSO.
- Revise DHS Component engineering and support baselines for all approved change requests.

13.4.4 Operating System and Network Patch Management

Patch management assists in the process of lowering the potential risk to the system by repairing known vulnerabilities in the system environment. The ISSO must ensure all patches and upgrades do not adversely impact either the performance or security posture of the system. In addition, patch management activity must comply with the Enterprise Vulnerability Management System (EVMS). The ISSO must subscribe to and adhere to instructions from EVMS Alerts and EVMS Bulletins.

Once the need for a patch has been identified, a change request should be submitted to the system support agent (or appropriate decision-making authority). To accomplish Operating System (OS) and Network Patch Management correctly, the following steps should be followed:

1. Submit Engineering Change Request (ECR) to Configuration Manager for all patches and upgrades.
2. Verify impact of change in system test bed for impact to information security and system settings.
3. Deploy relevant and tested patches to eliminate known vulnerabilities in systems and applications once it has been determined that the patch has no detrimental effect on security controls.

13.4.5 Security Impact Analysis

Analyze proposed and actual system changes to determine the information security impact of such changes. Specifically,

- Analyze and evaluate the security impact of proposed changes.

- Assess and validate the security impact of actual changes.
- Provide documentation of security impact analysis to ISSO

13.4.6 Security Control Selection

Security controls should be selected to reflect DHS Information Security priorities, and the importance of the information system to DHS operations. Those security controls that, if compromised, would result in the greatest harm to DHS operations and assets should be monitored, and their effectiveness evaluated, on a regular basis. The DHS Performance Plan identifies key controls to be tested each year. For High System Security Level information systems, a greater number and breadth of security controls shall be monitored on a regular basis. Conversely, a smaller number of security controls may be monitored for Low System Security Level systems. In cases where a system is deployed at many sites, a common set of security controls across all sites is desirable. Although site-specific environments may very well dictate that unique security controls be selected for some sites, a goal of this task is to minimize the number of the site-specific controls. Security Control Selection is comprised of the following activities:

- Identify and select a set of security controls to be monitored regularly.
- Determine the monitoring interval based on system security level.
- Conduct an annual review of the set of the selected security controls to be monitored with the ISSO.

13.4.7 Security Reporting and Documentation

Update the SSP so it reflects the most recent proposed or actual system changes and the potential security impact associated with each change, and to report the proposed or actual changes and associated security impact to the Component CISO and DAA.

The SSP should be updated to ensure that the plan contains the most current security-related information. During each update of the SSP, the System Security Level designation shall be re-evaluated.

- Update the SSP based upon the documented system changes and the results of the ongoing security control monitoring process.

It is crucial at DHS is to maintain up-to-date information in TAF so that the reports can be extracted. Updates to TAF should be made every month.

TAF serves as the repository of security metrics used for development of the monthly Information Assurance (IA) Compliance Scorecards, and the quarterly and annual FISMA reports. ISSOs are responsible for ensuring that the data in TAF is up-to-date. Monthly updates to all data are required, especially the status of weaknesses in the POA&M section.

13.5 Output

The following are output from the Continuous Monitoring Process:

- New RA
- Updated SSP

- Updated SRTM
- Updated POA&M

Appendix A. Information Assurance Compliance System

The Department of Homeland Security (DHS) Chief Information Security Officer (CISO) is responsible for ensuring DHS information security is consistent and complies with the goals and objectives set forth by federal and agency legislation, regulations, policies, directives, and standards. To support the accomplishment of these responsibilities, the CISO implemented the Information Assurance (IA) Compliance System. The IA Compliance System includes two commercial, web-based, enterprise applications that are hosted at a contractor owned and operated facility. The two applications are:

- **TrustedAgent FISMA (TAF):** The DHS Federal Information Security Management Act (FISMA) reporting application from Trusted Integration, Inc.
- **Risk Management System (RMS):** The DHS Certification and Accreditation (C&A) management tool from SecureInfo, Inc.

These applications facilitate security management, enterprise FISMA reporting, and C&A completion. These applications are available to all authorized users through the Intranet. *DHS Sensitive Systems Policy Directive 4300A* and *DHS 4300A Sensitive Systems Handbook* mandates their use for all sensitive systems. The core activities of creating and uploading C&A documents and collecting and reporting the information security metrics is managed through the use of these applications. These applications facilitate the collection and reporting of data in a fashion that can be aggregated across the Department. Figure 11 illustrates how these applications support implementation of information security policies and procedures across the Department.

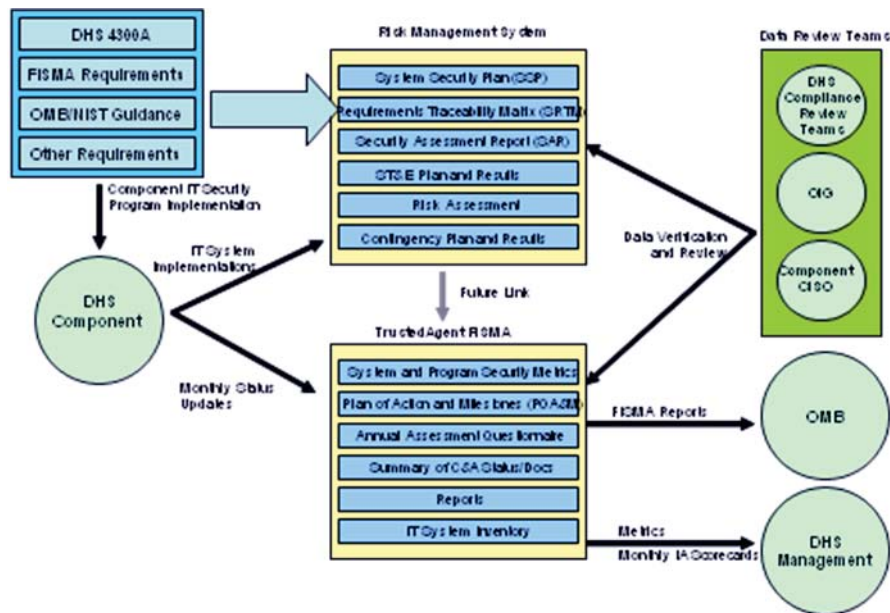


Figure 11. IA Compliance System Policy Implementation

A.1 TrustedAgent FISMA

TAF is used to facilitate FISMA reporting within DHS and the DHS Components. It is used for the Office of Management and Budget (OMB) mandated enterprise management of FISMA data, including National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 annual-assessments, Plan of Action and Milestones (POA&M), a consolidated Component inventory of information systems, and OMB information security performance metrics. TAF manages the collection and reporting of the following types of information:

- Status of all Component security programs and their compliance with DHS metrics
- POA&M by system, identifying deficiencies, sources of deficiencies, prioritization, and specific remediation plans
- Annual Assessments for each DHS system
- C&A documents and their approval status
- Quarterly and Annual FISMA Reports and data for the IA Compliance Monthly Scorecards
- Official DHS Information System Inventory for the Headquarters and each Component
- Contact information for each DHS system

Authorized DHS employees and contractors input general information such as the system name, assessment type, evaluation date, assessment purpose, and criticality levels. The system provides automation support for conducting NIST SP 800-53 system assessments through a standard set of questions or a customized template assigned to the user. Noncompliance issues that are identified during the annual assessments and independent audits are created, edited, or deleted. Weaknesses and milestones from self assessments and audits are maintained in an enterprise

database. Linkages with the capital planning and investment (OMB Exhibit 300) and RMS packages may occur in the future.

