

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE
07
PAGE OF PAGES
1 5

2. AMENDMENT/MODIFICATION NO. 54
3. EFFECTIVE DATE Jan. 09. 2001
4. REQUISITION/PURCHASE REQ. NO. 440000054(1F)
5. PROJECT NO. (If applicable)

6. ISSUED BY CODE PS41-D
7. ADMINISTERED BY (If other than Item 6) CODE PS41-D

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

PS41-D/Rita Mason/ 256-544-5511

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State, and Zip Code)
Prime: Lockheed Martin Engineering & Sciences Company
2625 Bay Area Boulevard
Houston, TX 77058

(√) 9A. AMENDMENT OF SOLICITATION NO.
9B. DATED (SEE ITEM 11)

C/O: Lockheed Martin Space Mission Systems & Services
Attn: Frank Barnes
P.O. Box 240006
Huntsville, AL 35824-6406

X 10A. MODIFICATION OF CONTRACT/ORDER NO.
NAS8-44000
10B. DATED (SEE ITEM 13)

Code 51017 FACILITY CODE August 19, 1996

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 ACKNOWLEDGEMENT 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)
N/A

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 date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
- X C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
The Changes Clause
- D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor is not, is required to sign this document and return 0 copies to the issuing office.

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

	Negotiated Estimated Cost	Provisional Est. Cost	Award Fee Earned	Potential Award Fee	Total Contract Value	Total Sum Alloted
Previous Total:	\$137,247,592	1,500,000	\$4,992,202	\$ 760,694	\$144,500,488	\$143,561,458
This Modification:	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>
Revised Total:	\$137,247,592	\$1,500,000	\$4,992,202	\$ 760,694	\$144,500,488	\$143,561,458

See Page 2 for description of this modification.

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)
16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
Harry B. Craig
Contracting Officer

15B. CONTRACTOR/OFFEROR
(Signature of person authorized to sign)
15C. DATE SIGNED
16B. UNITED STATES OF AMERICA
BY /s/Harry B. Craig
(Signature of Contracting Officer)
16C. DATE SIGNED
Jan. 9, 2001

The purpose of this Change Order is to delete clause H.7 entitled, "Security Requirements for Unclassified Automated Information Resources (18.52.204-76)(SEP 1993)" in its entirety and replace it with the following:

1. H.7 1852.204-76 Security Requirements for Unclassified Technology Information Resources.

As prescribed in 1804.470-4, insert the following clause:

**SECURITY REQUIREMENTS FOR UNCLASSIFIED
TECHNOLOGY INFORMATION RESOURCES
(JULY 2000)**

(a) The Contractor shall comply with the security requirements outlined in NASA Policy Directive (NPD) 2810.1, Security of Information Technology, and NASA Procedures and Guidelines (NPG) 2810.1, Security of Information Technology. These policies apply to all IT systems and networks under NASA's purview operated by or on behalf of the Federal Government, regardless of location.

(b) (1) The Contractor shall ensure compliance by its employees with Federal directives and guidelines that deal with IT Security including, but not limited to, OMB Circular A-130, Management of Federal Information Resources, OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.), and all applicable Federal Information Processing Standards (FIPS).

(2) All Federally owned information is considered sensitive to some degree and must be appropriately protected by the Contractor as specified in applicable IT Security Plans. Types of sensitive information that may be found on NASA systems that the Contractor may have access to include, but are not limited to --

(i) Privacy Act information (5 U.S.C. 552a et seq.);

(ii) Export Controlled Data, (e.g. Resources protected by the International Traffic in Arms Regulations (22 CFR Parts 120-130)).

(3) The Contractor shall ensure that all systems connected to a NASA network or operated by the Contractor for NASA conform with NASA and Center security policies and procedures.

(c) (1) The Contractor's screening of Contractor personnel will be conducted in accordance with NPG 2810.1, Section 4.5 for personnel requiring unescorted or unsupervised physical or electronic access to NASA systems, programs, and data.

(2) The Contractor shall ensure that all such employees have at least a National Agency Check investigation. The Contractor shall submit a personnel security questionnaire (NASA Form 531), Name Check Request for National Agency Check (NAC) investigation, and Standard Form 85P, Questionnaire for Public Trust Positions (for specified sensitive positions), and a Fingerprint Card (FD-258 with NASA overprint in Origin Block) to the Center Chief of Security for each Contractor employee requiring screening. The required forms may be obtained from the Center Chief of Security. In the event that the NAC is not satisfactory, access shall not be granted. At the option of the

Government, background screenings may not be required for employees with recent or current Federal Government investigative clearances.

- (3) The Contractor shall have an employee checkout process that ensures –
- (i) Return of badges, keys, electronic access devices and NASA equipment;
 - (ii) Notification to NASA of planned employee terminations at least three days in advance of the employee's departure. In the case of termination for cause, NASA shall be notified immediately. All NASA accounts and/or network access granted terminated employees shall be disabled immediately upon the employee's separation from the Contractor; and
 - (iii) That the terminated employee has no continuing access to systems under the operation of the Contractor for NASA. Any access must be disabled the day the employee separates from the Contractor.
- (4) Granting a non-permanent resident alien (foreign national) access to NASA IT resources requires special authorization. The Contractor shall obtain authorization from the Center Chief of Security prior to granting a non-permanent resident alien access to NASA IT systems and networks.

