

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE

PAGE 1 OF PAGES 16

2. AMENDMENT/MODIFICATION NO.
2

3. EFFECTIVE DATE
MAY 22 2003

4. REQUISITION/PURCHASE REQ. NO. 10370730C
C10-03-311

5. PROJECT NO. (If applicable)

6. ISSUED BY
CODE 3100
U.S. Nuclear Regulatory Commission
Jeffrey R. Mitchell, Div of Contracts
Two White Flint North - MS T-7-I-2
Contract Management Center 1
Washington, DC 20555

7. ADMINISTERED BY (If other than Item 6)
CODE 3100
U.S. Nuclear Regulatory Commission
Jeffrey R. Mitchell, Div of Contracts
Two White Flint North - MS T-7-I-2
Contract Management Center 1
Washington, DC 20555

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

Artel, Inc.
ATTN: Jane M. Brady
Vice President, Contracts
1893 Preston White Drive
Reston VA 22091

(X) 9A. AMENDMENT OF SOLICITATION NO.

RS-C10-03-311

9B. DATED (SEE ITEM 11)

10A. MODIFICATION OF CONTRACT/ORDER NO.
NRC-33-03-311

10B. DATED (SEE ITEM 13)

02-10-2003

CODE FACILITY CODE

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. 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 2

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)

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.)

See Page 2 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)

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

Joyce A. Fields
Contracting Officer

15B. CONTRACTOR/OFFEROR

15C. DATE SIGNED

16B. UNITED STATES OF AMERICA

16C. DATE SIGNED

(Signature of person authorized to sign)

BY Joyce A. Fields
(Signature of Contracting Officer)

5/22/03

The purpose of this modification is to issue Delivery Order No. 2 entitled, "NRC Web Site and Internal Network Security Vulnerability Testing" to be performed in accordance with the attached Statement of Work for the effort and your proposal dated March 31, 2003, including the revised Cost Proposal dated May 5, 2003. The Delivery Order will be in effect for 12 months from the effective date of the issuance of Modification No. 2 to NRC-33-03-311.

Section B.2, "Consideration and Obligation – Delivery Orders (Jun 1988)", the first sentence of paragraph (b) is deleted in its entirety and replaced with the following:

"(b) The amount presently obligated with respect to this contract is \$297,816.00."

Accounting Data for NRC-33-03-311 Mod No.2, Delivery Order No.2 is as follows:

Delivery Order 2
APPN No: 31X0200.310
B&R No: 310-15-550-398
Job Code: J1159
BOC: 252A
Obligated Amount: \$80,022.00

A summary of obligations for this contract, from award date through the date of this action, is given below:

Total FY03 Obligations:	\$100,000	Award IDIQ, Delivery Order No. 1
	\$117,794	Mod 1, Delivery Order No. 1 Mod 1
	\$80,022.00	Mod 2, Delivery Order No. 2
Cumulative Total of NRC Obligations:	\$297,816.00	

This modification obligates FY03 funds in the amount of \$80,022.00.

All other terms and conditions of this contract remain unchanged.

DELIVERY ORDER NO. 2

**“NRC Web Site and Internal Network Security Vulnerability Testing”
Statement of Work**

I. Purpose of Project

The U.S. Nuclear Regulatory Commission (NRC) has a requirement to perform Web Site Security Testing in support of its mission to conduct active monitoring of compliance throughout the NRC. Congressional Oversight, General Accounting Office, and Office of the Inspector General reviews have shown government web sites and networks to be vulnerable to computer hackers and information warfare professionals. The NRC also requires the capability to conduct detailed traffic analysis providing centralized secure situational awareness and visibility into network operations and potential internal and external security threats.

II. Background

The NRC is responsible for two web sites (<http://www.nrc.gov>). Each of NRC's web sites and our LAN/WAN infrastructure faces an ongoing and increasing risk. A successful attack could result in defacement, or the loss or manipulation of sensitive information. Abuse can result from the vulnerability of NRC web sites resulting in loss of public trust.

An effective way to determine if the NRC's web sites and the LAN/WAN infrastructure are secure is to test them for vulnerability to attacks. There are tens of thousands of potential Internet security vulnerabilities. Security gaps at NRC can result from off-the-shelf software, simple system changes, or advances in hacker technology. NRC's web sites and the LAN/WAN infrastructure are similar to all other systems: when they are changed or when they are expected to handle external developments (i.e. advances in hacker technology) they must be tested. The NRC also must account for an increasing threat to its network infrastructure from insider malicious activities.