A.1.1 TAF Content

The information systems, programs, and sites included in TAF for each Component are managed by the DHS Inventory Team. The information for each system, program, and site is organized in Tabs as illustrated in Figure 12.



Figure 12. System View

Table 24 summarizes the information recorded and managed in each tab.

Table 24. TrustedAgent FISMA Tab Descriptions

Tab	Information Recorded and Managed
Identification	<ul style="list-style-type: none"> • General assessment • System description, • Security categorization • Capital planning data
People and Inventory	<ul style="list-style-type: none"> • User access • Points of contact • Interconnections between internal and external DHS systems • Hardware and software inventory • Configuration Management Status • Systems/ subsystems
Security Controls	<ul style="list-style-type: none"> • The security controls that must be reviewed, tested, and evaluated • Status of the security control reviews
POA&Ms	<ul style="list-style-type: none"> • All of the weaknesses and audit recommendations that exist for a program, system, or site • Milestones for each weakness and recommendation • Contains features to navigate through the assessment questions (sequential/tree), setting the security effectiveness levels, and display the Weakness form (to add a new weakness or view/edit an existing weakness).
C&A Tracking	<ul style="list-style-type: none"> • Status and dates of C&A documents • C&A documents to include: • Approval status of C&A documents
Reports	Reports on the security status of the program, system, or site

A.1.2 Accessing TAF

The TAF production website is located at <https://tafisma.dhs.gov>.

A.2 Risk Management System

RMS is used for developing, tracking, and managing the requirements and supporting documentation necessary for effectively managing information system security. RMS provides a questionnaire that allows System Owners and/or Information System Security Officers (ISSOs) to identify the basic elements of the system such as the security categorizations of confidentiality, integrity, and availability; and data characteristics - e.g., financial data or Personally Identifiable Information (PII) to automatically generate a set of federal and departmental requirements necessary for operating the information system(s) in a safe and secure manner. Users have the ability to add unique requirements to build a comprehensive set of requirements for the system under consideration. RMS uses the requirements to generate a Security Requirements Traceability Matrix (SRTM) and a set of C&A document templates:

- System Security Plan (SSP)
- Risk Assessment (RA)
- Contingency Plan (CP)
- Contingency Plan Test Results (CPT)
- Security Test and Evaluation (ST&E) Plan
- Security Assessment Report (SAR)
- Accreditation Decision Letter
- Interconnection Security Agreement (ISA)
- Memorandum of Understanding (MOU)
- Memorandum of Agreement (MOA)

A.2.1 C&A Package

RMS organizes information by C&A Package. The C&A Package contains more documents than the Accreditation Package submitted to the Designated Accrediting Authority. The C&A Package includes the following security documents:

- Accreditation Decision Letter
- Contingency Plan (CP)
- Contingency Plan Test Results (CPT)
- E-Authentication Levels and Determination and Workbook
- Federal Information Processing Standards (FIPS) 199 Security Categorization and Workbook
- Information System Security Officer (ISSO) Letter(s)

- POA&M (reflects SAR & Accreditation Decision Letter)
- PTA
- RA
- SAR
- SSP
- ST&E Plan

A.2.2 Accessing RMS

The RMS production website is located at <https://canda.dhs.gov/rms>.

A.3 DHS Compliance Help Desk

The DHS Compliance Help Desk provides Level 1 help desk support which includes receiving initial calls or emails, logging and triage of calls, troubleshooting, and referring unresolved calls to appropriate Level 2 contacts. The help desk can provide copies of DHS documents mentioned in this guide and can provide limited assistance on using the applications.

The DHS Compliance Help Desk is available during normal business hours to answer questions regarding usage of the TAF and RMS. Help desk contact information is:

- Email: dhsinfosechelpdesk@dhs.gov

A.4 Getting TAF and RMS Accounts

TAF and RMS are web-based and can be securely accessed from the Internet. TAF and RMS account requests are made via the Component CISO or designated Point of Contact (POC) to the DHS Compliance Help Desk. The following information is required to obtain an account:

- First and last name
- Email address
- Phone number
- Role Requested (e.g., Component CISO, ISSO, Security Analyst)
- Component
- System and program

The Component CISO or designated POC is responsible for ensuring that the names submitted for user accounts are valid users for access to DHS information systems and have a valid need to access the systems. They are also responsible for ensuring that accounts that are no longer valid are reported to the help desk.

Appendix B. Certification and Accreditation Document Quality Reviews

In addition to the document acceptance process conducted by the Security Officer (CISO), Information System Security Officer (ISSO), Certifying Official, and Designated Accrediting Authority (DAA), all Department of Homeland Security (DHS) Certification and Accreditation (C&A) documents are subject to independent quality reviews as directed by the DHS Chief Information Security Officer (CISO). The quality review process and its output are illustrated in Figure 13. As illustrated in the figure, information security professionals conduct security document quality reviews (indicated by blue boxes). The DHS Privacy Office reviews privacy documents (indicated by the green boxes). Pass/Fail results are maintained in TrustedAgent FISMA (TAF). Monthly POA&M Reports and System Assessment Reports are provided to System Owner.

