

TPA = 02

OMB Approval #: 2700-0042

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE

01

PAGE OF PAGES

1

5

2. AMENDMENT/MODIFICATION NO.

47

3. EFFECTIVE DATE

SEP 27 2007

4. REQUISITION/PURCHASE REQ. NO.

See page 8

5. PROJECT NO. (If applicable)

6. ISSUED BY

CODE

PS-31/MEE

7. ADMINISTERED BY (If other than Item 6)

CODE

PS-31

Procurement Office
George C. Marshall Space Flight Center
National Aeronautics and Space Administration
Marshall Space Flight Center, AL 35812

Anne Lewis/(256) 544-5435
e-mail Frances.A.Lewis@nasa.gov

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State, and Zip Code)

EG&G Technical Services, Inc.
900 Clopper Road
Gaithersburg, MD 20878

9A. AMENDMENT OF SOLICITATION NO.

9B. DATED (SEE ITEM 11)

10A. MODIFICATION OF CONTRACT/ORDER NO.

GS-10F-0038M/H36049D

10B. DATED (SEE ITEM 13)

Effective Date August 1, 2003

CODE

Cage Code 34157

FACILITY CODE

SAP 112857

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

[] The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers [] is extended, [] is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15 and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

See page 8

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

(✓) A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.

B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation data, etc.) (SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103b) AND PS-OWI-05.

✓ C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: FAR Clause 52.212-4(c), CONTRACT TERMS AND CONDITIONS - COMMERCIAL ITEMS (OCT 2003), Changes, GSA LOGWORLD CONTRACT GS-10F-0038M, AND PS-OWI-05

D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor [] is not, [X] is required to sign this document and return 3 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

	Total Fixed Price, FFP Lump Sum	Potential Contract Val. Lump Sum	Total Not-to-Exceed FFP IDIQ	Not-to-Exceed Contract Value Adding IDIQ Amt.	Total Sum Allotted FFP Lump Sum Funding Amt.
Prev. Base Total	(b)(4)	\$ 61,047,300	\$40,495,120	\$78,652,580	\$33,570,124
This Modification	(b)(4)	\$ 20,118	\$-0-	\$ 20,118	\$ 500,000
New NTE Amount	(b)(4)	\$61,067,418	\$40,495,120	\$78,672,698	\$34,070,124

SEE PAGE 2 FOR DESCRIPTION OF CHANGES

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect

15A. NAME AND TITLE OF SIGNER (Type or print)

15B. CONTRACTOR/OFFEROR

15C. DATE SIGNED

SEP 27 2007

(Signature of person authorized to sign)

16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)

Frances Anne Lewis, Contract Specialist

16B. UNITED STATES OF AMERICA

16C. DATE SIGNED

SEP 27 2007

(Signature of Contracting Officer)

NSN 7540-01-152-8070
PREVIOUS EDITION UNUSABLE

30-105

STANDARD FORM 30 (Rev. 10-83)
Prescribed by GSA
FAR (48 CFR) 53.243

The purpose of this modification is to make changes/additions/deletions as described below.

The contract is changed as follows:

A. The purpose for this modification is to:

- (1) Add negotiated value of (b)(4) for implementation of revised NFS Clause 1852.204-76, "Security Requirements for Unclassified Information Technology Resources (May 2007), increasing the current value of the Lump Sum Fixed Price portion of this order to (b)(4)**
- (2) add Data Requirement Document (DRD) STD/CD-ITSRCD as DRD 988CD-003;**
- (3) Add revised DRD 988CD-001 in accordance with revised NFS Clause noted above in (1);**
- (4) Add incremental funding in the amount of (b)(4) for the firm-fixed lump-sum portion of the contract, increasing total allocated and available funding from (b)(4) to (b)(4); and**
- (5) Make appropriate changes to the Performance Work Statement (PWS) in accordance with the inclusion/revision of DRDs stated above; and**
- (6) Rescind email from writer dated May 3, 2007, subject: Exception to Mod 41 (HSPD12) to H36049D for Para b of new IT clause.**

B. Clause 51, 1852.204-76, "Security Requirements for Unclassified Information Technology Resources (November 2006) [Deviation]", is hereby deleted in its entirety and replaced by Clause 51, 1852.204-76, "Security Requirements for Unclassified Information Technology Resources (May 2007)."

Due to a revision in the regulations governing Information Technology and changes in the NASA FAR Supplement, the MSFC Office of Procurement is required to incorporate appropriate changes regarding Security of Information Technology into this order. Previously MSFC implemented the NFS IT Security Clause (Clause 51) by letter and modification to include the deviation version of the clause. Subsequently, the clause has been updated and the current clause is dated May 2007.

Negotiations were held on August 15, 2007, to determine increase in contract value for the new IT Security clause requirement and resulting changes to the Data Procurement Document (DPD) between the CO, the COTR, and the Contractor PM. The negotiated solution included the Contractor providing only the IT Security Plan as described and directed in Clause 51 and the pertinent DRDs. Total contract value increase agreed to by all parties was \$20,118 for this effort. Additional cost for reviews and/or updates/revisions in outyears (Award Terms 1 through 5, assuming all are awarded) will be addressed as the occasion occurs.

C. DPD 988 is changed to include revised DRD 988CD-001 and to add DRD 988CD-003 (DRD 988CD-002 was deleted in mod 41).

D. Clause 2, Firm-Fixed-Price for Lump Sum, paragraph A, is changed to reflect the new total Firm-Fixed-Price Lump Sum price of this GSA order through July 31, 2008, of (b)(4). This total includes phase-in costs and phase in adjustment for base year A, Base Years A, B, C, Option No. 1, HSPD-12 implementation, Wage Determination/ Collective Bargaining Agreement (CBA) adjustments for Option No. 1, Option No.2, and negotiated increase for IT Security implementation.

E. Section 2, Clause 3 entitled "Limitation of Funds", page 8, paragraph A, is changed from \$33,570,124 to add the new funding amount of \$500,000, making the new total allocated funds available of \$34,070,124.

F. Section 2, Clause 3 entitled "Limitation of Funds", page 9, paragraph C, is changed to read that funds presently allotted to this order will cover the work through December 31, 2007.

The table in Paragraph B providing option and award term periods is hereby deleted in its entirety and replaced by the following:

OPTION/AWARD TERM PERIOD COVERED	POP BEGIN DATE	POP END DATE	EXERCISED	FIRM FIXED PRICE LUMP SUM
Option No. 1	08/01/06	07/31/07	Mod 33	(b)(4)
Option No. 2	08/01/07	07/31/08	Mod 45	(b)(4)
Award Term Period 1	08/01/08	02/28/09		(b)(4)
Award Term Period 2	03/01/09	09/30/09		(b)(4)
Award Term Period 3	10/01/09	04/30/10		(b)(4)
Award Term Period 4	05/01/10	11/30/10		(b)(4)
Award Term Period 5	12/01/10	07/31/11		(b)(4)
Total Potential FFP Lump Sum Including Base Years A, B, and C				

G. Section 3, Attachment 1, Performance Work Statement, pages 1-11 through 1-13, are changed to include the new DRDs as well as additional verbiage provided by CIO through CDMS.