(d) (1) The Contractor shall ensure that its employees with access to NASA information resources receive annual IT security awareness and training in NASA IT Security policies, procedures, computer ethics, and best practices.

(2) The Contractor shall employ an effective method for communicating to all its employees and assessing that they understand any Information Technology Security policies and guidance provided by the Center Information Technology Security Manager (CITSM) and/or Center CIO Representative as part of the new employee briefing process. The Contractor shall ensure that all employees represent that they have read and understand any new Information Technology Security policy and guidance provided by the CITSM and Center CIO Representative over the duration of the contract.

(3) The Contractor shall ensure that its employees performing duties as system and network administrators in addition to performing routine maintenance possess specific IT security skills. These skills include the following:

- (i) Utilizing software security tools.
- (ii) Analyzing logging and audit data.
- (iii) Responding and reporting to computer or network incidents as per NPG 2810.1.
- (iv) Preserving electronic evidence as per NPG 2810.1.
- (v) Recovering to a safe state of operation.

(4) The Contractor shall provide training to employees to whom they plan to assign system administrator roles. That training shall provide the employees with a full level of proficiency to meet all NASA system administrators' functional requirements. The Contractor shall have methods or processes to document that employees have mastered the training material, or have the required knowledge and skills. This applies to all system

administrator requirements.

(e) The Contractor shall promptly report to the Center IT Security Manager any suspected computer or network security incidents occurring on any system operated by the Contractor for NASA or connected to a NASA network. If it is validated that there is an incident, the Contractor shall provide access to the affected system(s) and system records to NASA and any NASA designated third party so that a detailed investigation can be conducted.

(f) The Contractor shall develop procedures and implementation plans that ensure that IT resources leaving the control of an assigned user (such as being reassigned, repaired, replaced, or excessed) have all NASA data and sensitive application software permanently removed by a NASA- approved technique. NASA-owned applications acquired via a "site license" or "server license" shall be removed prior to the resources leaving NASA's use. Damaged IT storage media for which data recovery is not possible shall be degaussed or destroyed. If the assigned task is to be assumed by another duly authorized person, at the Government's option, the IT resources may remain intact for assignment and use of the new user.

(g) The Contractor shall afford NASA, including the Office of Inspector General, access to the Contractor's and subcontractor's facilities, installations, operations, documentation, databases and personnel. Access shall be provided to the extent required to carry out a program of IT inspection, investigation and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of NASA data, and to preserve evidence of computer crime.

(h) (1) The Contractor shall document all vulnerability testing and risk assessments conducted in accordance with NPG 2810.1 and any other IT security requirements specified in the contract or as directed by the Contracting Officer.

(2) The results of these tests shall be provided to the Center IT Security Manager. Any Contractor system(s) connected to a NASA network or operated by the Contractor for NASA may be subject to vulnerability assessment or penetration testing as part of the Center's IT security compliance assessment and the Contractor shall be required to assist in the completion of these activities.

(3) A decision to accept any residual risk shall be the responsibility of NASA. The Contractor shall notify the NASA system owner and the NASA data owner within 5 working days if new or unanticipated threats or hazards are discovered by the Contractor, made known to the Contractor, or if existing safeguards fail to function effectively. The Contractor shall make appropriate risk reduction recommendations to the NASA system owner and/or the NASA data owner and document the risk or modifications in the IT Security Plan.

(i) The Contractor shall develop a procedure to accomplish the recording and tracking of IT System Security Plans, including updates, and IT system penetration and vulnerability tests for all NASA systems under its control or for systems outsourced to them to be managed on behalf of NASA. The Contractor must report the results of these actions directly to the Center IT Security Manager.

(j) When directed by the Contracting Officer, the Contractor shall submit for NASA approval a post-award security implementation plan outlining how the Contractor intendsto meet the requirements of NPG 2810.1. The plan shall subsequently be incorporated into the contract as a compliance document after receiving Government approval. The plan shall demonstrate thorough understanding of NPG 2810.1 and shall include as a minimum, the security measures and program safeguards to ensure that IT resources acquired and used by Contractor and subcontractor personnel --

(1) Are protected from unauthorized access, alteration, disclosure, or misuse of information processed, stored, or transmitted;

(2) Can maintain the continuity of automated information support for NASA missions, programs, and functions;

(3) Incorporate management, general, and application controls sufficient to provide cost-effective assurance of the systems' integrity and accuracy;

(4) Have appropriate technical, personnel, administrative, environmental, and access safeguards;

(5) Document and follow a virus protection program for all IT resources under its control; and

(6) Document and follow a network intrusion prevention program for all IT resources under its control.

(k) Prior to selecting any IT security solution, the Contractor shall consult with their Center IT Security Manager to ensure interoperability and compatibility with other systems with which there is a data or system interface requirement.

(l) The Contractor shall comply with all Federal and NASA encryption requirements for NASA flight programs (e.g., secure flight termination systems, encryption for satellite uplinks, encryption for flight and satellite command and control for both up and down link) and involve the Center Communications Security (COMSEC) Manager when selecting encryption solutions.

(m) The Contractor shall incorporate this clause in all subcontracts where the requirements identified in this clause are applicable to the performance of the subcontract.

(End of clause)

2. All other terms and conditions remain unchanged.