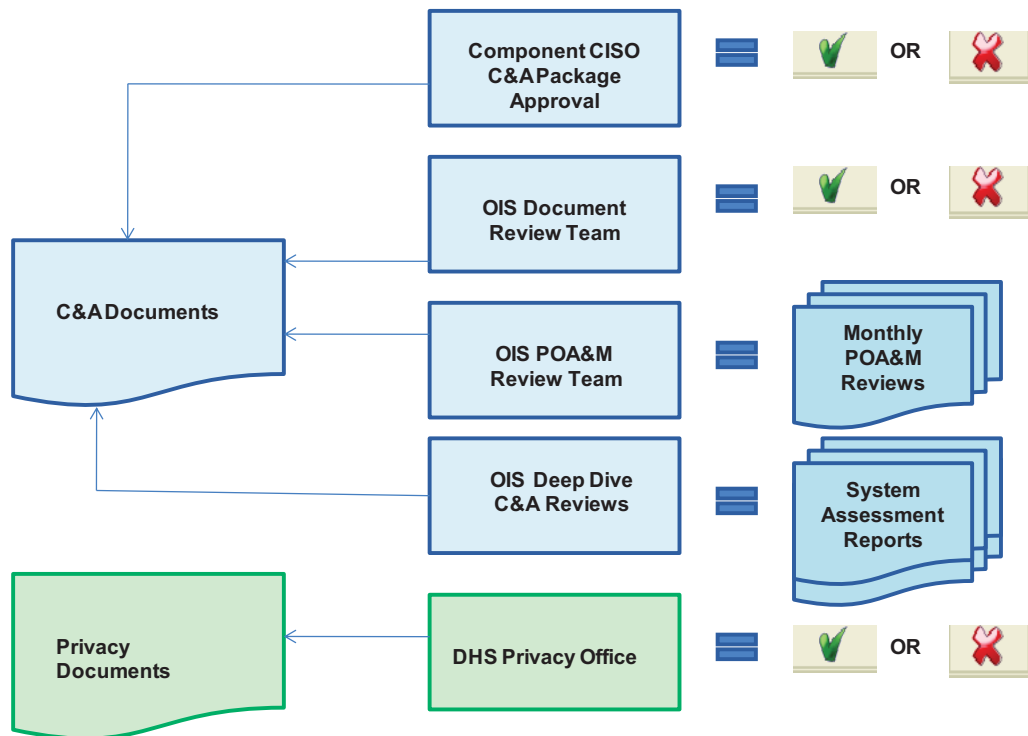


Figure 13. DHS C&A Quality Review Process

B.1 Component CISO C&A Package Approval

TAF contains a Component CISO validation feature. A user with CISO rights can click on the phrase “Not Started” under CISO Validation to change the status to ‘Pass’ or ‘Fail’ and enter comments. Criteria for Component CISO validation are Component-specific. All C&A Package artifacts and e-Authentication documents must be reviewed and approved by the Component CISO. At a minimum, the review criteria in current *DHS Information Security Performance Plan* should be confirmed prior to the Office of Information Security (OIS) Document Review. Additional criteria may be established by the Component.

B.2 OIS Document Review Team

Once the Component CISO validates a C&A Package, the OIS Review Team reviews the C&A Package. The criteria for initiation of an OIS Document Review Team are noted in Section 1.9 of the *DHS C&A Guide*.

The OIS Document Review Team reviews all of the documents submitted as part of the C&A process against a minimum set of quality standards set forth in the current *DHS Information Security Performance Plan*. The primary objective of OIS Document Review Team is to ensure consistency across C&A documents produced by every Component and assure a basic level of completeness for the documents. In addition to the document reviews, a follow-up conference call will be held. Once the OIS has completed the C&A Package review, a detailed list of issues will be provided and a conference call will be setup through the Component CISO. The conference call will enable the Components to provide immediate feedback and allow the OIS to verify and lingering questions. Specific discussion will focus on definition of the accreditation boundaries as well.

B.3 OIS POA&M Review Team

The Plan of Action and Milestones (POA&M) review team, provided by the CISO, is responsible for ensuring the department's weakness remediation process and that documents comply with established goals. Many of the routine activities have been incorporated into the POA&M Quality Checklist in the current *DHS Information Security Performance Plan*. However, several subjective reviews are still required in areas on delay reasoning, estimated POA&M resources, and to ensure an effective program. In addition, the team reviews all audit findings to identify gaps in the reported POA&M compliance.

B.4 OIS Deep Dive C&A Reviews

The OIS Deep Dive C&A Review teams are assigned by the CISO and provide an independent verification of the system security controls. The Deep Dive C&A Review is independent of the verification performed during normal Security Test and Evaluation (ST&E) processing. As a verification activity, it focuses on the actual implementation of security controls to ensure that controls described in the System Security Plan (SSP) are (in fact) implemented correctly. The verification of security controls is accomplished by means of:

- Technical testing (software/hardware)
- Technical automated tools (scripting)
- Physical testing and/or inspection
- Documentation and procedural reviews
- Walk-through inspections
- Interviews with key personnel

The deliverable produced by this team is a gap analysis report highlighting discrepancies that exist between the system security posture outlined in the C&A documentation and the actual system security posture discovered in an on-site review of system security controls. In addition, the OIS Deep Dive C&A Review Team provides specific metrics regarding shortfalls across many system types, Components and organizations, and control areas that need improvement

(e.g., patches, open ports). These metrics are useful for adjusting security policies and focusing effort in areas where most of the vulnerabilities exist.

B.5 DHS Privacy Office

The DHS Privacy Office owns the DHS Privacy policy and procedures. The office reviews and approves all Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), and System of Records Notice (SORN) documents.

Appendix C. List of Attachments

Attachment A	DHS Risk Assessment Template
Attachment B	DHS System Security Plan Template
Attachment C	DHS Security Test and Evaluation Plan Template
Attachment D	DHS Security Assessment Report Template
Attachment E	DHS Contingency Plan Template
Attachment F	DHS Contingency Plan Test Results Template
Attachment G	Accreditation Decision Letter Template
Attachment H	Interconnection Security Agreement Template
Attachment I	Memorandum of Understanding (MOU) Template
Attachment J	Memorandum of Agreement (MOA) Template

Acronyms

ATO	Authorization to Operate Authority to Operate
BRM	Business Reference Model
C&A	Certification and Accreditation
CFO	Chief Financial Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CO	Certifying Official
CP	Contingency Plan
CPO	Chief Privacy Officer
CPT	Contingency Plan Test
DAA	Designated Accrediting Authority
DHS	Department of Homeland Security
ECR	Engineering Change Request
FedCIRC	Federal Computer Incident Reporting Center
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
GFE	Government Furnished Equipment
GSS	General Support System
IA	Identification and Authentication Information Assurance
IG	Inspector General
IS	Information System
ISA	Interconnection Security Agreement
ISSO	Information System Security Officer

IT	Information Technology
ITAR	Information Technology Acquisition Review
MA	Major Application
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIS	Office of Information Security
OMB	Office of Management and Budget
OS	Operating System
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPOC	Privacy Point of Contact
PTA	Privacy Threshold Analysis
RA	Risk Assessment
RMS	Risk Management System
ROB	Rules of Behavior
SAR	Security Assessment Report
SELC	Systems Engineering Life Cycle
SDLC	System Development Life Cycle
SIIP	System Interconnection Implementation Plan
SLA	Service Level Agreement
SORN	System of Records Notice
SP	Special Publication
	Entity-wide Security Program Planning and Management (FISCAM)
SRTM	Security Requirements Traceability Matrix

SSH	Sensitive Systems Handbook
SSP	System Security Plan
ST&E	Security Test and Evaluation
TAF	TrustedAgent FISMA
VLAN	Virtual Local Area Network

Glossary

Acceptable Risk	Mission, organizational, or program-level risk deemed tolerable by the DAA to incur after adequate security has been provided.
Accreditation Boundary	The logical extent of the system defined in the SSP. Synonymous with Certification Boundary.
Accreditation Decision	A formal decision by the DAA to grant an Authorization-to-Operate (or a Denial of Authorization-to-Operate).
Accreditation Decision Letter	A formal letter from the DAA to the System Owner containing the decision to accredit (not accredit) an information system. Also referred to as ATO Letter.
Accreditation Package	The documents submitted to the DAA for the Accreditation Decision. An Accreditation Package consists of: <ul style="list-style-type: none">• Accreditation Decision Letter• System Security Plan• Security Assessment Report• Plan of Action and Milestones
Annual Assessment	DHS activity for meeting the annual FISMA self-assessment requirement.
ATO Letter	Synonymous with the more formal Accreditation Decision Letter
C&A Package	The set of documents required by DHS for a complete C&A. These documents are: <ul style="list-style-type: none">• Accreditation Decision Letter• CP• CPT• E-Authentication Levels and Determination and Workbook• Federal Information Processing Standards (FIPS) 199 Security Categorization and Workbook• Information System Security Officer (ISSO) Letter(s)• POA&M (reflects SAR & Accreditation Decision Letter)• PTA• RA• SAR• SSP• ST&E Plan
Certification/ Certifying Agent	A contractor that performs certification tasks as designated by the CO.
Certification Boundary	The logical extent of the system defined in the SSP.