H. Section 3, Attachment 2, Data Procurement Document 988, is changed to include a new revision number, and to include the new DRD and revised DRD by replacing pages A2-1 through A2-13.

I. Rescind email direction dated May 3, 2007, signed by the Contracting Officer (CO), subject: Exception to Mod 41 (HSPD-12) to H36049D for Para b of new IT clause. During HSPD-12 negotiations, it was agreed that, while subject clause was added in Modification

41, that paragraph (b), IT Security Requirements, of cited clause was deemed by both parties to be separate and apart from the negotiated terms and conditions and negotiated compensation for said Modification 41. Cited paragraph (b) was therefore subject to additional review and discussion and would be discussed as a separate issue. This issue has been negotiated within the terms and conditions of this modification, and the email and its inclusive direction is hereby rescinded in its entirety.

J. As a result of the foregoing changes, the following pages are deleted and the corresponding changes are substituted/added. Replacement pages are provided as appropriate. Specific changes are shown in bold text and/or by a change bar in the right margin.

Pages Deleted	Pages Substituted/Added
Section 2, page 8-9	Section 2, page 8-9
Section 2, pages 57-60	Section 2, pages 57-60
Section 3, Attachment , pages 1-11 – 1-13	Section 3, Attachment 1, pages 1-11 – 1-13
Section 3, Attachment 2, pages A2-1 – A2-13	Section 3, Attachment 2, pages A2-1 – A2-13

K. In consideration of the modifications agreed to herein as complete equitable adjustment for all claims arising out of or attributable to the issuance of the contract change(s) and/or contractor proposal(s) listed below, the contractor hereby releases the Government from any and all liability under this contract for further equitable adjustments attributable to such facts or circumstances giving rise to said contract change(s) and/or contractor proposal(s), and for such additional obligations as may be required by this modification.

Contract Change	Contractor
Modification 47	Proposal 1004-230-07, dated July 26,2007

**Accounting and Appropriation Data
 H36049D**

PR NUMBER	Fund	WBS	Cost Center	Internal Order	Fund Center	Amount
					PREVIOUS FUNDING	\$27,766,460.00
4200193136	ESAX22007D	292487.09.08.40	62AS40	FC000000	62	\$1,300,000.00
	ESAX22007D	158302.01.08.01	62AS10	FC000000	62	\$176,000.00
4200189962	EXCX22007D	931164.08.04.01.06	62EM01	FC000000	62	\$100,000.00
4200188604	ESAX22007D	299147.01.08.01	62AS50	FC000000	62	\$3,600.00
4200199883	ESAX22007D	292487.09.08.40	62AS40	FC000000	62	\$33,402.00
4200200580	EXCX22007D	763115.08.04.01.06	62ET01	FC000000	62	\$59,266.00
	ESAX22007D	763115.08.04.01.06	62EM01	FC000000	62	\$290,000.00
	ESAX22007D	292487.02.08.01	62HS01	FC000000	62	\$28,325.00
	ESAX22007D	691633.01.08.05	62EE04	FC000000	62	\$13,170.00
	ESAX22007D	136905.08.05.08.04.08	62EV23	FC000000	62	\$2,272.00
4200203744	ESAX22007D	763115.08.04.01.06	62EI03	FC000000	62	\$2,800.00
	ESAX22007D	292487.09.08.40	62AS40	FC000000	62	\$266,899
4200203744	ESAX22007D	292487.09.08.40	62AS40	FC000000	62	\$551,160
4200203744	ESAX22007D	292487.09.08.40	62AS40	FC000000	62	\$481,941
4200213759	ESAX22007D	411671.06.04.01	62VP63	FC000000	62	\$49,500
	ESAX22007D	397424.07.02.02.03	62VP62	FC000000	62	\$20,900
	ESAX22007D	411672.06.04.01	62VP63	FC000000	62	\$5,500
	ESAX22007D	281945.02.03.01.02	62VP61	FC000000	62	\$2,200
	ESAX22007D	763115.08.04.01.03	62ER33	FC000000	62	\$1,200
	ESAX22007D	763115.08.04.01.03	62ER01	FC000000	62	\$2,400
	ESAX22007D	292487.09.08.40	62AS40	FC000000	62	\$1,400,000
4200207324	ESAX22007D	763115.08.04.01.06	62ER41	FC000000	62	\$620
	ESAX22007D	763115.08.04.01.06	62EI03	FC000000	62	\$12,991
	ESAX22007D	698671.04.08	62AS20	FC000000	62	\$90,000
4200213030	ESAX22007D	390492.04.02.06.98	62VP63	FC000000	62	\$8,400
	EXCX22007R	892182.01.08.07.0796.01	62AS40	FC000000	62	\$40,381
	EXCX22007D	763115.08.04.01.06	62ET01	FC000000	62	\$173,000
4200215494	ESAX22007D	158302.01.08.01	62AS10	FC000000	62	\$564,000
	EXCX22007D	698671.01.08	62AS40	FC000000	62	\$41,932
	ESAX22007D	129985.01.08.13	62AS20	FC000000	62	\$81,805
4200217292	ESAX22007D	292487.09.08.40	62AS40	FC000000	62	\$500,000
TOTAL						\$34,070,124

2. FIRM-FIXED-PRICE FOR LUMP SUM

- A. The total Firm-Fixed-Price (FFP) Lump Sum of this GSA order for the base period from the effective date through **July 31, 2008** is: (b)(4) **This total includes phase-in costs and phase in adjustment for base year A, Base Years A, B, C, Option No. 1, HSPD-12 implementation, Wage Determination/Collective Bargaining Agreement (CBA) adjustments for Option No. 1, Option No. 2, and negotiated increase for IT Security Implementation.**
- B. If the Government exercises any options or awards any of the award-term periods pursuant to the terms of this GSA order, the total firm-fixed price of this GSA order shall be increased by the applicable amounts shown below:

OPTION/AWARD TERM PERIOD COVERED	POP BEGIN DATE	POP END DATE	EXERCISED	FIRM FIXED PRICE LUMP SUM
Option No. 1	08/01/06	07/31/07	Mod 33	(b)(4)
Option No. 2	08/01/07	07/31/08	Mod 45	
Award Term Period 1	08/01/08	02/28/09		
Award Term Period 2	03/01/09	09/30/09		
Award Term Period 3	10/01/09	04/30/10		
Award Term Period 4	05/01/10	11/30/10		
Award Term Period 5	12/01/10	07/31/11		
Total Potential FFP Lump Sum Including Base Years A, B, and C				

2A. EARNED AWARD TERM PERIODS

1. Based on the Findings and Determination of the Award Term Board, the following Award Term Periods have been earned by the contractor and shall be added to the end of the contract period of performance.

