

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE

PAGE OF PAGES

1 8

2. AMENDMENT/MODIFICATION NO.

008

3. EFFECTIVE DATE

APR 15 2002

4. REQUISITION/PURCHASE REQ. NO. E / 5 / 01

OCIO-01-175

5. PROJECT NO. (If applicable)

6. ISSUED BY

CODE

7. ADMINISTERED BY (If other than Item 6)

CODE

U.S. Nuclear Regulatory Commission
Division of Contracts and Property Mgt.
Attn: Mark Flynn, MS T-7-I-2
IT Acquisition Management Branch
Washington DC 20555

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

(X)

9A. AMENDMENT OF SOLICITATION NO.

FileNET Corporation
Attn: Gail Fitzmaurice
Professional Services Contract Manager
115 Standish Ave.
Plymouth, MA 02360

9B. DATED (SEE ITEM 11)

10A. MODIFICATION OF CONTRACT/ORDER NO
NRC-33-01-175

10B. DATED (SEE ITEM 13)

CODE

FACILITY CODE

X

11-22-2000

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 of 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.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

See pages 2-7.

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

(X) 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).

C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:

D. OTHER (Specify type of modification and authority) Section B.5, FAR 52.212-4 and mutual agreement of the parties

E. IMPORTANT: Contractor is not, X is required to sign this document and return 2 copies to the issuing office.

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

See pages 2-8 for description of 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)

Gail Fitzmaurice Contracts Manager

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

Mark J. Flynn Contracting Officer

15B. CONTRACTOR/OFFEROR

Signature of person authorized to sign

15C. DATE SIGNED

4/15/2002

16B. UNITED STATES OF AMERICA

BY

Signature of Contracting Officer

16C. DATE SIGNED

4/5/02

The purpose of this modification is to (1) increase the ceiling of the contract by \$835,920.00, from 692,325.00 to \$1,528,245.00, to add contract line items 006 - 010, and (2) extend the period of performance by 13 months to provide additional professional services required to support the ADAMS FileNET software. This modification also incorporates terms, for information technology security and equipment use, into the contract as these requirements are applicable to the effort being performed under the contract. FileNET personnel security clearances related to this effort have been, and should continue to be, processed through the NRC Project Officer for this contract. Accordingly, the contract is modified as follows:

Section B.4, "Price Schedule" is revised to add the following line items:

"PROFESSIONAL SERVICES (03/25/01 - 12/31/03)

| <u>ITEM NO.</u> | <u>DESCRIPTION</u>  | <u>EST. QTY.</u> | <u>UNIT</u> | <u>UNIT PRICE</u> | <u>AMOUNT</u> |
|-----------------|---|------------------|-------------|-------------------|---------------|
| 006             | Business/Lead Consultant  | [REDACTED]       | [REDACTED]  | [REDACTED]        | \$429,420.00  |
| 007             | Project Manager   | [REDACTED]       | [REDACTED]  | [REDACTED]        | 56,100.00     |
| 008             | Sr. Consultant  | [REDACTED]       | [REDACTED]  | [REDACTED]        | 127,600.00    |
| 009             | Lead Developer  | [REDACTED]       | [REDACTED]  | [REDACTED]        | 140,800.00    |
| 010             | Estimated Travel if required, not to exceed. Reimbursed in accordance with Fed. Travel Requirements." | [REDACTED]       | [REDACTED]  | [REDACTED]        | 82,000.00     |

Under Section B.5, "Consideration and Obligation--Delivery Orders (JUN 1988)," the first sentence of paragraph (a) is deleted in its entirety and replaced with the following:

" (a) The total estimated amount of this contract (ceiling) for the products/services ordered, delivered, and accepted under this contract is \$1,528,245.00."

Section B.6, "Duration of Contract Period (MAR 1987)" is changed to read as follows:

"This contract shall commence on November 22, 2000, and will expire on December 31, 2003."

Section C.11 is hereby incorporated into the contract as follows:

**“C.11 2052.204-70 SECURITY**

(a) Security/Classification Requirements Form. The attached NRC Form 187 (See List of Attachments) furnishes the basis for providing security and classification requirements to prime contractors, subcontractors, or others (e.g., bidders) who have or may have an NRC contractual relationship that requires access to classified information or matter, access on a continuing basis (in excess of 30 or more days) to NRC Headquarters controlled buildings, or otherwise requires NRC photo identification or card-key badges.

(b) It is the contractor's duty to safeguard National Security Information, Restricted Data, and Formerly Restricted Data. The contractor shall, in accordance with the Commission's security regulations and requirements, be responsible for safeguarding National Security Information, Restricted Data, and Formerly Restricted Data, and for protecting against sabotage, espionage, loss, and theft, the classified documents and material in the contractor's possession in connection with the performance of work under this contract. Except as otherwise expressly provided in this contract, the contractor shall, upon completion or termination of this contract, transmit to the Commission any classified matter in the possession of the contractor or any person under the contractor's control in connection with performance of this contract. If retention by the contractor of any classified matter is required after the completion or termination of the contract and the retention is approved by the contracting officer, the contractor shall complete a certificate of possession to be furnished to the Commission specifying the classified matter to be retained. The certification must identify the items and types or categories of matter retained, the conditions governing the retention of the matter and their period of retention, if known. If the retention is approved by the contracting officer, the security provisions of the contract continue to be applicable to the matter retained.