Certifying Official	A senior management official who certifies the results of the Security Assessment. Must be a Government Employee.
Detective Control	Controls designed to warn of conditions that violate security policy.
Compensating Control	An internal control intended to reduce the risk of an existing or potential control weakness.
Operational Risk	The risk contained in a system under operational status. It is the risk that a DAA accepts when granting an ATO.
Preventive Control	Controls designed to inhibit conditions that violate security policy.
Residual Risk	The risk remaining after security measures have been applied.
System	A discrete set of information system assets contained within the accreditation boundary.

References

1. Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, May 2004.
2. NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
3. NIST Special Publication 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.
4. NIST Special Publication 800-39, *DRAFT Managing Risk from Information Systems: An Organizational Perspective*, April 2008.
5. NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, December 2007.
6. NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, June 2008.
7. NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.
8. NIST Special Publication 800-63, *Electronic Authentication Guideline*, April 2006.
9. NIST Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*, June 2004.
10. NIST Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.
11. *DHS Sensitive Systems Policy Directive 4300A*.
12. *DHS 4300A, Sensitive Systems Handbook*.
13. *DHS 4300A, Sensitive Systems Handbook*, Attachment H, *Plan of Action and Milestones (POA&M) Process Guide*.
14. *DHS 4300A, Sensitive Systems Handbook*, Attachment R, *Compliance Framework for CFO Designated Financial Systems*.
15. *DHS 4300A, Sensitive Systems Handbook*, Attachment S, *Compliance Framework NIST SP 800-53 Controls for Privacy Sensitive Systems*.
16. *DHS Information Security Categorization Guide, FIPS 199 Workbook, and E-Authentication Workbook*.
17. *DHS FISMA Inventory Methodology*.
18. *DHS ISSO Guide (first expected publication in 2009)*

ESTABLISHING OR CONTRACTING WITH FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTERS (FFRDCs) AND NATIONAL LABORATORIES

I. Purpose

This Management Directive (MD) defines Department of Homeland Security (DHS) policies and procedures regarding the establishment, administration, and use of Federally Funded Research and Development Centers (FFRDCs) and related sponsoring agreements. This MD explains, for any DHS Component that seeks to sponsor an FFRDC task, the required interactions with DHS Science and Technology Directorate (S&T). These interactions do not necessarily represent all legal, financial, or contractual obligations nor do they seek to limit competition or contracting with the private sector. This MD replaces the DHS FFRDC Management Plan dated July 21, 2004.

II. Scope

A. This MD addresses the establishment of new DHS-sponsored FFRDCs; establishment of DHS participation in multiple agency sponsorship agreements for existing FFRDCs; management and administration of FFRDC sponsoring agreements, whether DHS is the primary sponsor or party to a multiple agency sponsorship agreement; and DHS use of other Departments' FFRDCs, regardless of whether DHS is a party to the FFRDC sponsoring agreement.

B. This MD is applicable to all DHS Components. This MD is released in cooperation with the DHS Office of the Chief Procurement Officer and the S&T Office of General Counsel (OGC).

III. Authorities

A. 6 U.S.C. Section 185, Federally funded research and development centers.

B. 6 U.S.C. Section 186(b), Miscellaneous Provisions/Coordination Requirements.

- C. 6 U.S.C. Section 189, Utilization of Department of Energy laboratories and sites in support of homeland security activities.
- D. 31 U.S.C. Section 1535, the Economy Act.
- E. 41 U.S.C. Section 253(c)(3)(B), Procurement procedures.
- F. Federal Acquisition Regulation (FAR) 17.5, Interagency Agreements under the Economy Act.
- G. Federal Acquisition Regulation (FAR) 35.017, Federally funded research and development centers.
- H. DHS Directive 125-02, Interagency Agreements.
- I. DHS Management Directive 10100, Organization of the Office of the Under Secretary for Science and Technology.
- J. Memorandum of Agreement Between the Department of Energy and the Department of Homeland Security, dated February 23, 2003.

IV. Definitions

- A. **Acquisition Planning**. Acquisition planning means the process by which the efforts of all personnel responsible for an acquisition are coordinated and integrated through a comprehensive plan for fulfilling the agency need in a timely manner and at a reasonable cost. It includes developing the overall strategy for managing the acquisition.
- B. **Contracting Activity**. As referred to in this MD, the DHS contracting activity is the governmental entity that awards a contract or contracts under the authority of 6 U.S.C. § 185 for FFRDCs.
- C. **Core Statement**. The core statement describes the purpose and mission of the FFRDC, the nature of the strategic relationship between the FFRDC and DHS, the general scope of efforts to be performed for DHS, and core competencies the FFRDC must maintain so that it can assist in accomplishing the DHS mission.
- D. **Core Work**. Core work is work appropriate for performance by the FFRDC because it is consistent with the mission, purpose, and competencies of the FFRDC, and draws on or sustains a strategic relationship between the FFRDC and its sponsor.

E. **Federally Funded Research and Development Centers.**

1. FFRDCs can take a variety of forms including, but not limited to those that perform systems engineering, conduct studies and analyses, or operate a national laboratory. FFRDCs provide a unique service to the government and include organizations such as national laboratories associated with federal agencies.
2. An FFRDC meets certain special long-term research or development needs that cannot be met as effectively by existing in-house or contractor resources. In addition to meeting long-term and intermediate-term needs of sponsor(s) and users, FFRDCs enable agencies to use private sector resources to accomplish tasks that are integral to the mission and operations of their sponsor(s).
3. FFRDCs are outside the government to permit the management flexibility necessary to attract and retain high-quality scientific, technical, and analytic expertise and to provide an independent perspective on the critical issues that they address for their sponsor(s) and users.
4. Long-term relationships between the government and FFRDCs are desirable in order to provide the continuity that will attract high-quality personnel to the FFRDC. This relationship should be of a type to encourage the FFRDC to maintain currency in its field(s) of expertise, maintain its objectivity and independence, preserve its familiarity with the need(s) of its sponsor(s), develop institutional DHS memory, and provide a quick response capability.
5. An FFRDC has access, beyond that which is common to the normal contractual relationship, to government and supplier data, including sensitive and proprietary data, and to government employees and facilities. The FFRDC is required to conduct its business in a manner befitting its special relationship with the government, to operate in the public interest with objectivity and independence, to be free from organizational conflicts of interest, and to have full disclosure of its affairs to the sponsoring agency.
6. FFRDCs may be operated, managed or administered by a university or consortium of universities, other not-for-profit or nonprofit organization, an industrial firm as an autonomous organization or as an identifiable separate operating unit of a parent organization under a strict conflict of interest regime to prevent the influence of shareholders of the for-profit board, which could undermine the objectivity of the FFRDC organization.

