

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT ID CODE 01	PAGE OF 1	PAGES 2
---	--	---------------------------	--------------	------------

2. AMENDMENT/MODIFICATION NO. 37	3. EFFECTIVE DATE NOV 06 2006	4. REQUISITION/PURCHASE REQ. NO. N/A	5. PROJECT NO. (If applicable)
-------------------------------------	---	---	--------------------------------

6. ISSUED BY CODE PS31-MEF	7. ADMINISTERED BY (If other than Item 6)	CODE PS31-MEF
-------------------------------	---	------------------

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

A. Carol Terrell
256-544-6710
azona.c.terrell@nasa.gov
AUTOMATED INVOICE PAYMENT INFORMATION: (256) 544-5566

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State, and Zip Code) Coastal International Securities, Inc. Attn: Mr. John Vitale 7025 Newington Lorton, VA 22079	(x)	9A. AMENDMENT OF SOLICITATION NO. 9B. DATED (SEE ITEM 11) 10A. MODIFICATION OF CONTRACT/ORDER NO. H-34723D 10B. DATED (SEE ITEM 13) August 6, 2001
CODE OTL97 CAGE CODE 100753	X	

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)
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 FAR 43.103 (a) (3)
	D. OTHER PURSUANT TO THE AUTHORITY OF FAR 43.103(a)

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

	Fixed Amount	ID/IQ	Sum Allotted
Previous Amount	\$26,813,114	\$1,658,025.50	\$24,692,217
This Mod	-0-	\$ -0-	\$ -0-
Revised Total	\$26,813,114	\$1,658,025.50	\$24,692,217

See page 2 for description.

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) Michael E. Mateer Vice President <i>CURTIS L. WREN JR</i> PRESIDENT	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) A. Carol Terrell Contracting Officer
15B. CONTRACTOR/OFFEROR <i>Carl Terrell</i> (Signature of person authorized to sign)	15C. DATE SIGNED 30 Oct 06
16B. UNITED STATES OF AMERICA BY <i>A. Carol Terrell</i> (Signature of Contracting Officer)	
16C. DATE SIGNED NOV 06 2006	

The purposes of this modification are to: (1) incorporate the appropriate changes on Delivery Order H-34723D in accordance with Homeland Security Presidential Directive (HSPD-12) by adding FAR Clause 52.204-9, Personal Identity Verification (PIV) of Contractor Personnel; and (2) to incorporate a deviation issued by NASA Headquarters to require the use of the revised NASA FAR Supplement Clause 1852.204-76 "Security Requirements for Unclassified Information Technology (IT) Resources [Deviation]". It is mutually agreed that these actions will not require an adjustment to the contract value. The foregoing action is further implemented by the inclusion of the following changes:

1. Terms and Conditions, Page 3, Paragraph A. Federal Acquisition Regulation (48 CFR Chapter 1) Clauses are revised, as delineated to add FAR 52.204-9, Personal Identity Verification of Contractor Personnel (Jan 2006), and to delete from Paragraph B. NASA/FAR Supplement (48 CFR Chapter 18) Clauses NFS Clause 1852.204-76 "Security Requirements for Unclassified Information Technology (IT) Resources (Nov 2004).

2. Pages 34 thru Page 38 are revised as delineated to include in full text the revised NASA FAR Supplement Clause 1852.204-76 "Security Requirements for Unclassified Information Technology (IT) Resources (November 2004) [Deviation]" and adjust page numbers accordingly. Existing clauses following this inclusion are renumbered.

3. As a result of the foregoing changes, the following pages are deleted and the corresponding pages are substituted/added. Changes are noted by a vertical line in the right margin.

Clause (s) Changed	Pages Deleted	Pages Substituted/Added
Terms and Conditions	Page 3 (Mod 35)	Page 3 (Mod 37)
Adding Clause listed in Item No. 2 above and adjusting page numbers accordingly.	34 - 38 (Mod 35)	34 - 40 (Mod 37)

4. All other terms and conditions remain unchanged.

THE TERMS INCLUDED HEREIN ARE IN ADDITION TO THOSE INCLUDED IN THE GSA CONTRACT. IN THE EVENT THERE IS/ARE ANY CONFLICT(S), THE TERMS INCLUDED HEREIN WILL TAKE PRECEDENCE.

Note - The words *contract* and *order* as shown herein are used synonymously

The following clauses are incorporated by reference, with the same force and effect as if they were given in full text.

A. FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1) CLAUSES

<u>Clause No.</u>	<u>Title</u>
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)
52.204-9	Personal Identity Verification of Contractor Personnel (Jan 2006)
52.222-4	Contract Work Hours and Safety Standards Act -- Overtime Compensation (Jul 2005)
52.223-5	Pollution Prevention and Right-to-Know Information (Aug 2003)
52.223-6	Drug-Free Workplace (May 2001)
52.224-1	Privacy Act Notification (Apr 1984)
52.224-2	Privacy Act (Apr 1984)
52.228-5	Insurance - Work on a Government Installation (Jan 1997)
52.237-2	Protection of Government Buildings, Equipment, and Vegetation (Apr 1984)
52.237-3	Continuity of Services (Jan 1991)
52.245-2	Government Property (Fixed-Price Contracts) (May 2004)
52.253-1	Computer Generated Forms (Jan 1991)

B. NASA/FAR SUPPLEMENT (48 CFR CHAPTER 18) CLAUSES

<u>Clause No.</u>	<u>Title</u>
1852.204-75	Security Classification Requirements (Sep 1989) Performance under this contract will involve access to and/or generation of classified information, work in a security area, or both, up to the level of [Secret]. See Federal Acquisition Regulation clause 52.204-2 in this contract and DD Form 254, Contract Security Classification Specification, Attachment 8 and DD Form 254].

21. Security Requirements for Unclassified Information Technology Resources
(1852.204-76)(NOVEMBER 2004 [(DEVIATION)])

(a) The Contractor shall be responsible for information and information technology (IT) security when 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 where 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, 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 and the NASA Security Operations Center.

(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 all individuals who perform tasks as a system administrator, or have authority to perform tasks normally performed by a system administrator, 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, network services, files storage, and/or web services, to someone else 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) 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) The Contractor shall insert this clause, including this paragraph (f), in all subcontracts when the subcontractor is required to --

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

(2) 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.

(End of clause)

22. Access to Sensitive Information (1852.237-72) (JUNE 2005)

(a) As used in this clause, "sensitive information" refers to information that a contractor has developed at private expense, or that the Government has generated that qualifies for an exception to the Freedom of Information Act, which is not currently in the public domain, and which may embody trade secrets or commercial or financial information, and which may be sensitive or privileged.

(b) To assist NASA in accomplishing management activities and administrative functions, the Contractor shall provide the services specified elsewhere in this contract.

(c) If performing this contract entails access to sensitive information, as defined above, the Contractor agrees to –

(1) Utilize any sensitive information coming into its possession only for the purposes of performing the services specified in this contract, and not to improve its own competitive-position in another procurement.

(2) Safeguard sensitive information coming into its possession from unauthorized use and disclosure.

(3) Allow access to sensitive information only to those employees that need it to perform services under this contract.

(4) Preclude access and disclosure of sensitive information to persons and entities outside of the Contractor's organization.

(5) Train employees who may require access to sensitive information about their obligations to utilize it only to perform the services specified in this contract and to safeguard it from unauthorized use and disclosure.

(6) Obtain a written affirmation from each employee that he/she has received and will comply with training on the authorized uses and mandatory protections of sensitive information needed in performing this contract.

(7) Administer a monitoring process to ensure that employees comply with all reasonable security procedures, report any breaches to the Contracting Officer, and implement any necessary corrective actions.

(d) The Contractor will comply with all procedures and obligations specified in its Organizational Conflicts of Interest Avoidance Plan, which this contract incorporates as a compliance document.

(e) The nature of the work on this contract may subject the Contractor and its employees to a variety of laws and regulations relating to ethics, conflicts of interest, corruption, and other criminal or civil matters relating to the award and administration of government contracts. Recognizing that this contract establishes a high standard of accountability and trust, the Government will carefully review the Contractor's performance in relation to the mandates and restrictions found in these laws and regulations. Unauthorized uses or disclosures of sensitive information may result in termination of this contract for default, or in debarment of the Contractor for serious misconduct affecting present responsibility as a government contractor.

(f) The Contractor shall include the substance of this clause, including this paragraph (f), suitably modified to reflect the relationship of the parties, in all subcontracts that may involve access to sensitive information.

(End of Clause)

23. Release of Sensitive Information (1852.237-73) (JUNE 2005)

(a) As used in this clause, "sensitive information" refers to information, not currently in the public domain, that the Contractor has developed at private expense, that may embody trade secrets or commercial or financial information, and that may be sensitive or privileged.