(c) In connection with the performance of the work under this contract, the contractor may be furnished, or may develop or acquire, proprietary data (trade secrets) or confidential or privileged technical, business, or financial information, including Commission plans, policies, reports, financial plans, internal data protected by the Privacy Act of 1974 (Pub. L. 93-579), or other information which has not been released to the public or has been determined by the Commission to be otherwise exempt from disclosure to the public. The contractor agrees to hold the information in confidence and not to directly or indirectly duplicate, disseminate, or disclose the information in whole or in part to any other person or organization except as may be necessary to perform the work under this contract. The contractor agrees to return the information to the Commission or otherwise dispose of it at the direction of the contracting officer. Failure to comply with this clause is grounds for termination of this contract.

(d) Regulations. The contractor agrees to conform to all security regulations and requirements of the Commission which are subject to change as directed by the NRC Division of Facilities and Security and the Contracting Officer. These changes will be under the authority of the FAR Changes clause referenced in this document.

(e) Definition of National Security Information. The term National Security Information, as used in this clause, means information that has been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(f) Definition of Restricted Data. The term Restricted Data, as used in this clause, means all data concerning design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but does not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended.

(g) Definition of Formerly Restricted Data. The term Formerly Restricted Data, as used in this clause, means all data removed from the Restricted Data category under Section 142-d of the Atomic Energy Act of 1954, as amended.

(h) Security Clearance Personnel. The contractor may not permit any individual to have access to Restricted Data, Formerly Restricted Data, or other classified information, except in accordance with the Atomic Energy Act of 1954, as amended, and the Commission's regulations or requirements applicable to the particular type or category of classified information to which access is required. The contractor shall also execute a Standard Form 312, Classified Information Nondisclosure Agreement, when access to classified information is required.

(i) Criminal Liabilities. It is understood that disclosure of National Security Information, Restricted Data, and Formerly Restricted Data relating to the work or services ordered hereunder to any person not entitled to receive it, or failure to safeguard any Restricted Data, Formerly Restricted Data, or any other classified matter that may come to the contractor or any person under the contractor's control in connection with work under this contract, may subject the contractor, its agents, employees, or subcontractors to criminal liability under the laws of the United States. (See the Atomic Energy Act of 1954, as amended, 42 U.S.C. 2011 et seq.; 18 U.S.C. 793 and 794; and Executive Order 12958.)

(j) Subcontracts and Purchase Orders. Except as otherwise authorized in writing by the contracting officer, the contractor shall insert provisions similar to the foregoing in all subcontracts and purchase orders under this contract.

(k) In performing the contract work, the contractor shall classify all documents, material, and equipment originated or generated by the contractor in accordance with guidance issued by the Commission. Every subcontract and purchase order issued hereunder involving the origination or generation of classified documents, material, and equipment must provide that the subcontractor or supplier assign classification to all documents, material, and equipment in accordance with guidance furnished by the contractor.

## **C.12 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY SERVICES**

The proposer/contractor must identify all individuals and propose the level of Information Technology (IT) approval for each, using the following guidance. The NRC sponsoring office shall make the final determination of the level, if any, of IT approval required for all individuals working under this contract.

The Government shall have and exercise full and complete control over granting, denying, withholding, or terminating building access approvals for individuals performing work under this contract.

### **CONTRACTOR SECURITY REQUIREMENTS FOR LEVEL I**

Performance under this contract will involve prime contractor personnel, subcontractors or others who perform services requiring direct access to or operate agency sensitive information technology systems or data (IT Level I).

The IT Level I involves responsibility for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning, and design of a computer system, including hardware and software; or the capability to access a computer system during its operation or maintenance in such a way that could cause or that has a relatively high risk of causing grave damage; or the capability to realize a significant personal gain from computer access. Such contractor personnel shall be subject to the NRC contractor personnel security requirements of NRC Management Directive (MD) 12.3, Part I and will require a favorably adjudicated Limited Background Investigation (LBI).

A contractor employee shall not have access to NRC facilities, sensitive information technology systems or data until he/she is approved by Personnel Security Branch, Division of Facilities and Security (PERSEC/DFS) first for temporary access (based on a favorable adjudication of their security forms and checks) and final access (based on a favorably adjudicated LBI) in accordance with the procedures found in NRC MD 12.3, Part I. The individual will be subject to a reinvestigation every 10 years. Timely receipt of properly completed security applications is a contract requirement. Failure of the contractor to comply with this condition within the ten work-day period may be a basis to void the notice of selection. In that event, the Government may select another firm for award.

The contractor shall submit a completed security forms packet, including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the Project Officer to PERSEC/DFS for review and favorable adjudication, prior to the individual performing work under this contract. The contractor shall assure that all forms are accurate, complete, and legible (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the contractor in a sealed envelope), as set forth in MD 12.3 which is incorporated into this contract by reference as though fully set forth herein. Based on PERSEC review of the applicant's security forms and/or the receipt of adverse information by

NRC, the individual may be denied access to NRC facilities, sensitive information technology systems or data until a final determination is made of his/her eligibility under the provisions of MD 12.3. Any questions regarding the individual's eligibility for IT Level I approval will be resolved in accordance with the due process procedures set forth in MD 12.3 Exhibit 1 and E. O. 12968.