7. An FFRDC may not use its privileged information or access to facilities to compete with the private sector. With few exceptions, FFRDCs may not participate in competitive procurements by the U.S. government.

F. **Multiple Agency Sponsorship Agreement.** A multiple agency sponsorship agreement is a written document between the government (primary sponsor and other sponsors) and the FFRDC's parent institution that contains a core statement for each sponsor as well as other items identified in FAR 35.017-1.

G. **Nonsponsor.** A nonsponsor is any other organization, in or outside of the federal government, which funds specific work to be performed by the FFRDC but is not a party to the sponsoring agreement or multiple agency sponsorship agreement.

H. **Parent Institution.** The parent institution is the entity that contracts with the primary sponsor to operate the FFRDC or a national laboratory. FFRDCs may be operated, managed, or administered by many different types of organizations, as described in paragraph IV.E.6. above. A parent institution may also be called a parent organization.

I. **Primary Sponsor.** The primary sponsor is the lead agency responsible for managing, administering, or monitoring overall use of the FFRDC under a multiple sponsorship agreement on behalf of DHS. The US(S&T) is the primary sponsor for DHS FFRDCs. Multiple agency sponsorship is possible as long as one agency agrees to act as the "primary sponsor."

J. **Sponsor.** A sponsor is an executive agency which manages, administers, monitors, funds, and is responsible for the overall use of an FFRDC, other than the primary sponsor, that is party to a multiple agency sponsorship agreement. The US(S&T) is the DHS sponsor for DHS use of a non-DHS FFRDC under a multiple agency sponsorship agreement.

K. **Sponsoring Agreement.** The sponsoring agreement is a written agreement between the government (primary sponsor) and the FFRDC's parent institution that is prepared when the FFRDC is established. The sponsoring agreement contains the core statement as defined herein, as well as other items identified in FAR 35.017-1.

L. **Strategic Relationship**. The nature of their mission requires that FFRDCs operate in a strategic relationship with their sponsor(s) and other users. Strategic relationships enable FFRDCs to develop and maintain in-depth institutional knowledge of the sponsor's programs and operations; to maintain continuity and currency in their special fields of expertise, and a high degree of competence in their staff and work; to maintain their objectivity and independence; and to respond effectively to the emerging needs of the sponsor(s) and other users.

M. **User**. The user, or tasking activity, is an entity that requires the services of an FFRDC for performance of work.

V. Responsibilities

Consistent with the provisions of this MD, the US(S&T) is responsible to the Secretary of DHS to:

- A. Oversee the implementation and execution of this MD.
- B. Ensure all DHS work proposed to be placed with any FFRDC is within the purpose, mission, general scope of effort, or special competency of the FFRDC.
- C. Oversee each FFRDC for which DHS is the primary sponsor by:
 - 1. Ensuring that the sponsoring agreement is consistent with FAR 35.017-1 and contains a core statement that is specific enough to differentiate between work that is within the scope of effort for which the FFRDC is intended and work that should be performed elsewhere.
 - 2. Working closely with the contracting activity and potential users early in the acquisition planning process.
 - 3. Serving as the single DHS point of contact to conduct reviews (in consultation with the contracting activity and the S&T OGC) and recommending to the contracting activity authorization of work by DHS FFRDCs via Inter-Agency Agreements. Such reviews will ensure that all work proposed by DHS users to be performed by the FFRDC is suitable for an FFRDC and within the purpose, mission, general scope of effort, or special competency of the FFRDC as delineated in the core statement. Legal review by S&T OGC does not supersede the need for a Component legal sufficiency review.

4. Consulting regularly with the DHS Office of the Chief Procurement Officer to ensure that DHS FFRDC operational practices are consistent with prevailing federal standards on FFRDC management and to ensure that DHS FFRDC interests are properly represented with the FAR Council, with the Office of Federal Procurement Policy (OFPP), and similar groups that establish overarching federal contracting policies.

5. Ensuring, in consultation with S&T OGC, that there are proper mechanisms in place for the DHS FFRDCs to report their development of federally funded intellectual property, track and report on such federally funded intellectual property as required by applicable law and DHS policies, and promote the technology transition of such developments to end users.

6. Assuring the Secretary that the above provisions are being satisfied by making a specific statement in the Annual Review Assessment required in accordance with [Appendix A](#).

D. Oversee DHS use under a multiple agency sponsorship agreement of FFRDCs for which DHS is not the primary sponsor by:

1. Ensuring that the multiple agency sponsorship agreement contains a DHS-specific core statement defining the nature of the strategic relationship between the FFRDC, its primary sponsor, and DHS; the general scope of efforts to be performed for DHS; and core competencies the FFRDC must maintain so that it can assist in accomplishing the DHS mission.

2. Serving as the single DHS point of contact to conduct reviews of proposed actions (in consultation with the contracting activity and S&T OGC) and recommending to the contracting activity authorization of work by such FFRDCs. Such reviews will ensure that all work proposed by DHS users to be performed by the FFRDC is suitable for an FFRDC and within the purpose, mission, general scope of effort, or special competency of the FFRDC as delineated in the DHS-specific core statement.

3. Consulting regularly with the DHS Office of the Chief Procurement Officer to ensure that DHS FFRDC operational practices are consistent with prevailing federal standards on FFRDC management and to ensure that DHS FFRDC interests are properly represented with the FAR Council, with OFPP, and similar groups that establish overarching federal contracting policies.

4. Ensuring, in consultation with S&T OGC, that there are proper mechanisms in place for the FFRDCs to report their development of federally funded intellectual property, track and report on such federally funded intellectual property as required by applicable law and DHS policies, and promote the technology transition of such developments to end users.

5. Ensuring, on behalf of the Secretary and all other FFRDC customers, that the multiple agency FFRDCs to which DHS is a sponsor, but not the primary sponsor, are being continually assessed for quality, cost-effectiveness, conformity with the policies in this MD, and return on investment factors using Annual Review Assessment required in accordance with [Appendix A](#).

E. Oversee DHS use of non-DHS-sponsored FFRDCs (i.e., DHS is neither the primary sponsor nor a party to a multiple agency sponsorship agreement) by:

1. Acting as the primary DHS focal point for work to be performed by non-DHS FFRDCs and reviewing descriptions of work to ensure that the work is within the scope of the non-DHS FFRDC. Such reviews will ensure that work proposed by DHS users to be performed by a non-DHS FFRDC is suitable for that FFRDC and within its purpose, mission, general scope of effort, or special competency of the FFRDC as delineated in the core statement. US(S&T) will further review descriptions of all work to ensure that the work could not be appropriately performed by a DHS-sponsored FFRDC (i.e., DHS is either the primary sponsor or a party to a multiple agency sponsorship agreement) and that the work is (a) appropriate for an FFRDC and (b) consistent with that FFRDC's sponsoring agreement. If the proposed work is within the core statement of a DHS-sponsored FFRDC, the US(S&T) will work with the users to determine whether the proposed use of the non-DHS-sponsored FFRDC is appropriate.

