

**NATIONAL O.R.E. MANAGEMENT & MARKETING SERVICES**

**BASIC ORDERING AGREEMENT**

BOA  
Version 3.6  
July 2004

## TABLE OF CONTENTS

	<u>Page</u>
ARTICLE I. APPOINTMENT AND DUTIES OF CONTRACTOR; TASK ORDERS	1
1.1 Independent Contractor	1
1.2 Duties	1
1.3 Task Order	2
1.4 Standard of Performance	2
1.5 Calendar Days	3
1.6 Monthly Report	3
ARTICLE II. PERIOD OF PERFORMANCE	3
2.1 Initial Period of Performance	3
2.2 Option Period	3
2.3 Notice of Exercise of Option	4
ARTICLE III. SECURITY AND CONFIDENTIALITY REQUIREMENTS	4
3.1 Background Investigations	4
3.2 Risk Level Designation	5
3.3 Confidentiality of Information, Data, and Systems	5
3.4 Security Requirements for Information Technology.	5
3.5 IT Security Plan	6
3.6 Training Requirements	7
3.7 Security Awareness Website Training	8
3.8 General Requirements	8
3.9 FDIC Access	8
3.10 Subcontractor Requirements	9
ARTICLE IV. PERSONNEL AND SUBCONTRACTING	9
4.1 Key Personnel	9
4.2 FDIC Personnel.	9
4.3 Contractor Personnel	10
4.4 Personnel Qualifications.	10
4.5 Subcontractors	10
4.5.1 Authorization; Selection of Subcontractors.	10
4.5.2 Contracts with Subcontractors	11
4.6 Subcontracting Plan Compliance	11
ARTICLE V. COMPENSATION AND BILLING	12
5.1 (a) Fixed Price	12
5.1 (b) Labor Rates	12
5.1.1 Compensation Ceiling	12
5.1.2 Other Reimbursable Expenses	12
5.1.3 Travel Expenses	13
5.1.4 Fees and Expenses of Subcontractors	13
5.2 Billing Instructions	13
5.2.1 General Provisions	13

5.2.2	Contractor's Remittance Address	14
5.2.3	Schedule for Invoicing	14
5.2.5	Certification of Contractor	14
5.2.6	FDIC Review	14
5.3	Method of Payment-EFT	15
ARTICLE VI.	INSPECTION AND ACCEPTANCE	15
6.1	Inspection and Acceptance of Work Product	15
6.2	Risk of Loss or Damage	15
ARTICLE VII.	RIGHTS IN SOFTWARE AND SYSTEMS	15
7.1	Proprietary Interest and License in Software and Systems	15
ARTICLE VIII.	REPRESENTATIONS	15
8.1	Representations of Contractor	15
ARTICLE IX.	RESERVED	16
ARTICLE X.	INSURANCE COVERAGE	16
10.1	Liability Insurance	16
10.2	Fidelity Bond Coverage	17
10.3	Errors and Omissions Insurance	17
10.4	Certificates of Insurance	18
10.5	Notice to the FDIC	18
10.6	Cost of Insurance	18
ARTICLE XI.	INDEMNITY	18
11.1	Contractor Indemnity	18
ARTICLE XII.	CONFLICT OF INTEREST	19
12.1	Notice to the FDIC	19
ARTICLE XIII.	LEGAL REPRESENTATION	19
13.1	Relationship of Contractor and FDIC Legal Division	19
13.2	Contact Points	19
13.3	Contractor's Authority	19

## BASIC ORDERING AGREEMENT NUMBER

Agreement executed on \_\_\_\_\_, 2008 ("Execution Date") and effective as of November 14, 2008 ("Effective Date") between the FEDERAL DEPOSIT INSURANCE CORPORATION, acting as receiver for various institutions and acting in its corporate capacity ("FDIC"), and PRESCIENT, INCORPORATED, a corporation organized and existing under the laws of Florida with its principal place of business at 2100 Coral Way, #504, Miami, FL 33145 ("Contractor").