PERIOD EARNED	DATES	EARNED MOD
Award Term Period 1	08/01/08 – 02/28/09	Mod 27
Award Term Period 2	03/01/09 – 09/30/09	Mod 42

3. LIMITATION OF FUNDS

- A. Of the total price of the services identified as lump sum, the sum of **\$34,070,124** is presently available for payment and allotted to this GSA order through **December 31, 2007**. It is anticipated that from time to time additional funds will be allocated to this GSA order in accordance with the following schedule, until the total price of said items is allotted:

SCHEDULE FOR ALLOTMENT OF FUNDS

<u>Date</u>	<u>Amounts</u>
December 15, 2007	\$1,500,000

*NOTE: THE IDIQ PORTION OF THE CONTRACT SHALL BE PAID BY INDIVIDUAL DELIVERYS WITH FUND CITATIONS ON EACH ORDER.

- B. The Contractor agrees to perform, or have performed work, as specified in the PWS up to the point at which, if this order is terminated pursuant to paragraph (I) of FAR Clause 52.212-4 applicable to this order, the total amount payable by the Government (including amounts payable for subcontracts and settlement costs) pursuant to that clause would, in the exercise of reasonable judgment by the Contractor, approximate the total amount at the time allotted to the order. The Contractor is not obligated to continue performance of the work beyond that point. The Government is not obligated in any event to pay or reimburse the Contractor more than the amount from time to time allotted to the order, anything to the contrary in the termination clause notwithstanding.
- C. 1. It is contemplated that funds presently allotted to this order will cover the work to be performed until **December 31, 2007**.
2. If funds allotted are considered by the Contractor to be inadequate to cover the work to be performed until that date, or an agreed date substituted for it, the Contractor shall notify the Contracting Officer in writing when within the next 60 days the work will reach a point at which, if the order is terminated pursuant to paragraph (I) of FAR Clause 52.212-4 applicable to this order, the total amount payable by the Government (including amount payable for subcontracts and settlement costs) pursuant to that clause will approximate 75 percent of the total amount then allotted to the order.
3. (i) The notice shall state the estimated date when the point referred to in subparagraph 3.C.(2) above will be reached and the estimated amount of additional funds required to continue performance to the date specified in subparagraph 3.C.(1) above, or an agreed date substituted for it.
- (ii) The Contractor shall, 60 days in advance of the date specified in subparagraph 3.C.(1) above, or an agreed date substituted for it, advise the Contracting Officer of the estimated amount of additional funds required for the timely performance of the contract for a further period as may be specified in the order or otherwise agreed to by the parties.
4. If, after the notification referred to in subdivision 3.C.(3).(ii) above, additional funds are not allotted by the date specified in subparagraph 3C(1) above, or an agreed date substituted for it, the Contracting Officer shall, upon the Contractor's written request, terminate this order on that date or on the date set forth in the request, whichever is later, pursuant to paragraph (I) of FAR Clause 52.212-4.
- D. When additional funds are allotted from time to time for continued performance of the work under this order, the parties shall agree on the applicable period of order performance to be covered by these funds. The provisions of subparagraphs 3.A and 3.C above shall apply to the additional funds and the substituted date pertaining to them, and the order shall be modified accordingly.

51. 1852.204-76 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (MAY 2007)

(a) The Contractor shall be responsible for information and information technology (IT) security when –

(1) The Contractor or its subcontractors must obtain physical or electronic (i.e., authentication level 2 and above as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Electronic Authentication Guideline) access to NASA's computer systems, networks, or IT infrastructure; or

(2) Information categorized as low, moderate, or high by the Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems is stored, generated, processed, or exchanged by NASA or on behalf of NASA by a contractor or subcontractor, regardless of whether the information resides on a NASA or a contractor/subcontractor's information system.

(b) IT Security Requirements.

(1) Within 30 days after contract award, a Contractor shall submit to the Contracting Officer for NASA approval an IT Security Plan, Risk Assessment, and FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, Assessment. These plans and assessments, including annual updates shall be incorporated into the contract as compliance documents.

(i) The IT system security plan shall be prepared consistent, in form and content, with NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, and any additions/augmentations described in NASA Procedural Requirements (NPR) 2810, Security of Information Technology. The security plan shall identify and document appropriate IT security controls consistent with the sensitivity of the information and the requirements of Federal Information Processing Standards (FIPS) 200, Recommended Security Controls for Federal Information Systems. The plan shall be reviewed and updated in accordance with NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, and FIPS 200, on a yearly basis.

(ii) The risk assessment shall be prepared consistent, in form and content, with NIST SP 800-30, Risk Management Guide for Information Technology Systems, and any additions/augmentations described in NPR 2810. The risk assessment shall be updated on a yearly basis.

(iii) The FIPS 199 assessment shall identify all information types as well as the "high water mark," as defined in FIPS 199, of the processed, stored, or transmitted information necessary to fulfill the contractual requirements.

(2) The Contractor shall produce contingency plans consistent, in form and content, with NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, and any additions/augmentations described in NPR 2810. The Contractor shall perform yearly "Classroom Exercises." "Functional Exercises," shall be coordinated with the Center CIOs and be conducted once every three years, with the first conducted within the first two years of contract award. These exercises are defined and described in NIST SP 800-34.

(3) The Contractor shall ensure coordination of its incident response team with the NASA Incident Response Center (NASIRC) and the NASA Security Operations Center, ensuring that incidents are reported consistent with NIST SP 800-61, Computer Security Incident Reporting Guide, and the United States Computer Emergency Readiness Team's

(US-CERT) Concept of Operations for reporting security incidents. Specifically, any confirmed incident of a system containing NASA data or controlling NASA assets shall be reported to NASIRC within one hour that results in unauthorized access, loss or modification of NASA data, or denial of service affecting the availability of NASA data.

(4) The Contractor shall ensure that its employees, in performance of the contract, receive annual IT security training in NASA IT Security policies, procedures, computer ethics, and best practices in accordance with NPR 2810 requirements. The Contractor may use web-based training available from NASA to meet this requirement.

(5) The Contractor shall provide NASA, including the NASA Office of Inspector General, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out IT security inspection, investigation, and/or audits to safeguard against threats and hazards to the integrity, availability, and confidentiality of NASA information or to the function of computer systems operated on behalf of NASA, and to preserve evidence of computer crime. To facilitate mandatory reviews, the Contractor shall ensure appropriate compartmentalization of NASA information, stored and/or processed, either by information systems in direct support of the contract or that are incidental to the contract.