2. Acting as the primary DHS focal point for work to be performed by DOE national laboratories pursuant to a "work for others" arrangement formalized by the Memorandum of Agreement Between Department of Energy and Department of Homeland Security dated February 23, 2003, and in accordance with 6 U.S.C. § 189(a)(1)(c). The DHS Office of National Laboratories (within the US(S&T)) will be the primary point of contact to conduct reviews (in consultation with S&T OGC, as required) and recommend contracting activity approval of work by such DOE national laboratories via an Inter-Agency Agreement. Pursuant to 6 U.S.C. § 189(g), the DHS Office of National Laboratories will review all statements of work issued from DHS and directed to DOE national laboratories prior to preparation of a final procurement requisition package and submission to the DHS contracting activity for processing. Such

reviews will ensure that work proposed by DHS users to be performed by the DOE national laboratories complies with the terms and conditions of the prime contracts between DOE and each of the national laboratory operators.

3. Ensuring, in consultation with S&T OGC, that there are proper mechanisms in place for the non-DHS FFRDCs to report their development of federally funded intellectual property, track and report on such federally funded intellectual property as required by applicable law and DHS policies, and promote the technology transition of such developments to end users.

F. Liaise with other federal agencies that operate FFRDCs to ensure that DHS FFRDC management practices and procedures represent the “best practice” among federal agencies.

The reviews and other requirements of this section are intended to represent a minimally intrusive approach to achieve S&T coordination called for in Title 6 U.S.C. § 186(b).

VI. Policy & Procedures

Title 6 U.S.C. § 185 authorizes the Secretary, acting through the US(S&T), to establish or contract with one or more FFRDCs to provide independent analysis of homeland security issues, or to carry out other responsibilities assigned under the Act.

A. **Primary Sponsor.** Consistent with the authorizing legislation, the US(S&T) is designated as the primary sponsor for DHS-sponsored FFRDCs. The US(S&T) establishes, manages, and administers the FFRDCs via the sponsoring agreement, which contains the core statement and defines specific policies and procedures relating to the management and administration of the FFRDC. On a case-by-case basis, other Components may be designated as the sponsor of an FFRDC; however, that Component shall closely conduct its management thereof with US(S&T).

B. **DHS Sponsor.** Consistent with the authorizing legislation, the US(S&T) is designated as the DHS Sponsor for establishment and administration of multiple agency sponsorship agreements enabling DHS use of FFRDCs whose primary sponsor is a different government agency.

1. The US(S&T) shall establish and administer the DHS-specific portion of the multiple agency sponsorship agreement which shall contain, at a minimum:

a. The core statement governing DHS use of the FFRDC;

b. Procedures for annual assessment of the performance (including cost, quality, and timeliness) of the FFRDC on DHS-sponsored work;

c. DHS procedures for avoidance of individual and organizational conflict of interest;

d. DHS procedures for protection of sensitive and proprietary information.

2. The multiple agency sponsorship agreement may contain additional DHS-specific policies and procedures if appropriate (e.g., level of effort for DHS-sponsored work).

C. **Core Statement.** FFRDCs shall be used in a manner that is consistent with their core statement. The core statement will be part of or incorporated by reference into the sponsorship agreement. The core statement must be specific enough to differentiate between work that is within the purpose, mission, general scope of effort, or special competency of the FFRDC and work that is not. The US(S&T) maintains a core statement for each FFRDC for which DHS is the primary sponsor or is a sponsoring party under a multiple agency sponsorship agreement and reviews work proposed by DHS users to ensure that it is consistent with the core statement.

D. **Sponsoring Agreement.** DHS shall administer and use FFRDCs in a manner that is consistent with their sponsoring agreements. The specific content of a sponsoring agreement may vary depending on the nature of the relationship between DHS and the FFRDC. Sponsoring agreements may be supplemented with operating instructions; however, at a minimum sponsoring agreements must include the following:

1. Core statement, as described in paragraph VI.C above.

2. Provisions for the orderly termination or nonrenewal of the contract, disposal of assets, retention and/or disposition of retained earnings, and settlement of liabilities. The responsibility for capitalization of the FFRDC must be defined in such a manner that ownership of assets may be readily and equitably determined upon termination of the FFRDC's relationship with DHS.

3. A prohibition against the FFRDC competing with any non-FFRDC concern in response to a formal federal agency request for proposal for other than the operation of an FFRDC or certain types of broad agency announcements. This prohibition is ordinarily applied to any parent organization in its non-FFRDC operations. The US(S&T) may expand this prohibition as deemed necessary and appropriate for DHS-sponsored FFRDCs.

4. A determination of whether the FFRDC may accept work from other than DHS (nonsponsors). If nonsponsor work can be accepted, a description of the procedures to be followed will be included, along with any limitations as to the nonsponsor from which work can be accepted (e.g., other federal agencies; state, local or foreign governments; or not-for-profit organizations that operate in the public interest; that is, public charities). An FFRDC for which DHS is the primary sponsor may only perform core work as defined in its core statement and in accordance with the following guidelines:

- a. The US(S&T) or its designee must approve all work.
- b. Work may only be accepted from DHS, other federal entities, state and municipal governments, and not-for-profit organizations that operate in the public interest; i.e., public charities.
- c. A DHS FFRDC may accept no commercial work.

5. Limitations on non-FFRDC work by the parent institution. Parent institutions operating DHS-sponsored FFRDC(s) may perform non-FFRDC work subject to US(S&T) or its designee review for compliance with established criteria mutually agreed upon by the US(S&T) and the parent institution. The criteria shall be addressed in the sponsoring agreement. In establishing these criteria, the following guidelines shall be used:

- a. Non-FFRDC work by parent institutions should be in the national interest, such as addressing economic, social, or governmental issues.
- b. Non-FFRDC work shall not undermine the independence, objectivity, or credibility of the FFRDC by posing an actual or perceived conflict of interest, nor shall it detract from the performance of FFRDC work.
- c. Non-FFRDC work shall not be acquired by taking unfair advantage of the parent institution's operation of its FFRDC(s) or of information that is available to that parent institution only through its FFRDC(s).

d. Non-FFRDC work may be done for public sector entities and not-for-profit organizations that operate in the public interest; e.g., public charities. Commercial work (i.e., work for for-profit entities) may only be accepted if the sponsor grants a specific exception in writing for the commercial work request at issue. If the sponsor grants an exception, such work may not exclusively benefit any individual for-profit entity to avoid the appearance that an FFRDC parent organization is endorsing a particular product, company, or industrial process.

e. There are no specified dollar limits on the volume of non-FFRDC work. However, subject to any specific terms in the sponsoring agreement, the US(S&T) will periodically assess whether the non-FFRDC work performed by the parent institution is impairing its ability to perform its FFRDC work.

f. Universities operating DHS-sponsored FFRDCs are not restricted from performing non-FFRDC work. Such work must be obtained, however, in a manner compliant with applicable procurement policies to ensure that the work is not acquired through an unfair advantage associated with the FFRDC mission, purpose, or special relationship.

6. Technology transfer activities. Sponsoring agreements may include authority for FFRDCs to participate with industry in technology transfer activities when appropriate. The US(S&T) will include adequate safeguards to ensure the FFRDC remains free of organizational conflicts of interest and that the conditions for establishing and maintaining the FFRDC are not compromised. The safeguards should include specific review and approval of technology transfer work by the US(S&T) or its designee on a case-by-case basis.