WITNESSETH:

The FDIC, as receiver for various institutions (the "Institutions") and in its corporate capacity, desires to retain Contractor, and Contractor desires to perform the services or provide the goods described in this Basic Ordering Agreement ("Agreement") and in any Task Order ("Task Order") issued hereunder, upon the terms and conditions set forth below.

Now, therefore, in consideration of the mutual covenants and agreements set forth below, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by the parties, the FDIC and Contractor agree as follows:

### ARTICLE I. APPOINTMENT AND DUTIES OF CONTRACTOR; TASK ORDERS

#### 1.1 Independent Contractor

The FDIC and Contractor agree to be bound by the terms and conditions of this Agreement when a Task Order is executed for a specific task. The FDIC hereby retains Contractor as an independent contractor for the sole purpose of performing the services or providing the goods described herein and in the Task Orders awarded to Contractor.

#### 1.2 Duties

Contractor hereby agrees to perform such services (the "Services") or provide such goods (the "Goods") on the terms and conditions set forth below, in the particular Task Order, in the Statement of Work (Attachment [1] to this Agreement), and in Contractor's Proposal or Amended Proposal, if any (Attachment [2] to this Agreement), all of which are incorporated herein by reference. Attachment [3], entitled FDIC General Provisions, is also hereby incorporated into and made a part of this Agreement.

Contractor is required to notify the FDIC Contracting Officer and Oversight Manager in writing of any change in Contractor's physical location for the Place of Performance of this Contract. This includes without limitation any facilities relocation and/or re-construction activity or any other planned event that may impact the continued operation of FDIC-owned network equipment

located on the Contractor's premises. The notification must be made at least thirty days in advance of the planned change or start date for any such activity to allow the FDIC time to take appropriate action.

Contractor must ensure that all connections and access to the FDIC network and systems are removed and no longer active using appropriate security procedures at the time of expiration or termination of this Agreement and any Task Order issued hereunder, whether contractor or subcontractor employees are working on-site or off-site, and notice must be provided to the Oversight Manager upon completion of these requirements. Contractor must also undergo the FDIC pre-exit clearance procedures at the time of separation from this Agreement or any Task Order.

### 1.3 Task Order

At any time during the Period of Performance (as defined in Article II below), the FDIC Contracting Officer may send to Contractor, and any other Contractors awarded this Agreement, a Request for Task Order Proposal (the "Request") describing the nature of one or more specific tasks, the structure for Contractor's offer and any other information relating to the task. When selecting one of the contractors for a specific task order award, the FDIC will issue a Task Order for services. Before issuing a task order the FDIC will consider a variety of factors including specifics of the portfolio of assets subject to the Task Order, their origin, relationship to other assets, and unique needs, contract pricing, past performance and other factors. The Contractor waives all rights to challenge or protest the selection of a contractor to provide contingency contract services and the FDIC makes no guarantee for services under the agreement except as provided on each task order.

If Contractor wishes to offer its goods or services for the task, it must deliver an offer pursuant to the terms of the Request. Based on the offers received, the FDIC may select one or more contractors to perform these specific tasks. If Contractor is selected, the Task Order must be executed by Contractor and the FDIC Contracting Officer and there will exist a binding obligation between Contractor and the FDIC pursuant to the terms of this Agreement, and the Task Order, regarding the goods or services. The FDIC and Contractor agree that the form of the Task Order, an example of which is set forth as Attachment [4] to this Agreement, may change during the period of performance of this Agreement.

### 1.4 Standard of Performance

Contractor must at all times act in good faith and in the best interests of the FDIC, use its best efforts and exercise all due care and sound business judgment in performing its duties under this Agreement. Contractor must at all times comply with FDIC policies, procedures and directives, which are incorporated by reference and made part of this contract.

### 1.5 Calendar Days

Unless specifically provided otherwise in this Agreement, the term "days" used anywhere in this Agreement means calendar days.