(6) The Contractor shall ensure that system administrators who perform tasks that have a material impact on IT security and operations demonstrate knowledge appropriate to those tasks. Knowledge is demonstrated through the NASA System Administrator Security Certification Program. A system administrator is one who provides IT services (including network services, file storage, and/or web services) to someone other than themselves and takes or assumes the responsibility for the security and administrative controls of that service. Within 30 days after contract award, the Contractor shall provide to the Contracting Officer a list of all system administrator positions and personnel filling those positions, along with a schedule that ensures certification of all personnel within 90 days after contract award. Additionally, the Contractor should report all personnel changes which impact system administrator positions within 5 days of the personnel change and ensure these individuals obtain System Administrator certification within 90 days after the change.

(7) The Contractor shall ensure that NASA's Sensitive But Unclassified (SBU) information as defined in NPR 1600.1, NASA Security Program Procedural Requirements, which includes privacy information, is encrypted in storage and transmission.

(8) When the Contractor is located at a NASA Center or installation or is using NASA IP address space, the Contractor shall --

(i) Submit requests for non-NASA provided external Internet connections to the Contracting Officer for approval by the Network Security Configuration Control Board (NSCCB);

(ii) Comply with the NASA CIO metrics including patch management, operating systems and application configuration guidelines, vulnerability scanning, incident reporting, system administrator certification, and security training; and

(iii) Utilize the NASA Public Key Infrastructure (PKI) for all encrypted communication or non-repudiation requirements within NASA when secure email capability is required.

(c) Physical and Logical Access Requirements.

(1) Contractor personnel requiring access to IT systems operated by the Contractor for NASA or interconnected to a NASA network shall be screened at an appropriate level in accordance with NPR 2810 and Chapter 4, NPR 1600.1, NASA Security Program Procedural Requirements. NASA shall provide screening, appropriate to the highest risk level, of the IT systems and information accessed, using, as a minimum, National Agency Check with Inquiries (NACI). The Contractor shall submit the required forms to the NASA Center Chief of Security (CCS) within fourteen (14) days after contract award or assignment of an individual to a position requiring screening. The forms may be obtained from the CCS. At the option of NASA, interim access may be granted pending completion of the required investigation and final access determination. For Contractors who will reside on a NASA Center or installation, the security screening required for all required access (e.g., installation, facility, IT, information, etc.) is consolidated to ensure only one investigation is conducted based on the highest risk level. Contractors not residing on a NASA installation will be screened based on their IT access risk level determination only. See NPR 1600.1, Chapter 4.

(2) Guidance for selecting the appropriate level of screening is based on the risk of adverse impact to NASA missions. NASA defines three levels of risk for which screening is required (IT-1 has the highest level of risk).

(i) IT-1 -- Individuals having privileged access or limited privileged access to systems whose misuse can cause very serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of spacecraft, satellites or aircraft.

(ii) IT-2 -- Individuals having privileged access or limited privileged access to systems whose misuse can cause serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of payloads on spacecraft, satellites or aircraft; and those that contain the primary copy of "level 1" information whose cost to replace exceeds one million dollars.

(iii) IT-3 -- Individuals having privileged access or limited privileged access to systems whose misuse can cause significant adverse impact to NASA missions. These systems include, for example, those that interconnect with a NASA network in a way that exceeds access by the general public, such as bypassing firewalls; and systems operated by the Contractor for NASA whose function or information has substantial cost to replace, even if these systems are not interconnected with a NASA network.

(3) Screening for individuals shall employ forms appropriate for the level of risk as established in Chapter 4, NPR 1600.1.

(4) The Contractor may conduct its own screening of individuals requiring privileged access or limited privileged access provided the Contractor can demonstrate to the Contracting Officer that the procedures used by the Contractor are equivalent to NASA's personnel screening procedures for the risk level assigned for the IT position.

(5) Subject to approval of the Contracting Officer, the Contractor may forgo screening of Contractor personnel for those individuals who have proof of a --

- (i) Current or recent national security clearances (within last three years);
- (ii) Screening conducted by NASA within the last three years that meets or exceeds the screening requirements of the IT position; or

(iii) Screening conducted by the Contractor, within the last three years, that is equivalent to the NASA personnel screening procedures as approved by the Contracting Officer and concurred on by the CCS.

(d) The Contracting Officer may waive the requirements of paragraphs (b) and (c)(1) through (c)(3) upon request of the Contractor. The Contractor shall provide all relevant information requested by the Contracting Officer to support the waiver request.

(e) The Contractor shall contact the Contracting Officer for any documents, information, or forms necessary to comply with the requirements of this clause.

(f) At the completion of the contract, the contractor shall return all NASA information and IT resources provided to the contractor during the performance of the contract and certify that all NASA information has been purged from contractor-owned systems used in the performance of the contract.

(g) The Contractor shall insert this clause, including this paragraph (g), in all subcontracts

(1) Have physical or electronic access to NASA's computer systems, networks, or IT infrastructure; or

(2) Use information systems to generate, store, process, or exchange data with NASA or on behalf of NASA, regardless of whether the data resides on a NASA or a contractor's information system.

(End of clause)

The Contractor shall be required to attend applicable meetings to appropriately plan and execute order requirements.

The Contractor shall provide Monthly Status Reports in accordance with DRD 988MA-003.

The Contractor shall provide Contractor Cost Reports in accordance with DRD 988MA-004.

PERFORMANCE SUMMARY		
Function: General Order Requirements - Security		
WORK REQUIREMENT	PERFORMANCE MEASURE	PERFORMANCE STANDARDS
Contract Information Technology Security Program Plan and Compliance	Management commitment and employee involvement/ compliance in the Security Process per MPR 1600.1 and IT Security Plan per NPR 2810.1	Maintaining the safeguards as specified in DRDs 988CD-001 and 988CD-003 providing for the availability, integrity, and confidentiality of Information Technology resources. No major security audit findings. All IT security activities IAW the above cited DRDs .

1.2.D Security

Information Technology Security

The Contractor shall prepare an IT system security plan, risk assessment, and contingency plan for each IT system identified for information stored, generated, processed or exchanged by/with NASA or on behalf of NASA by the contractor or subcontractor. The Contractor shall comply with the NASA IT security requirements found in NPR 2810.1, Security of Information Technology and shall submit the required documents following the NASA Certification and Accreditation requirements. The Contractor shall coordinate its incident response with the NASA Incident Response Center (NASIRC) and the NASA Security Operations Center or an appropriate NASA point of contact. Any confirmed incident of a system containing NASA information or controlling NASA assets shall be reported to NASIRC within one hour. The Contractor shall ensure its employees with access to NASA IT resources or information receive annual IT security training and system administrators have demonstrated appropriate knowledge. The Contractor shall ensure that NASA's Sensitive But

Unclassified (SBU) information, as defined in NPR 1600.1, NASA Security Program Procedural Requirements, is encrypted in storage and transmission. The Contractor shall (i) submit requests for non-NASA provided external Internet connections to the Contracting Officer for approval by the Network Security Configuration Control Board (NSCCB); (ii) comply with the NASA CIO IT security metrics; and (iii) utilize the NASA Public Key Infrastructure (PKI) for all encrypted communication or non-repudiation requirements within NASA when security email capability is required. The contractor shall ensure that personnel be screened at an appropriate level in accordance with NPR 2810.1, NASA Procedural Requirement for the Security of Information Technology. At the completion of the contract, the Contractor shall return all NASA information and IT resources provided to the contractor during the performance of the contract and certify that all NASA information has been purged from contractor-owned systems used in the performance of the contract. The Contractor shall insert the appropriate IT security requirements in all subcontracts when the subcontractor is required to (i) have physical or electronic access to NASA's computer systems, networks, or IT infrastructure or (ii) use information systems to generate, store, or exchange data with NASA or on behalf of NASA, regardless of whether the data resides on a NASA or a contractor's information system.