7. A description of the procedures used to make an annual assessment to evaluate performance in the areas of technical quality, responsiveness, value, cost and timeliness. A description of the feedback mechanism used to identify and resolve any perceived or real problems is also required. The US(S&T) maintains and implements the annual assessment procedures for DHS-sponsored FFRDCs and provides feedback to the primary sponsor.

8. Advance Agreements. When cost-type contracts are used, the US(S&T) should identify any cost elements or fees that require advance agreement and/or approval. Such items may include, but are not limited to personnel compensation, depreciation, various indirect costs such as independent research and development, or others as deemed appropriate by the sponsor. Any excess funding will be deobligated and returned to DHS.

9. Prepublication review policies. While DHS is sensitive to the need for the FFRDC, or its parent institution, to publish its research findings in appropriate professional fora, the US(S&T) in the sponsorship agreement will ordinarily establish pre-publication controls on the publication of research results that have been funded by DHS, or another US government sponsor that wishes to limit dissemination of the findings. This restriction is necessary to protect the needs of the government to enjoy a long-term and “trusted agent” relationship with the FFRDC’s parent institution and the need for the FFRDC to have extraordinary levels of access to sensitive government information.

E. ***FFRDC Level of Effort.*** It is the policy of DHS to use staff years of technical effort (STEs) in sizing and managing DHS-funded FFRDC work. Although the total number of STEs available will be constrained by DHS budgetary considerations, STEs will provide a standard measure across all of DHS’ FFRDCs for projecting DHS workload and funding requirements. [Appendix B](#) contains the standard definition of STEs to be used in computing workload requirements. DHS reserves the right to establish on an annual basis (and prior to each new fiscal year) a ceiling on the maximum number of STEs for DHS-funded FFRDC work (including work by DHS-sponsored FFRDCs, DHS work by FFRDCs under multiple agency sponsorship agreements, and DHS work by FFRDCs sponsored by other government agencies).

1. General guidelines. Annual levels of effort shall be based upon application of the core concept and the following guidelines:

- a. Maintain a relatively stable level of effort; and
- b. Maintain competency in core areas.

2. Establishment of level of effort. The US(S&T) will establish a workload annually by STE for each FFRDC based on:

- a. DHS needs;
- b. A determination that those needs require one or more of the core capabilities of the FFRDC; and

c. The general guidelines laid out in subparagraph V1.E.1. above.

3. Nonsponsor use of DHS-sponsored FFRDCs. FFRDC work funded using non-DHS appropriations will comply with the same policies and constraints as DHS-funded work and will be reported in accordance with [Appendix A](#).

F. **Strategic Relationship**. It is the policy of DHS to maintain a strategic relationship with each FFRDC for which DHS is the primary sponsor or is a party to a multiple agency sponsorship agreement. Strategic relationships enable FFRDCs to develop and maintain in-depth knowledge of their sponsor's programs and operations; to maintain continuity and currency in their special fields of expertise, and a high degree of competence in their staff and work; to maintain their objectivity and independence; and to respond to the emerging needs of their sponsor and users. The US(S&T) fosters the strategic relationship by:

1. Ensuring that DHS users are aware and make appropriate use of the capabilities accessible via FFRDC sponsoring agreements (including multiple agency sponsorship agreements);
2. Helping to ensure that the FFRDC has access to all necessary information required to effectively execute assigned tasks;
3. Helping to ensure that the FFRDC has sufficient insight into DHS priorities and emerging issues to enable FFRDC management to sustain and adapt FFRDC competencies consistent with its core statement; and
4. Providing oversight to guard against conflict of interest issues.

G. **Comprehensive Review**. For DHS-sponsored FFRDCs, prior to renewal of the FFRDC contract, the US(S&T) shall conduct a comprehensive review of the continuing use of and need for the FFRDC. This review must comply with FAR 35.017. The resulting determination to approve continuation or termination of the sponsorship shall be made by the US(S&T) in consultation with the relevant Component customers prior to the anticipated contract renewal date. [Appendix C](#) contains guidelines for the conduct of comprehensive reviews to ensure consistency and thoroughness in the review process.

H. **Reports**. The Secretary of Homeland Security requires specified and *ad hoc* reports in order to perform necessary oversight functions and responsibilities. The schedule and content of reports and other submissions currently required are shown in [Appendix A](#).

I. **The Office of the Inspector General (OIG)**. OIG is responsible under the Inspector General Act of 1978, as amended, to oversee programs of the DHS, including activities conducted by and through FFRDCs, and has the right to access any DHS and FFRDC records relating to programs receiving support from DHS. Nothing in this MD or any sponsoring agreement shall limit the authority of the OIG as prescribed by the Inspector General Act and MD 0810.1, The Office of Inspector General.

J. **Requirements to Work with FFRDCs**. The process for working with FFRDCs begins with the identification of a requirement and early in the acquisition planning stage. Potential task sponsors should contact the appropriate program management office within US(S&T) when a requirement exists to determine if the potential task is within the general scope of effort, mission, purpose, or special competency of an FFRDC. US(S&T) will post detailed guidance on the dhs.gov website on how to work with FFRDCs. The program management office will provide guidance and assistance to task sponsors. [Appendix D](#) is an overview of the process.

REPORTING REQUIREMENTS FOR DHS FFRDCs

ANNUAL REPORTING REQUIREMENTS	DUE DATE	DESCRIPTION
Annual Report on Staff Years of Technical Effort (STEs) and Funding	15 November	Provide the Secretary of Homeland Security with a report showing STEs and associated funding data (DHS and non-DHS). US(S&T) will provide required data for: (1) Congressional Reporting (2) Budget Estimates.
Mid-Year Status Update	30 April	Provide the Secretary of Homeland Security a report for use in monitoring FFRDC obligations (DHS and non-DHS). The report should address the US(S&T)'s ability to use and fund all authorized DHS-funded STEs; if excess STEs are anticipated; and if exceptions are anticipated.
Annual Review Assessment	30 days after completion of the assessment	Provide to the Secretary of Homeland Security a copy of the annual review assessment. The requirements for an annual assessment may be met by the Comprehensive Review during the year that a Comprehensive Review is required.
Changes to Sponsoring Agreement or Core Statement	Within 30 days of change implementation	Provide the Secretary of Homeland Security with copies of changes to the sponsoring agreement or core statement.
Comprehensive Review Notification	One year prior to due date of the review	Advise the Secretary of Homeland Security of Comprehensive Review initiation. The Secretary of Homeland Security will advise the US(S&T) of any special review requirements.
Comprehensive Review	NLT 90 days prior to renewal of the FFRDC contract	Provide to the Secretary of Homeland Security the results of the Comprehensive Review for the use and need of the FFRDC in accordance with this MD (see Appendix C) and FAR Part 35.017. Secretary of Homeland Security concurrence is required prior to renewal of the FFRDC contract.