### 1.6 Monthly Report

If subcontracting or joint venturing is approved, Contractor must submit to the Contracting Officer a Subcontractor/Joint Venture/Team Arrangement Activity Report, on a monthly basis, addressing for each subcontractor and/or Joint Venture participant(s), the following:

- a. Name, address, tax identification number and type of business concern [Minority Women Owned Business, Small Disadvantaged Business and applicable Standard Industrial Classification (SIC) Code and corresponding geographic location if applicable] for each subcontractor and/or Joint Venture participants.
- b. Period covered by the Report.
- c. Description of work performed by subcontractor and/or Joint Venture participants during the report period.
- d. Percentage of services planned and actually provided by subcontractor and/or Joint Venture participants during the report period and cumulative to date by SIC code if applicable.
- e. Total compensation paid to subcontractor and/or Joint Venture participants during the report period and cumulative to date.
- f. Percentage completion toward Subcontracting Plan goals and/or Joint Venture commitments.

## **ARTICLE II. PERIOD OF PERFORMANCE**

### 2.1 Initial Period of Performance

This Agreement has a three (3) year initial period of performance starting on the Effective Date and expiring on November 13<sup>th</sup>, 2011 (the "Period of Performance") subject to exercise of an option, if applicable, or to earlier termination under the General Provisions of this Agreement.

### 2.2 Option Period

This Agreement may be extended, at the discretion of the FDIC, for up to three (3) 2-year period(s) (an "Option Period"). Except where specifically indicated otherwise, "Period of Performance" as used hereafter in this Agreement refers both to the initial Period of Performance and to any Option Period which may be exercised.

### 2.3 Notice of Exercise of Option

If the FDIC desires to exercise the option to extend the Period of Performance, the FDIC must notify Contractor, in writing, of its intent not less than sixty (60) days before the expiration of the initial Period of Performance.

## ARTICLE III. SECURITY AND CONFIDENTIALITY REQUIREMENTS

### 3.1 Background Investigations

- 3.1.1 Background investigations will be conducted for all contractor and subcontractor personnel. The extent of the investigations will be in direct relation to the risk level assigned to the contract or to the individual job classifications, which can be found in Section 3.2 of this contract. No background investigations or fingerprinting will be required under receiverships except when a receivership is of a long-term nature, when both are required.]
- 3.1.2 Each contractor and subcontractor employee working on the contract must complete an electronic fingerprint application and credit report authorization. No employee will be permitted to begin work (including access to FDIC facilities, network, and systems) until a favorable fingerprint records check and credit report has been received by the FDIC, unless a waiver has been obtained.
- 3.1.3 Within 5 days after the effective date hereof, the contractor must provide the Contracting Officer with a list of all contractor and subcontractor personnel working on the contract. This list must include the employee's name, current home address, and assigned risk level. The contractor must identify each employee who has a previous current or otherwise valid background investigation, and such background investigations must be furnished to FDIC with the list of personnel.

For those employees of the contractor or subcontractor who do not have a valid and current background investigation, a background investigation will be conducted for them. In that event, the requirements relating to background investigations contained herein will control.

NOTE: A valid background investigation is one that meets the minimum investigation for the risk level established for the contract or contract job category, and that has been conducted within 5 years of the date of contract award.

- 3.1.4 An adverse finding during the background investigation or fingerprinting review (e.g., felony conviction), or a completed background investigation or fingerprint

check that indicates that the employee cannot meet the designated security requirements, may prohibit a contractor or subcontractor employee from working on the contract. That employee may be removed at the discretion of the Contracting Officer and replaced with an employee acceptable to FDIC by the Contractor at no additional expense to FDIC and without relief in all contractual performance and delivery requirements.