(b) In accomplishing management activities and administrative functions, NASA relies heavily on the support of various service providers. To support NASA activities and functions, these service providers, as well as their subcontractors and their individual employees, may need access to sensitive information submitted by the Contractor under this contract. By submitting this proposal or performing this contract, the Contractor agrees that NASA may release to its service providers, their subcontractors, and their

individual employees, sensitive information submitted during the course of this procurement, subject to the enumerated protections mandated by the clause at 1852.237-72, Access to Sensitive Information. (c)(1) The Contractor shall identify any sensitive information submitted in support of this proposal or in performing this contract. For purposes of identifying sensitive information, the Contractor may, in addition to any other notice or legend otherwise required, use a notice similar to the following:

Mark the title page with the following legend:

This proposal or document includes sensitive information that NASA shall not disclose outside the Agency and its service providers that support management activities and administrative functions. To gain access to this sensitive information, a service provider's contract must contain the clause at NFS 1852.237-72, Access to Sensitive Information. Consistent with this clause, the service provider shall not duplicate, use, or disclose the information in whole or in part for any purpose other than to perform the services specified in its contract. This restriction does not limit the Government's right to use this information if it is obtained from another source without restriction. The information subject to this restriction is contained in pages [insert page numbers or other identification of pages].

Mark each page of sensitive information the Contractor wishes to restrict with the following legend:

Use or disclosure of sensitive information contained on this page is subject to the restriction on the title page of this proposal or document. (2) The Contracting Officer shall evaluate the facts supporting any claim that particular information is "sensitive." This evaluation shall consider the time and resources necessary to protect the information in accordance with the detailed safeguards mandated by the clause at 1852.237-72, Access to Sensitive Information. However, unless the Contracting Officer decides, with the advice of Center counsel, that reasonable grounds exist to challenge the Contractor's claim that particular information is sensitive, NASA and its service providers and their employees shall comply with all of the safeguards contained in paragraph (d) of this clause.

(d) To receive access to sensitive information needed to assist NASA in accomplishing management activities and administrative functions, the service provider must be operating under a contract that contains the clause at 1852.237-72, Access to Sensitive Information. This clause obligates the service provider to do the following:

(1) Comply with all specified procedures and obligations, including the

Organizational Conflicts of Interest Avoidance Plan, which the contract has incorporated as a compliance document. (2) Utilize any sensitive information coming into its possession only for the purpose of performing the services specified in its contract.

(3) Safeguard sensitive information coming into its possession from unauthorized use and disclosure.

(4) Allow access to sensitive information only to those employees that need it to perform services under its contract.

(5) Preclude access and disclosure of sensitive information to persons and entities outside of the service provider's organization.

(6) Train employees who may require access to sensitive information about their obligations to utilize it only to perform the services specified in its contract and to safeguard it from unauthorized use and disclosure.

(7) Obtain a written affirmation from each employee that he/she has received and will comply with training on the authorized uses and mandatory protections of sensitive information needed in performing this contract.

(8) Administer a monitoring process to ensure that employees comply with all reasonable

security procedures, report any breaches to the Contracting Officer, and implement any necessary corrective actions.

(e) When the service provider will have primary responsibility for operating an information technology system for NASA that contains sensitive information, the service provider's contract shall include the clause at 1852.204-76, Security Requirements for Unclassified Information Technology Resources. The Security Requirements clause requires the service provider to implement an Information Technology Security Plan to protect information processed, stored, or transmitted from unauthorized access, alteration, disclosure, or use. Service provider personnel requiring privileged access or limited privileged access to these information technology systems are subject to screening using the standard National Agency Check (NAC) forms appropriate to the level of risk for adverse impact to NASA missions. The Contracting Officer may allow the service provider to conduct its own screening, provided the service provider employs substantially equivalent screening procedures (f) This clause does not affect NASA's responsibilities under the Freedom of Information Act.

(g) The Contractor shall insert this clause, including this paragraph (g), suitably modified to reflect the relationship of the parties, in all subcontracts that may require the furnishing of sensitive information.

(End of clause)

REVISED LIST OF ATTACHMENTS

Attachment	Title
1.	Performance Work Statement (includes revised Performance Requirements Summary)
2.	Data Procurement Documents
3.	Wage Determination and Comparability Statement
4	Procedural and Regulatory Guidance
6.	Installation-Provided Property Listing
7.	Contract Security Classification Specification
8.	ID/IQ Schedule of Fully Burdened Not-to-Exceed(NTE) Labor Rates and Other Direct Cost Not-To-Exceed Burden Rates