STAFF YEAR OF TECHNICAL EFFORT (STE)

In calculating workload requirements to be delivered during the fiscal year, FFRDCs and the US(S&T) shall use the standard definition of STE and work year shown below:

- STEs apply to direct professional and consultant labor, performed by researchers, mathematicians, programmers, analysts, economists, scientists, engineers, and others who perform professional-level technical work primarily in the fields of studies and analyses, systems planning, and program and policy planning and analysis.
- Minimum educational requirements for STE employees and consultants are a baccalaureate degree from an accredited college or university. In rare instances, non-degree personnel may be included, but only if they possess the equivalent of a baccalaureate degree in education and experience, and are performing work of the same type and level as that performed by degreed STE employees.
- An STE work year is defined to be 1,810 hours of paid effort for technical services. STE work years include both FFRDC employees and subcontracted consultant technical effort.

COMPREHENSIVE REVIEW GUIDELINES FOR DHS- SPONSORED FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTERS (FFRDCs)

PURPOSE: The purpose of the comprehensive review is to analyze formally the use and need for the FFRDC in order to assist the Secretary of DHS in determining whether to continue sponsorship of the FFRDC. The FFRDC sponsor will perform the comprehensive review with the advice and assistance of the office of the US (S&T) and the contracting activity.

This appendix provides guidelines for reporting the results of FFRDC comprehensive reviews in accordance with this MD and the FAR.

- Identify the FFRDC, its primary sponsor and contracting activity. Include the date and term of the FFRDC's current sponsoring agreement.
- Provide a detailed examination of the sponsor's special technical needs and mission requirements that are being performed by the FFRDC to determine whether, and at what level, they should continue to exist (FAR 35.017-4 (c)(1)).

Identify requirements for FFRDC support including known specific programs involved, the level of effort required and the types of tasks to be performed.

- Consider alternative sources (FAR 35.107-4(c)(2)):

Specify the special research, systems development, or analytical needs, skills, and/or capabilities involved in accomplishing FFRDC tasks.

Explain why the capabilities cannot be provided as effectively by in-house personnel, for-profit or not-for-profit contractors, university-affiliated organizations, or another existing FFRDC. Include statements on the alternatives to the FFRDC that were considered and the rationale for not selecting each of them.

- Provide a detailed assessment of the efficiency and effectiveness of the FFRDC in meeting a sponsor's/user's needs including the FFRDC's ability to maintain its objectivity, independence, quick response capability, currency in its field(s) of expertise, and familiarity with the needs of its sponsor (FAR 35.017-4(c)(3)).

Include a summary of FFRDC accomplishments and their effectiveness in meeting user needs since the last comprehensive review. As a minimum, the quality and timeliness of the work produced, the number and dollar value of projects and programs assessed, and the user evaluations of performance should be addressed. A summary of the results of the most recent annual review should be included. All major users should participate in this portion of the comprehensive review. Discuss any criticisms or concerns that the users had with FFRDC performance and the steps taken to resolve them.

APPENDIX C

- Assess the FFRDC management controls to ensure cost-effective operation (FAR 35.017-4(c) (4)).

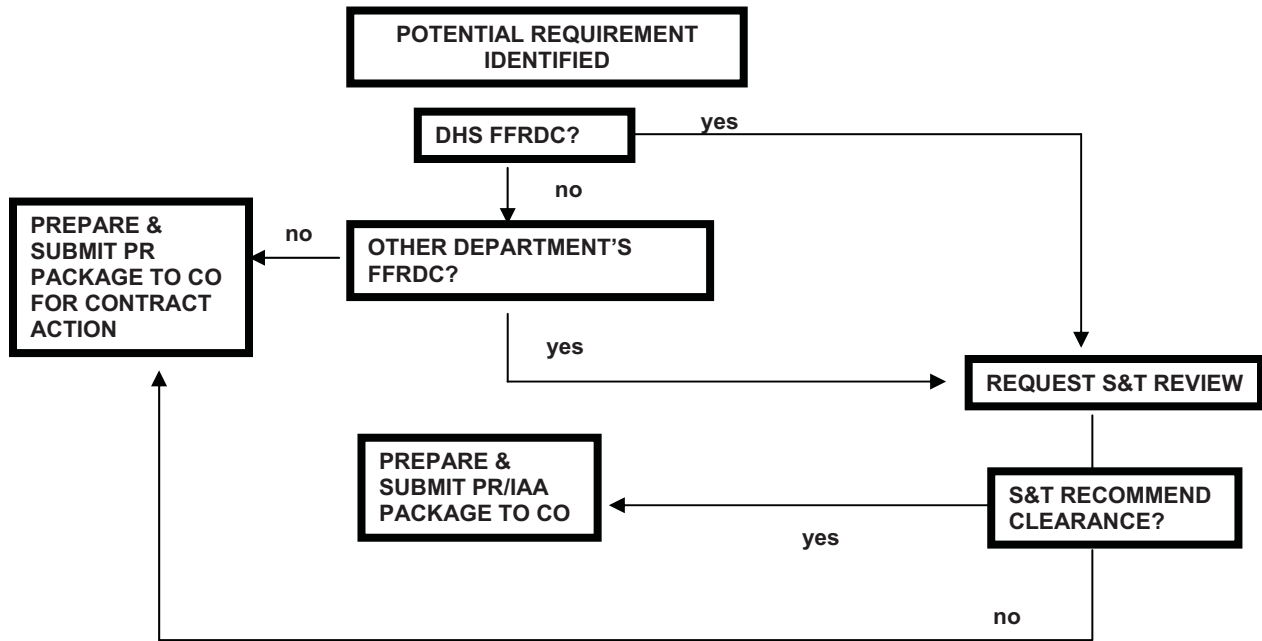
Discuss accounting and purchasing systems; overhead costs and fees; oversight actions taken to verify cost-effective operations; and other management issues as deemed appropriate.

- Determine that the criteria for establishing the FFRDC are satisfied and that the sponsoring agreement is in compliance with FAR 35.017, FAR 35.017-2, and DHS MD 143-04 on Establishing or Contracting with Federally Funded Research and Development Centers (FFRDCs). Include a statement addressing each of the criteria. Provide a certification that the current sponsoring agreement accurately reflects the mission of the FFRDC.

Discuss agreements between the government and the FFRDC. These agreements may cover such items as authorization of fees, provision of government facilities and equipment, distribution of residual assets of settlement and liabilities in event of dissolution, maintenance of specific cash reserves, and waivers to accounting policies or regulatory requirements.

- Provide a recommended course of action that is signed by the head of the sponsoring agency.
- Work closely with the contracting office and the office of the US (S&T) and Component customers most affected by a termination decision in accomplishing the comprehensive review and prior to forwarding the recommendation(s) to the Secretary.
- Obtain the DHS Secretary's concurrence with the results of the comprehensive review prior to renewal of the contract or termination of the FFRDC.

WORKING WITH FFRDCs: AN OVERVIEW



- S&T review consists of analyzing the requirement; ensuring tasks are within the FFRDC's purpose, mission, general scope of effort, or special competency; and that the appropriate authority is cited (e.g., Economy Act, Section 305 of the HSA, or other).
- Contracting Officer is responsible for Determinations & Findings pursuant to FAR 17 and executing subsequent Interagency Agreements (IAAs).

Note: If sponsoring agency is not FAR covered, approval authority is CPO.