- 3.1.5 All contractor and subcontractor employees regularly working on-site at an FDIC facility will be issued a yellow identification/access control badge. Such employees will not be granted on-site access until FDIC receives a favorable fingerprint criminal records check from the FBI. The badges will be issued for a six-month period and must be renewed after each six-month period.
- 3.1.6 Contractor must notify the Contracting Officer of any new contractor or subcontractor personnel assigned to the contract or any change in assignment of current personnel. FDIC will perform the appropriate background investigations and fingerprint check for any such personnel. Access to FDIC facilities, network, and systems will be as set forth in this section 3.1.

### 3.2 Risk Level Designation

The following risk level has been assigned to this contract: MODERATE. The post-award background investigations and fingerprinting required for all contractor employees (and subcontractor employees, if applicable) will be for this risk level.

### 3.3 Confidentiality of Information, Data, and Systems

Contractor must ensure the confidentiality of all information, data, and systems provided by FDIC or used or obtained by Contractor personnel under this contract and prevent its inappropriate or unauthorized use or disclosure. Contractor and all employees working on an FDIC contract must sign the Contractor Confidentiality Agreement (attached) no later than five (5) business days after starting performance and prior to receiving such information, or when receiving their badges, and return the signed Agreements to the Contracting Officer. This includes Contractor personnel who are required to work on-site at an FDIC facility or have access to FDIC sensitive information or data, systems or network. Failure to provide the signed Agreements may result in the removal of the employee from performing under the contract.

### 3.4 Security Requirements for Information Technology.

The Contractor is responsible for Information Technology (IT) security for all personnel with access to the FDIC network, systems connected to the FDIC network or those systems developed and/or operated by the Contractor for FDIC. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor may have physical or electronic access to FDIC's information contained in its systems. This includes but is not limited to information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer

systems, networks, and telecommunications systems. Examples of tasks that require security provisions include but are not limited to acquisition, transmission or analysis of data owned by FDIC or access to FDIC networks or computers at a level beyond that granted the general public, e.g., bypassing the FDIC firewall.

Contractor, its subcontractors, and the employees of each must sign a confidentiality agreement at any time prior to or during the performance of this contract at the direction and discretion of the Contracting Officer.

### 3.5 IT Security Plan

The Contractor must provide as a deliverable, implement, and maintain an IT Security Plan ("Plan") for the duration of this contract. This Plan must describe the processes, procedures and training of personnel that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The Plan must describe those parts of the contract to which this clause applies. It must address the security measures and program safeguards that will be provided by the Contractor. These measures and safeguards must ensure that all information systems, data, and resources acquired and utilized in the performance of this contract by the Contractor personnel:

- a. Are protected from unauthorized access, alteration, disclosure, or misuse of processed, stored, or transmitted information;
- b. Can maintain the continuity of IT support for the FDIC and its programs and operations;
- c. Incorporate management, operational, and technical controls sufficient to provide cost-effective assurance of the system's integrity, availability and confidentiality;
- d. Have appropriate technical, personnel, administrative, environmental, and access safeguards; and
- e. Operate effectively and accurately.

#### 3.5.1 Compliance Requirements

The Contractor's Plan must be compliant with Federal laws that include, but are not limited to, OMB Circular A-130, Transmittal 4, Management of Federal Information Resources, Appendix III and the Federal Information Security Management Act of 2002 (Title 3 of P.L. 107-347). In addition, the Plan must implement IT security requirements stated in the policies and procedures that include, but are not limited to:

- a. FDIC, Division of Information Resources Management (DIRM) Policy Memorandum (PM) No. 98-009, Security of Network Connectivity for Contractor Support, dated September 22, 1998;
- b. FDIC, Division of Information Resources Management (DIRM) Policy Memorandum (PM) No. 98-010S, Personal Computer Information Security, November 1998;
- c. FDIC Circular 1310.5, Encryption and Digital Signature for Electronic Mail;