Due to the critical sensitivity of the content of the required IT security documents, the contractor shall prepare and deliver an IT Security Requirements Compliance Report (ITSRCR) as evidence that they have complied with the requirements of NFS 1852.204-76, Security Requirements for Unclassified Information Technology Resources. It shall include a statement of compliance to be signed by an Organization Senior Manager responsible for IT. The Contractor shall submit the ITSRCR in accordance with DRD 988CD-003.

Access Control

Access control to the MSFC, and to any other areas as directed by the Contracting Officer in writing, shall be in accordance with the requirements of Clause 50, 52.204-9, Personal Identity Verification of Contactor Personnel (NOV 2006).

It shall be the Contractor's responsibility to coordinate (with PSD) access to buildings and facilities not open to the general MSFC public and for any required after hour access.

It shall be the Contractor's responsibility to obtain authorized access to buildings and facilities, and arrange for them to be opened and closed to accomplish work under this order. Note, that a higher level of security and limited access to some buildings demands that scheduled work be well

coordinated. Typically, access may be coordinated through the building manager and/or approved by an employee listed on the posted Label 24, Controlled Security Area. MPR 1600.1 (Chapter 9) provides guidance for entrance into secure areas or offices.

Keys may be issued to the Contractor on a case-by-case basis when there is an established need approved by the PSD. MPR 1600.1 (Chapter 10) provides guidance for ensuring compliance with MSFC lock and key procedures. However, it shall be the Contractor's responsibility to arrange for adequate security of the buildings and facilities at the end of each workday. The Contractor shall be responsible for the cost of replacing any keys that are furnished to and lost by its employees. If the COTR decides that a lock must be replaced because of the loss of a key by any Contractor employee, the Contractor shall pay the cost of that replacement. The Contractor shall pay the cost of changing a lock or a lock combination if the COTR has reasonable cause to believe the combination has been compromised. The Contractor shall identify a single point key coordinator to interface with the Government for all issues related to key control.

No employee or representative of the Contractor will be admitted to the site of work unless they furnish satisfactory proof that they are a citizen of the United States, or, if an alien, their residence within the United States is legal.

Security Administration

The Contractor shall prepare and deliver a Badged Employee and Remote Location Listing in accordance with DRD 988MA-005.

The Contractor shall prepare and deliver Contractor Employee Clearance Document in accordance with DRD 988MA-006.

The Contractor shall prepare and deliver a Position Risk Designation for Non-NASA Employee Form in accordance with DRD 988MA-007.

The Contractor shall provide assistance to applicable NASA/MSFC organizations, investigative organizations, and the OSHA inspector if a complaint is filed or an investigation or inquiry is initiated on a company employee.

The Contractor shall remove from the site any individual whose behavior is deemed by the CO, COTR, or PSD to be contrary to the public interest or inconsistent with the best interests of Government security.

DATA PROCUREMENT DOC.
NO. ISSUE
988 **Revision D**

H36049D

CONTRACT/RFP

EXHIBIT NUMBER

2

ATTACHMENT NUMBER

**Logistics Services for the Marshall Space Flight
Center
PROJECT/SYSTEM**

DATA PROCUREMENT DOCUMENT

EG & G

CONTRACTOR

September 7, 2007

DATE

National Aeronautics and
Space Administration

National Aeronautics and Space Administration					DATA PROCUREMENT DOC.
DOCUMENT CHANGE LOG					NO. ISSUE
					988 Revision D
INCORPORATED REVISIONS OUTSTANDING REVISIONS			AS OF:	SUPERSEDING:	PAGE:
			09-07-07	05-01-07	1 of 1
AUTHORITY	PORTION AFFECTED - PAGE NO./NO.				REMARKS
	INTRO	SGR	DRL	DRD	
Contract Mod. 1			X		Corrected data type for the following DRDs: 988LS-002 988LS-018
				988MA-004	Changed OPR from "RS40" to "AD40"
Contract Mod. 41			X	X	Added the following DRDs: 988MA-005, Badged Employee and Remote IT User Listing 988MA-006, Contractor Employee Clearance Document 988MA-007, Position Risk Designation for Non-NASA Employee
				988CD-002	Deleted - replaced by 988MA-005
			X	X	Updated the Office of Primary Responsibility (OPR) Codes throughout the DPD
			X	X	Added DRD's included in previous modifications to the DPD.
Contract Mod. 47				988CD-001	Replaced DRD 988CD-001, Contractor Information Technology (IT) Security Program Plan with the current standard.
			X	X	Added the following DRD: 988CD-003, Information Technology (IT) Security Requirements Compliance Reports

MSFC - Form 3461-1 (Rev August 1970)

National Aeronautics and Space Administration			DATA PROCUREMENT DOC.		
PAGE REVISION LOG			NO. ISSUE:		
			988 Revision D		
NOTE: The current revision is denoted by a vertical line in the outer margin adjacent to the affected text.		AS OF:	SUPERSEDING:	PAGE:	
		09-07-07	05-01-07	1 of 1	
INSERT LATEST REVISED PAGES.			DISCARD SUPERSEDED PAGES.		
ITEM	PAGE	STATUS	ITEM	PAGE	STATUS
DPD	ALL	Revision D			

1.0 Subject to the Rights in Data clause, this Data Procurement Document (DPD) sets forth the data requirements in each Data Requirements Description (DRD) and shall govern that data required by the DPD for the contract. The contractor shall furnish data defined by the DRD's listed on the Data Requirements List (DRL) by category of data, attached hereto, and made a part of this DPD. Such data shall be prepared, maintained, and delivered to MSFC in accordance with the requirements set forth within this DPD. In cases where data requirements are covered by a Federal Acquisition Regulation (FAR) or NASA FAR Supplement (NFS) regulation or clause, the regulation will take precedence over the DPD, per FAR 52.215-8.