III. Project Scope

The goal of this project is to run independent external penetration tests on NRC web sites and internal situational awareness testing of the NRC LAN/WAN infrastructure to discover vulnerabilities that could be exploited by an attacker to damage or deface NRC web sites and their underlying network infrastructure systems. The deliverable will be in the form of reports on the NRC web site and on the LAN/WAN infrastructure vulnerabilities. The NRC will take action to mitigate those vulnerabilities as they are discovered. The Contractor shall conduct penetration testing work from its own site remotely, and the contractor shall also conduct part of the testing here at NRC,

specifically in support of the testing, monitoring, and determining the situational awareness of the security posture for the internal LAN/WAN infrastructure.

The following laws, regulations, and guidance, address computer security matters:

- Public Law 100-235, Computer Security Act of 1987 • Information Technology Management Reform Act (Clinger-Cohen Act) of 1996
- Government Information Security Reform Act (GISRA) of 2000
- Federal Information Security Management Act (FISMA) of 2002
- OMB Circular A-11
- Federal Information Processing Standards (FIPS)
- Office of Management and Budget Circular A-130, Management of Federal Information Resources, updated November 3, 2000, App. III
- Office of Management and Budget Circular A-123, Management Accountability and Control
- Presidential Decision Directive (PDD) 63
- The Government Information Security Reform Act 2000, Title X, subtitle G of the 2001 Defense Authorization Act (P.L. 106-398)
- NIST Special Publications 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems and 800-12, An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-18
- Draft NIST Special Publication on Intrusion Detection Systems
- The Government Paperwork Elimination Act
- Electronic Signatures in Global and National Commerce Act
- Public Law 93-579, Privacy Act of 1974
- Executive Order 12958, National Security
- Atomic Energy Act of 1954
- Nuclear Regulatory Commission Directive 12.5, NRC AIS Security Program

IV Project Tasks

The Contractor shall conduct non-destructive remote penetration testing of NRC's computing enterprise, employing the full range of manual and automated tactics, techniques, tools and procedures available to the Contractor. The Contractor shall not perform any illegal activity in this penetration testing, and shall not disrupt NRC's computing resources or destroy NRC's digital assets. The Contractor shall document its findings from the penetration testing in reports

to be delivered quarterly to the NRC in both hardcopy and softcopy. In addition, the Contractor shall make available to the NRC a representative to discuss the reports and present an overview of the techniques, technologies, and methodologies used to test the NRC's security.

The process of the Contractor identifying security gaps, and an NRC team addressing them, will result in constantly improving NRC's security. Testing, analysis, and reporting shall take place over a quarterly cycle, be performed remotely and/or locally, and be transparent to NRC.

The Contractor's quarterly report shall include detailed information on each NRC security gap that is identified: NRC's business risk, technical details, a CVE reference for additional information (if there is a CVE reference), and recommended remediation steps for NRC to take to correct the vulnerability. In addition, the Contractor's report shall include an executive summary overview, an NRC risk overview, a listing of all the NRC hosts that are visible to external hackers, or vulnerable to internal hackers, other network security anomalies, and an explanation of the vulnerabilities tested.

The Contractor shall assist the Government in the development of a formal policy specification for the security relevant aspects of the NRC network infrastructure and information architecture topology. The generation of this policy definition document (PDD) by the Government provides for a formalization of the legacy application business practices, the actual security policies, and the necessary network accesses to permit verification that the network behaves according to set security policy.. This PDD is input to an appropriate security audit application and will also allow NCR to represent the baseline information architecture logical map for applications that traverse the monitored network.

A. Testing

Multiple Testing Tools – The Contractor shall use a variety of testing tools, manual and automatic, including proprietary and modified open source, to attempt to penetrate NRC systems. In order to conduct the situational awareness testing, the Contractor shall procure, lease, or borrow, the commercially available tools needed to complete that testing. The NRC requires that the penetration test specifically include (at a minimum), checking for the top 20 vulnerabilities listed in the most recent SANS/FBI vulnerability listing. For example:

- 6
1. For network enumeration, port scanning, and OS fingerprinting: dnswalk, firewalk, hping2, and netcat.
 2. For initial and follow-up scanning - with adjustment of parameters: Arirang, ESS, Nessus, Saint, and Whisker.
 3. For follow-up scanning - selection varied depending upon the network being tested: authforce, cgichk.pl, cum, dctest, DSniff, ftpcheck.pl, fts-rvscan, LDAP Miner, nemesis, nsat, rascan, relaychk.pl, scanssh, sniffit, snmpscan, snmpwalk, strobe, and vetescan.