- d. FDIC, Division of Information Resources Management (DIRM) Circular No. 1360.15, Access Control for Automated Information Systems;
- e. FDIC, Division of Information Resources Management (DIRM) Circular No. 1360.16, Mandatory Information Security Awareness Training;
- f. FDIC, Division of Information Resources Management (DIRM) Circular No. 1360.17, Information Technology Security Guidance for FDIC Information Technology Procurements/Third Party Products;
- g. FDIC, Division of Administration (DOA) Circular No. 1610.2, Security Policies and Procedures for Contractors, October 1, 2001;
- h. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-4, Security Considerations in Federal Information Technology Procurements;
- i. NIST, SP 800-14, Generally Accepted Principles and Practices in Securing IT Systems, September, 1996; and
- j. NIST, SP 800-18, Guide for Developing Security Plans for Information Technology Systems, December 1998.

These documents may be accessed through the FDIC DOA website, [www.fdic.gov/](http://www.fdic.gov/), and may be cross-referenced through the FDIC DIRM website, [www.fdic.gov/](http://www.fdic.gov/).

### 3.5.2 Plan Submissions

Within ten (10) days after contract award, the Contractor must submit the Plan for FDIC approval. The Plan must be consistent with and further detail the general outline and approach contained in their proposal that resulted in the award of this contract and must be in compliance with the requirements stated in this Article. The Plan must be submitted to the Contracting Officer and, after approval by the Oversight Manager, will be incorporated into the contract as a requirement and will remain in effect throughout the period of contract performance. The Contractor must obtain the prior written approval of the Contracting Officer for any changes to the Plan.

### 3.6 Training Requirements

The Contractor must ensure that its personnel designing, programming, operating, using, or managing FDIC systems/network and/or data in performance of the contract, are properly trained and must receive training at least annually in IT security awareness and security practices, policies, and procedures as required under the Computer Security Act of 1987 and OMB Circular A-130, including Appendix III. The Contractor's approach and IT security training program must be defined in the IT Security Plan. In addition, the Contractor must ensure that IT security training also meets the requirements stated in the NIST special publications and in the FDIC circulars referenced in this Article. The Contractor must certify on an annual basis that its personnel working on the contract have successfully completed all required IT security training and that they are aware of their IT security responsibilities.

### 3.7 Security Awareness Website Training

3.7.1 All contractor and subcontractor employees being granted access to FDIC's network/systems must review the FDIC Security Awareness Website (located at [http://fdic01/division/dirm/itm\\_web/dirm\\_pages/infosec/secawareness/secawareness.htm](http://fdic01/division/dirm/itm_web/dirm_pages/infosec/secawareness/secawareness.htm)) and provide electronic certification of their review within five (5) business days of receiving a network ID.

3.7.2 In addition to 3.7.1, for multi-year contracts and contracts with options, all contractor employees with network access must again review the Security Awareness Website on an annual basis and provide electronic certification of their review within five (5) business days after the anniversary of the effective date of the contract.

3.7.3 The contractor must certify annually that all contractor employees having network access have complied with the security requirements stated in 3.7.1 and 3.7.2. This certification must be provided to the Oversight Manager by email or in writing within five (5) business days after the anniversary of the effective date of the contract.

3.7.4 Failure to complete the review and certification discussed in 3.7.1, 3.7.2, and 3.7.3 may result in revocation of network access privileges and possible removal of the individual employees from the contract.

### 3.8 General Requirements

#### 3.8.1 Network Access Requirements

The Contractor must comply with all provisions of FDIC Circular 1360.17, Information Technology Security Guidance for FDIC Information Technology Procurements/Third Party Products, which can be found on FDIC's website at [www.fdic.gov](http://www.fdic.gov).

#### 3.8.2 Cost of Information Security

For all contracts valued at \$3 million or more, the Contractor must identify on its invoices as a separate line item any direct cost to the contractor for information security as a specific element of the cost of providing information services.

### 3.9 FDIC Access

The Contractor must afford FDIC, including the Office of Inspector General, access to the Contractor's and all subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access must 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 FDIC data, systems,