1.2 Data Requirements Descriptions (DRD's): Each data requirement listed on the DRL is given complete definition by a DRD. The DRD prescribes content, format, maintenance instructions, and submittal requirements. For the purpose of classification and control, DRD's of this DPD are grouped into the following broad functional data categories:

<u>CATEGORY SYMBOL</u>	<u>DESCRIPTION</u>
CD	Contractual Data
EE	Environmental Engineering
LS	Logistics Support
MA	Management
QE	Quality
SA	Safety

The symbols representing these data categories form part of the prefix of the DRD identification number. The first numerical characters reflect the DPD number.

1.3 Data Types for Contractual Efforts: The types of data and their contractually applicable requirements for approval and delivery are:

<u>TYPE</u>	<u>DESCRIPTION</u>
1	All issues and interim changes to those issues require written approval from the requiring organization before formal release for use or implementation.
2	MSFC reserves a time-limited right to disapprove in writing any issues and interim changes to those issues. Data shall be submitted to the procuring activity for review not less than 45 calendar days prior to its release for use or implementation. The contractor shall clearly identify the release target date in the "submitted for review" transmittal. If the contractor has not been notified of any disapproval prior to the release target date, the data shall be considered approved. To be an acceptable delivery, disapproved data shall be revised to remove causes for the disapproval before its release.
3	These data shall be delivered by the contractor as required by the contract and do not require MSFC approval. However, to be a satisfactory delivery, the data must satisfy all applicable contractual requirements.

2.0 STATEMENT OF GENERAL REQUIREMENTS

2.1 Applicable Documents: Documents included as applicable documents in this DPD are the issue specified in the Statement of Work, and form a part of the DPD to the extent specified herein. References to documents other than applicable documents in the data requirements of this DPD may sometimes be utilized. These do not constitute a contractual obligation on the contractor. They are to be used only as a possible example or to provide related information to assist the contractor in developing a response to that particular data requirement.

- 2.2 Printing: All printing, duplicating, or binding shall be in accordance with NFS 1852.208-81, Restrictions on Printing and Duplicating.
- 2.3 Distribution
- 2.3.1 Distribution of required documentation shall be specified in the "Distribution" statement (item 10) of each DRD. Recipient names and email addresses shall be noted on a separate distribution list to be furnished by the Contracting Officer or Contracting Officer's Technical Representative.
- 2.3.2 Electronic submission of data deliverables is required where feasible and software compatible, unless otherwise specified. Acceptable formats include Microsoft Word, Excel, or formats readable by Microsoft Word or Microsoft Excel as appropriate. The software versions shall be confirmed prior to submittals. Delivery shall be made on CD-ROMs in Personal Computer (PC) format. The Government utilizes Microsoft Windows and Office 98 for the PC.
- 2.4 Contractor's Internal Documents: The contractor's internal documents shall be used to meet the data requirements of this DPD unless a specific format is required by the applicable DRD.
- 2.5 Document Identification: Type 1 and 2 documents published by the contractor and submitted in response to the data requirements of this DPD shall be identified within an organized identification numbering system prescribed to MSFC by the contractor and, if applicable, as approved by MSFC. This number, change legend, date, and title constitute the minimum identification of the specific document and shall appear on the cover and title page. The contract number shall also appear on the cover and title page as separate markings. The originator and organization shall be included on the title page. The document number, change legend, and date shall appear on each page of the document. In the front matter of each document, identify the DPD number and applicable DRD number(s) required for document preparation. Drawings and ECP's are excluded from the marking provisions of this paragraph. All Type 1 documentation, excluding configuration management requirements, will be marked "PRELIMINARY PENDING MSFC APPROVAL," and once approved shall be reissued with "APPROVED BY MSFC" and the date and approval authority annotated on the cover.
- 2.6 Reference to Other Documents in Data Submittals: All referenced documents shall be made readily available to the cognizant MSFC organization upon request. The contractor should make sure that the references are available to MSFC in a manner which does not incur delays in the use of the response document.
- 2.7 Maintenance of Type 1 Document Submittals: Revisions of Type 1 documentation may be accomplished either by individual page revision or by a complete reissue of the document identified. Individual page revisions shall be made as deemed necessary by the contractor or as directed by the Contracting Officer. When complete reissues are made, the entire contents of the document shall be brought up to date and shall incorporate revised pages.
- 3.0 DPD MAINTENANCE PROCEDURES
- 3.1 MSFC-Initiated Change: New and/or revised data requirements will be incorporated by contract modification to which the new or revised portion of the DPD will be appended.
- 3.2 Contractor-Initiated Change: Contractor-proposed data requirements, or proposed changes to existing requirements shall be submitted to MSFC for approval.

- 3.3 DPD Change Procedures: Changes to a contractual issue of this DPD will be identified by placing a heavy vertical line in the right-hand margin extending the entire length of the change. In addition, the numerical control number of the contractual direction authorizing the change shall be placed adjacent to the vertical revision line. These revision identifiers shall be used to reflect the current revision only; any previous symbols on a page will be deleted by the current revision.
- 3.4 DPD Reissues: When conditions warrant, the DPD will be reissued by MSFC and will supersede the existing DPD in its entirety. Reissues will be issued by contractual direction. All revision symbols (vertical lines and contractual direction control numbers) will be removed from all pages; revision dates shall remain in the Date Revised block on DRD's that have been revised. The issue symbol, which will commence with "A" and progress through "Z," will be entered in the DPD identification block of each DRD page of the DPD.