Continuous and Random Testing – The Contractor shall test the two NRC web sites and the LAN/WAN infrastructure numerous random times throughout each quarterly testing cycle: different times of day, days/nights, weekdays/weekends, and holidays. (Internal testing of the NRC network infrastructure must be coordinated by the Government project officer). Real world events or other network priorities may result in the internal testing being deferred.

Transparent and Peak Period Testing – The Contractor shall not write to or modify any of NRC's files or reduce response time.

Situational Awareness Testing - The contractor shall make use of commercially available security tools that will provide a capability to audit the NRC's network security policies and provide a secure real-time view and measurement of compliance data. The tools should provide the capability to perform periodic monitoring and measurement of network traffic compliance with NRC network security policies, with near real time notification of anomalies and deviations to the policies. This will provide real-time situational awareness into the overall security posture of the NRC network infrastructure.

B. Testing Schedule

1. Testing/Reporting Cycle – Day 1 - Contractor begins the first quarterly testing/reporting cycle for the NRC.

2. Testing/Reporting Cycle – Day 2 to Day 91 – For the external web sites, the Contractor conducts at least one testing cycle consisting of the following steps: penetration testing with many testing tools, analysis and cross-analysis of the findings, additional manual testing, verification of the findings, and then adjustment and refining of the testing parameters. For the internal NRC network infrastructure situational awareness testing, as coordinated by the Government project officer, the Contractor shall conduct a detailed network traffic analysis providing visibility into network operations and potential security threats. The analysis will provide a measurement of conformance to NRC network security policies. The internal network monitoring and testing can only be accomplished after the Government has developed, (or re-validated), the network security policy definition document (PDD). The contractor will provide technical

assistance to the Government project officer in the initial development of the PDD, and subsequent updates or (quarterly) re-validation of the PDD. When the internal network situational awareness testing is accomplished, the contractor will provide a secure real-time view of the network security compliance status utilizing commercially available security tools. The contractor shall deliver an NRC Internal Network Security Situational Awareness Test Report each time the testing is accomplished. (Expect a minimum of at least one report for this delivery order.)

3. Testing/Reporting Cycle – Day 92 – The Contractor delivers (within 5 calendar days of end-of-cycle testing) to the NRC an Independent Computer Security Testing Report for each of the NRC sites tested. If internal network testing is conducted, a summary of the results will be included in the report.

4. Testing/Reporting Cycle – Day 92 – Contractor begins the next quarterly testing/reporting cycle.

5. Testing/Reporting Cycle – Day 95 (to be scheduled by NRC and Contractor) – After completion of first quarterly report, if desired by the NRC, Contractor and NRC will meet at NRC to completely review the deliverable and process in detail, to be sure that any questions and issues are answered and resolved.

6 Testing/Reporting Cycle – Repeat steps 1 to 5 each quarter for twelve months. Note: each quarter's testing/reporting cycle's schedule will vary slightly based on when holidays and weekends fall in a particular quarter.

C. Reporting

Secure Delivery – The Contractor shall not post NRC's quarterly report on a web site or send it via e-mail. NRC's reports shall be sent in hard copy (with accompanying softcopy disks) within the stated 5 calendar days.

Concise - Each report shall document the test results. The report shall:

- ▶ Include NRC's security successes and security gaps,
- ▶ Explain how the testing was performed,
- ▶ Provide detailed explanations of each NRC security gap, including the: business risk, technical details, CVE reference (if applicable), and recommended remediation.
- ▶ Rate each NRC security gap's risk level,
- ▶ List each of the NRC machines that are visible to hackers, and
- ▶ Document each of the potential vulnerabilities tested.

Discussion With Experts - Representatives of the Contractor's Information Assurance and testing teams shall be available (at NRC's option) for a one hour telephone conversation to conduct a comprehensive review and discussion of each NRC report.

Table of Deliverables and Schedule of Delivery

Deliverables and due dates are summarized in the table below. Deliverable due dates are based on workdays.

Item	Deliverable Description	Deliverable Due Date
1	Kick-Off Meeting	5 workdays after award (project start, PS) or earlier
2	NRC Web Site Security Test Report	Quarterly; 10 th day of each quarter.
3	NRC Internal Network Security Situational Awareness Test Report; (Expect a minimum of at least one report for this delivery order)	5 days after tasked by Government Project Officer, (or as directed by the Government Project Officer);

Instructions for Deliverables

Deliverables shall be delivered on the dates specified in the order and be consistent with the deliverables schedules as shown in this statement of work. If for any reason a deliverable cannot be delivered within the scheduled time frame, the Contractor shall notify the Agency Project Officer in writing with cause of delay and the proposed revised schedule. This notice shall include the impact on the overall project. The Agency Project Officer shall make a business decision about the impact of the delay and forward the impact to the Contracting Officer.