In accordance with NRCAR 2052.204-70 "Security," IT Level I contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments) which furnishes the basis for providing security requirements to prime contractors, subcontractors or others (e.g., bidders) who have or may have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems and data or other access to such systems and data; access on a continuing basis (in excess of 30 days) to NRC Headquarters controlled buildings; or otherwise requires NRC photo identification or card-key badges.

#### CONTRACTOR SECURITY REQUIREMENTS FOR LEVEL II

Performance under this contract will involve contractor personnel that develop and/or analyze sensitive information technology systems or data or otherwise have access to such systems and data (IT Level II).

The IT Level II involves responsibility for the planning, design, operation, or maintenance of a computer system and all other computer or IT positions. Such contractor personnel shall be subject to the NRC contractor personnel requirements of MD 12.3, Part I, which is hereby incorporated by reference and made a part of this contract as though fully set forth herein, and will require a favorably adjudicated Access National Agency Check with Inquiries (ANACI).

A contractor employee shall not have access to NRC facilities, sensitive information technology systems or data until he/she is approved by PERSEC/DFS first for temporary access (based on a favorable review of their security forms and checks) and final access (based on a favorably adjudicated ANACI) in accordance with the procedures found in MD 12.3, Part I. The individual will be subject to a reinvestigation every 10 years. Timely receipt of properly completed security applications is a contract requirement. Failure of the contractor to comply with this condition within the ten work-day period may be a basis to void the notice of selection. In that event, the Government may select another firm for award.

The contractor shall submit a completed security forms packet, including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the Project Officer to the NRC PERSEC/DFS for review and favorable adjudication, prior to the individual performing work under this contract. The contractor shall assure that all forms are accurate, complete, and legible (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the contractor in a sealed envelope), as set forth in MD 12.3. Based on PERSEC review of the applicant's security forms and/or the receipt of adverse information by NRC, the individual may be denied access to NRC facilities, sensitive

information technology systems or data until a final determination is made of his/her eligibility under the provisions of MD 12.3. Any questions regarding the individual's eligibility for IT Level II approval will be resolved in accordance with the due process procedures set forth in MD 12.3 Exhibit 1 and E. O. 12968.

In accordance with NRCAR 2052.204-70 "Security," IT Level II contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments) which furnishes the basis for providing security requirements to prime contractors, subcontractors or others (e.g. bidders) who have or may have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems and data or other access to such systems and data; access on a continuing basis (in excess of 30 days) to NRC Headquarters controlled buildings; or otherwise requires NRC photo identification or card-key badges.

#### CANCELLATION OR TERMINATION OF IT ACCESS/REQUEST

When a request for investigation is to be withdrawn or canceled, the contractor shall immediately notify the Project Officer by telephone in order that he/she will contact the PERSEC/DFS so that the investigation may be promptly discontinued. The notification shall contain the full name of the individual, and the date of the request. Telephone notifications must be promptly confirmed in writing to the Project Officer who will forward the confirmation to the PERSEC/DFS. Additionally, PERSEC/DFS must be immediately notified when an individual no longer requires access to NRC sensitive automated information technology systems or data, including the voluntary or involuntary separation of employment of an individual who has been approved for or is being processed for access under the NRC Personnel Security Program.

#### **C.13 APPROPRIATE USE OF GOVERNMENT FURNISHED INFORMATION TECHNOLOGY (IT) EQUIPMENT AND/ OR IT SERVICES/ ACCESS (MARCH 2002)**

As part of contract performance the NRC may provide the contractor with information technology (IT) equipment and IT services or IT access as identified in the solicitation or subsequently as identified in the contract or delivery order. Government furnished IT equipment, or IT services, or IT access may include but is not limited to computers, copiers, facsimile machines, printers, pagers, software, phones, Internet access and use, and email access and use. The contractor (including the contractor's employees, consultants and subcontractors) shall use the government furnished IT equipment, and / or IT provided services, and/ or IT access solely to perform the necessary efforts required under the contract. The contractor (including the contractor's employees, consultants and subcontractors) are prohibited from engaging or using the government IT equipment and government provided IT services or IT access for any personal use, misuse, abuses or any other unauthorized usage.

The contractor is responsible for monitoring its employees, consultants and subcontractors to ensure that government furnished IT equipment and/ or IT services, and/ or IT access are not being used for personal use, misused or abused. The government reserves the right to

withdraw or suspend the use of its government furnished IT equipment, IT services and/ or IT access arising from contractor personal usage, or misuse or abuse; and/ or to disallow any payments associated with contractor (including the contractor's employees, consultants and subcontractors) personal usage, misuses or abuses of IT equipment, IT services and/ or IT access; and/ or to terminate for cause the contract or delivery order arising from violation of this provision."

This modification does not obligate funds.

All other terms and conditions of this contract remain unchanged.