LOGISTICS SERVICES FOR THE MARSHALL SPACE FLIGHT CENTER

DATA REQUIREMENTS LIST

<u>DRD</u>	<u>DATA TYPE</u>	<u>TITLE</u>	<u>OPR</u>
CD – Contractual Data			
988CD-001	2	Contractor Information Technology (IT) Security Program Plan	IS10
988CD-002	3	On-Site Employee Location Listing	PS10
988CD-003	2	Information Technology (IT) Security Requirements Compliance Reports	IS10
EE – Environmental Engineering (EE)			
988EE-001	1	Environmental Operations Plan	AS10
988EE-002	3	Environmental Monthly Report	AS10
988EE-003	3	Treatment, Storage, Disposal, Recycling Facilities Audit Reports	AS10
988EE-004	3	Tier II Report	AS10
988EE-005	3	Toxic Release Inventory Report	AS10
988EE-006	3	Biennial Hazardous Waste Report	AS10
988EE-007	3	Polychlorinated Biphenyl Annual Report	AS10
988EE-008	2	Special Waste Permits	AS10
988EE-009	2	Notification of Regulated Waste Activity (ADEM Form 8700-12)	AS10
988EE-010	1	Integrated Hazardous and Solid Waste Management Plan	AS10
988EE-011	3	Process Safety Report	AS10
988EE-012	2	Pollution Prevention Plan	AS10
988EE-013	3	Storm Water Inspection Log	AS10
988EE-014	3	Vapor Balance Test Report	AS10
988EE-015	3	Hazardous Air Pollutant (HAP) Reports	AS10
988EE-016	3	Air Emission Estimate Reports	AS10
LS – Logistics Support			
988LS-001	2	Government Property Management Plan	AS41
988LS-002	1	Maintenance Plan	AS40
988LS-003	2	Equipment Inventory Schedule	AS41
988LS-004	3	Inventory Progress Reports	AS41
988LS-005	1	Annual Inventory Report	AS41
988LS-006	3	Monthly Move Services Progress Report	AS41
988LS-007	2	Warehouse/Storage Requirements Plan	AS40
988LS-008	3	Performance Measures for Equipment Support Services Report	AS41
988LS-009	3	Performance Measures Physical Inventory Accuracy Report	AS41
988LS-010	3	Annual Walk-Thru Report	AS41
988LS-011	3	Annual Report of Utilization and Disposal of Domestic NASA Personal Property; Section D – Remarks, Cost of Sales	AS41
988LS-012	3	Government Furnished Equipment Inventory	AS41
988LS-013	3	Government Furnished Equipment Discrepancy Report	AS41
988LS-014	3	Annual Solid Waste Disposal Report	AS41
988LS-015	3	Annual Recyclables Report	AS41
988LS-016	3	Annual Affirmative Procurement Report	AS41
988LS-017	1	Report of Activities Generating Precious Metals	AS41
988LS-018	3	Packaging and Crating Services Report	AS42
988LS-019	3	Traffic Management Workload Report	AS42

LOGISTICS SERVICES FOR THE MARSHALL SPACE FLIGHT CENTER

DATA REQUIREMENTS LIST

<u>DRD</u>	<u>DATA TYPE</u>	<u>TITLE</u>	<u>OPR</u>
LS – Logistics Support (continued)			
988LS-020	3	Personnel Transport System Report	AS42
988LS-021	3	Mail Operations/Courier Services Report	AS42
988LS-022	3	Monthly Food Services Activities Report	AS60
988LS-023	3	Mail Services Report	AS40
988LS-024	3	Explosives and Propellants Inventory List	AS41
988LS-025	3	Monthly Retail Store Activities Report	AS40
MA – Management			
988MA-001	1	Management Operating Plan	AS40
988MA-002	2	Personnel Certification and Training Plan	AS40
988MA-003	3	Monthly Status Report	AS42
988MA-004	3	Contractor Cost Report	AS40
988MA-005	3	Badged Employee and Remote IT User Listing	AS50
988MA-006	3	Contractor Employee Clearance Document	AS50
988MA-007	3	Position Risk Designation for Non-NASA Employee Employee	AS50
QE – Quality			
988QE-001	1	Quality Control/Assurance Plan	AS40
SA - Safety			
988SA-001	2	On-site Safety and Health Plan	AS10/QD50
988SA-002	3	Mishap and Safety Statistics Reports	QD50
SW – Software			
988SW-001	2	Flight Hardware Support Request System Operations Manual and Users Guide	AS42

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.:** 988 **ISSUE:** Revision D
2. **DRD NO.:** **988CD-001**
3. **DATA TYPE:** 2
4. **DATE REVISED:** 09-07-07
5. **PAGE:** 1/2

6. **TITLE:** Contractor Information Technology (IT) Security Program Plan

7. **DESCRIPTION/USE:** To ensure that the contractor fully understands their responsibility for information and information technology (IT) security as required in NFS 1852.204-76. This plan will describe the contractor's information technology security program that addresses the management, operational, and technical aspects of protecting the confidentiality, integrity and availability of information and information technology systems.

8. **OPR:** IS10 9. **DM:** AS40

10. **DISTRIBUTION:** Per Contracting Officer's letter

11. **INITIAL SUBMISSION:** 30 days after contract modification

12. **SUBMISSION FREQUENCY:** Revise after any significant changes. Review and update every three years.

13. **REMARKS:** The Federal Information Processing Standards (FIPS) Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA) of 2002. FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems, specifies minimum security requirements for information and information systems supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements.

The seventeen security-related areas to be addressed in the content of the Contractor IT Security Program Plan represent a broad-based, balanced information technology security program that addresses the management, operational, and technical aspects of protecting information and information technology systems. Additional information for these security-related areas can be found in FIPS Pub 200.

14. **INTERRELATIONSHIP:** PWS paragraphs 1.2 (Performance Summary table), 1.2.D and 1.2.I.2.a.(12)

15. **DATA PREPARATION INFORMATION:**
- 15.1 **SCOPE:** The extent of the Contractor IT Security Program Plan can vary and shall be appropriate to comply with the breadth of sensitivity level security requirements for protecting information and information technology (IT) when the Contractor or its subcontractors must obtain physical or electronic access to NASA's computer systems, networks, or IT infrastructure, or where information is stored, generated, processed or exchanged by/with NASA or on behalf of NASA by a contractor or subcontractor, regardless of whether the information resides on a NASA or a contractor/ subcontractor's information system.

- 15.2 **APPLICABLE DOCUMENTS:**
NFS 1852.204-76 *Security Requirements for Unclassified Information Technology Resources (May 2007)*

DRD Continuation Sheet

TITLE: Contractor Information Technology (IT) Security
Program Plan

DRD NO.: **988CD-001**

DATA TYPE: 2

PAGE: 2/2

15. **DATA PREPARATION INFORMATION (CONTINUED):**

15.3 **CONTENTS:** The Contractor IT Security Program Plan shall contain:

- a. A brief description of the types of information that will be stored, generated, processed, or exchanged with NASA or on behalf of NASA during the performance of the contract. Provide the security categorization of the information (LOW, MODERATE, or HIGH). A description of the policy or procedure to ensure the return of all NASA information and IT resources provided to the contractor during the performance of the contract and certify that all NASA information has been purged from contractor-owned systems used in the performance of the contract.
- b. A brief description regarding personnel (location, local or remote connections or access, privileged users, etc.) and the IT resources (NASA provided or contractor-owned) and environments utilized in the support of the work to be performed and their access to information identified.
- c. A brief description of policy or procedure that ensures the contractor inserts NFS 1852.204-76 in all subcontracts as required.
- d. Provide a description of each of the security-related areas (see Remarks) with regard to policies and procedures of the contractor's enterprise-wide information technology security program protecting the confidentiality, integrity, and availability of information and information technology systems.
 1. Management.
 - (a) Certification, Accreditation, and Security Assessments.
 - (b) Planning.
 - (c) Risk Assessment.
 - (d) Systems and Services Acquisition.
 2. Operational.
 - (a) Awareness and Training.
 - (b) Configuration Management.
 - (c) Contingency Planning.
 - (d) Incident Response.
 - (e) Maintenance.
 - (f) Media Protection.
 - (g) Physical and Environmental Protection.
 - (h) Personnel Security.
 - (i) System and Information Integrity.
 3. Technical.
 - (a) Access Control.
 - (b) Audit and Accountability.
 - (c) Identification and Authentication.
 - (d) System and Communications Protection.