Each deliverable shall first be submitted in draft for NRC review. NRC shall have 5 working days to review each draft deliverable and respond with comments or approval. Upon approval by NRC of the original draft or the corrected draft, the deliverable shall be delivered in final form to the NRC Project Officer and NRC Contracting Officer. For each deliverable (draft or final), the Contractor shall provide one (1) hard copy and one (1) electronic version of the deliverable to the NRC Project Manager, unless otherwise indicated. All deliverables shall be

formatted and prepared using Corel WordPerfect software for the documentation and reports, and Microsoft Powerpoint for the briefings. All written deliverables shall be phrased in language that can be understood by the non-technical layperson. Statistical and other technical terms used in the deliverable shall be defined in a glossary.

V. Period of Performance

The period of performance for this delivery order will be for twelve months, starting from the date of award, and shall have two, 1 year renewal options. The NRC will provide funding as a firm fixed-rate contract. NRC and the Contractor agree to keep confidential the results of the testing and all reports relating to the testing.

VI. Information Handling and Ownership

The products and information associated with, or generated from, this project are considered sensitive information and property of the Nuclear Regulatory Commission and shall NOT be distributed, copied, transmitted, or by any other method, disclosed to the public or any individual without the express written permission of the NRC. Data appropriate for Incident Reporting will be controlled by the OCIO in conjunction with the Emergency Operations Center.

VII. SECURITY

(a) Security/Classification Requirements Form. The attached NRC Form 187 (Attachment 1) 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 delivery order 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 delivery order 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 delivery order 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.

SITE ACCESS BADGE REQUIREMENTS

During the life of this contract, the rights of ingress and egress for contractor personnel must be made available, as required, provided that a badge is issued after favorable adjudication from the Personnel Security Branch, Division of Facilities and Security (PERSEC/DFS). In this regard, all contractor personnel whose duties under this delivery order require their presence on-site shall be

clearly identifiable by a distinctive badge furnished by the Government. The Project Officer shall assist the contractor in obtaining the badges for the contractor personnel. It is the sole responsibility of the contractor to ensure that each employee has a proper Government-issued identification/badge at all times. All prescribed identification must be immediately (no later than three days) delivered to PERSEC/DFS for cancellation or disposition upon the termination of employment of any contractor personnel. Contractor personnel must have this identification in their possession during on-site performance under this contract. It is the contractor's duty to assure that contractor personnel enter only those work areas necessary for performance of delivery order work, and to assure the safeguarding of any Government records or data that contractor personnel may come into contact with.

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 delivery order 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 delivery order 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 delivery order 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 delivery order 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 delivery order 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 delivery order 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 (enclosed), 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

15

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.

The Contractor shall not post NRC's monthly report on a web site or send it via e-mail. The products and information associated with or generated from this project are considered sensitive information and property of the Nuclear Regulatory Commission and shall NOT be distributed, copied, transmitted, or by any other method, disclosed to the public or any individual without the express written permission of the NRC Office of the Chief Information Officer..

VIII. FOIA EXEMPTION STATUS

Penetration tests of NRC systems will contain sensitive information about computer network vulnerabilities, NRC critical infrastructure and infrastructure protection, cyber security problems, solutions, test practices and test results, and is to be shielded from public disclosure under the provisions described in the Cyber Security Information Act, HR 4246. This contract is expected meet the criteria set forth in the Cyber Security Information Act, Cyber Security Statement as follows:

- I. Concerns the assessment, projection, or estimate concerning the cyber security of various entities throughout NRC, NRC computer systems, NRC software programs, or similar facilities of its own;
- II. Concerns plans, objectives, or timetables for implementing or verifying the cyber security thereof;
- III. Concerning test plans, test dates, test results, or operational problems or solutions related to the cyber security thereof;
- IV. Includes reviews, comments on, or otherwise directly or indirectly relating to the cyber security thereof.

IX. CONFIDENTIALITY AND NONDISCLOSURE

It is agreed that:

1. The preliminary and final deliverables and all associated working papers, application source code, and other material deemed relevant by NRC which have been generated by the contractor in the performance of this task order are the exclusive property of the U.S. Government and shall be submitted to the Contracting Officer at the conclusion of the task order.

2. The Contracting Officer will be the sole authorized official to release verbally or in writing, any data, the draft deliverables, the final deliverables, or any other written or printed materials pertaining to this task order. The contractor shall release no information. Any request for information relating to this task order presented to the contractor shall be submitted to the Contracting Officer for response.

3. Press releases, marketing material or any other printed or electronic documentation related to this project, shall not be publicized without the written approval of the Contracting Officer.