NOTE: Any security-related area not currently implemented in the Contractor's IT security program shall be identified and the contractor's plan of action for implementation shall be explained.

15.4 **FORMAT:** Contractor format is acceptable and shall be consistent with contents of paragraph 15.3d of this DRD.

15.5 **MAINTENANCE:** Changes shall be incorporated by change page or complete reissue.

DATA REQUIREMENTS DESCRIPTION (DRD)

1. **DPD NO.:** 988 **ISSUE:** Revision D
2. **DRD NO.:** **988CD-003**
3. **DATA TYPE:** 2
4. **DATE REVISED:** 09-07-07
5. **PAGE:** 1/3

6. **TITLE:** Information Technology (IT) Security Requirements Compliance Reports

7. **DESCRIPTION/USE:** To provide an overview of the Contractor's compliance with the IT security requirements in NFS 1852-204-76 and any additions/augmentations described in NPR 2810.1. This document will be used to verify the contractor's compliance including approval of their Organization Senior Management responsible for IT. An IT Security Requirements Compliance Report is required for each IT system identified for information stored, generated, processed or exchanged by/with NASA or on behalf of NASA by the contractor or subcontractor. This document will be used for the preparation of NASA IT security assessment for identifying the IT systems and appropriate Contractor IT security points of contact.

8. **OPR:** IS10 9. **DM:** AS40

10. **DISTRIBUTION:** Per Contracting Officer's letter

11. **INITIAL SUBMISSION:** For existing IT systems, 60 days after contract award. For new IT systems, initial submission is required at the conclusion of the Implementation phase and before the Operational phase of the System Development Life Cycle (SDLC).

12. **SUBMISSION FREQUENCY:** The reports shall be reviewed and updated on a yearly basis and after any significant changes to the IT System including personnel changes required to keep point of contact (POC) information current.

13. **REMARKS:** The NFS 1852.204-76 identifies security requirements for IT Security and Physical and Logical Access for unclassified information technology resources. It specifically identifies IT security requirements that include the preparation of certain IT security documents that are included in the Security Accreditation package required for a National Institute of Standards and Technology (NIST) Certification and Accreditation (C&A) process (reference NIST 800-37). However, NFS 1852.204-76 does not require the Contractor to follow a formal NIST C&A process unless there are any additions/ augmentations described in the NASA C&A processes established in NPR 2810.1.

The NFS 1852.204-76 requires the Contractor to submit to the Contracting Officer an IT Security Plan, Risk Assessment and FIPS 199 Assessment that shall be incorporated into the contract as compliance documents. Due to the critical sensitivity of the content of these documents, this IT Security Requirements Compliance Report will be accepted as evidence that these requirements have been completed. The IT System Security Plan and Risk Assessment documents will be prepared and maintained by the contractor and made available to MSFC IT Security Office upon request as part of any audit or assessment. Any exchange of such sensitive information will utilize appropriate measures to ensure the security of the information they contain. Due to the nature of some contracts, these required documents will be submitted and incorporated into the NASA C&A processes per NPR 2810.1 and are not submitted directly to the Contracting Officer.

14. **INTERRELATIONSHIP:** PWS paragraph 1.2.D

DRD Continuation Sheet

TITLE: Information Technology (IT) Security Requirements
Compliance Report(s)

DRD NO.: **988CD-003**

DATA TYPE: 2

PAGE: 2/3

15. **DATA PREPARATION INFORMATION:**

15.1 **SCOPE:** The IT Security Requirements Compliance Reports includes non-sensitive information about the IT system(s) utilized for performance of the contract, provide reference to policies and procedures required for compliance to IT security requirements, provides dates of compliance and a statement of compliance to be signed by Organization Senior Management responsible for IT.

15.2 **APPLICABLE DOCUMENTS:**

FIPS 200	<i>Minimum Security Requirements for Federal Information and Information Systems</i>
FIPS 199	<i>Standards for Security Categorization of Federal Information and Information Systems</i>
NFS 1852.204-76	<i>Security Requirements for Unclassified Information Technology Resources (May 2007)</i>
NPR 2810.1	<i>Security of Information Technology</i>
NIST SP 800-18	<i>Guide for Developing Security Plans for Federal Information Systems</i>
NIST SP 800-26	<i>Security of Self-Assessment Guide for Information Technology Systems</i>
NIST SP 800-30	<i>Risk Management Guide for Information Technology Systems</i>
NIST SP 800-34	<i>Contingency Planning Guide for Information Technology Systems</i>
NIST SP 800-61	<i>Computer Security Incident Handling Guide</i>

15.3 **CONTENTS:** In response to the requirements of NFS 1852.204-76, the IT Security Requirements Compliance Reports shall include the IT system name, the Security Category per FIPS 199 assessment, key IT security personnel contact information, dates of completion of the IT System Security Plan document prepared per NIST SP 800-18 and its annual review and update per NIST SP 800-26 and FIPS 200; Risk Assessment report prepared per NIST SP 800-30 and its annual update; and approval by Organization Senior Management for the IT system to operate. It shall identify the Contingency Plan document per NIST SP 800-34 and the date of completion of the annual "Classroom Exercises"; policies and procedures for Incident Response and Annual IT security training. It shall include a statement of compliance of providing NASA access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract; ensuring that incidents are reported per NSIT SP 800-61 and any confirmed incident of a system containing NASA information or controlling NASA assets is reported as required; ensuring contractor system administrator have demonstrated appropriate knowledge; ensuring that NASA's Sensitive But Unclassified (SBU) information is encrypted in storage and transmission; ensuring the return of all NASA information and IT resources at contract completion as required; certify that all NASA information has been purged from contractor-owned systems used in the performance of the contract; completing contractor personnel screening requirement and the inclusion of NFS 1852.204-76 in all subcontracts, as required. The statement of compliance shall be signed by Organization Senior Management responsible for IT ensuring that the requirements have been met.

When the Contractor is located at a NASA Center or installation or is using NASA IP address space, the IT Security Requirements Compliance Report shall also identify the processes for submitting requests for non-NASA provided external Internet connections to the Contracting Officer for approval by the NSCCB, compliance with NASA CIO metrics and the utilization of the NASA Public Key Infrastructure.

DRD Continuation Sheet

TITLE: Information Technology (IT) Security Requirements **DRD NO.:** **988CD-003**
Compliance Reports

DATA TYPE: 2 **PAGE:** 3/3

- 15. **DATA PREPARATION INFORMATION (CONTINUED):**
- 15.4 **FORMAT:** A template shall be provided by the MSFC IT Security Office (IS10).
- 15.5 **MAINTENANCE:** Changes shall be incorporated by complete reissue.