INFORMATION SECURITY CONTRACT CLAUSES

December 11, 2006

INTRODUCTION

As a federal agency, the Corporation for National and Community Service (CNCS) is subject to and complies with the requirements of the Federal Information Security Management Act (FISMA). FISMA requires that CNCS provide appropriate and adequate protection for its Information Technology (IT) systems and associated assets: hardware, software, and data. As a provider of IT services and/or products, CNCS contractors shall ensure that the services and products they provide are in compliance with FISMA, as defined in the CNCS Information Security Policy and with the security requirements contained herein.

1. Use Of Government Computers

1.1 CNCS rules regarding security of information technology (IT) systems and associated assets (hardware, software, data) apply to all personnel (employees, contractors, consultants) with access to that equipment or data. The rules are described in the following paragraphs:

1.1.1 The CNCS IT Security Program is defined in Corporation policy CIO-2006-001; Information Security Program / Policy which is available on its public websites.

1.1.2 In performance of the contract, it is the contractor's responsibility to ensure that all of their personnel are familiar with CNCS computer and information systems security policies, standards, and procedures and that they abide by the CNCS Rules of Behavior, applicable to the applications and/or systems to which they have been authorized access.

1.1.3 The contractor and its employees and subcontractors shall not install any personal or company-owned software or applications on Government-owned equipment without the express permission of the COTR. Use of unnecessary user applications (e.g., personal use of external instant messaging, desktop search engine, peer-to-peer file sharing services), and services that are not needed or duplicate the Government-provided equivalents (e .g., alternate e-mail services) is prohibited.

1.1.4 If employees of the contractor or any of its subcontractors are given user accounts in CNCS email systems, the Contractor will ensure that they have been correctly identified in the email system as contractors and have included the name of their company in the directory and in an automatic signature line, so that any email correspondence is readily recognized as coming from a contractor rather than a CNCS employee.

2. Contractor Personnel Clearance and Identity Credentials

2.1 CNCS rules regarding physical security and personnel security apply to all personnel in CNCS facilities.

2.2 Each contractor (or subcontractor) employee requiring recurring access to CNCS facilities and/or information systems will be required to submit to a background investigation. The type of background investigation required is based on the individual's assigned position's risk/sensitivity level designation, as described in the Statement of Work. For most positions, this background investigation is required to obtain a CNCS-issued identification credential (badge). This requirement does not apply if the contractor does not have any unsupervised IT system access and will only need building access for less than 6 months or only occasional building access (such as for periodic equipment maintenance). In those cases, building procedures for visitors will be applied.

2.3 One week before starting work, the contractor will provide a listing to the COTR, identifying contractor and subcontractor employees requiring access to CNCS facilities or systems for performance of work under this task/contract.

2.4 The contractor employees are required to complete the applicable background investigation request forms provided by the COTR. The following forms, or their equivalent may be used to initiate the credentialing process: SF 85 or SF 85-P (which includes authorization for credit check and fingerprint cards). The completed forms shall be provided to the COTR within 7 days after the individual's start date on this task/contract. The contractor employee may be allowed temporary, supervised access up to 30 days without completing this application process if a justified reason for delay is provided. An employee's refusal to provide or authorize provision of information may constitute grounds for denial or revocation of credentials. Government personnel may contact the contractor/subcontractor employee being screened or investigated in person, by telephone or in writing, and the contractor agrees to make them available for such contact. If a contractor employee already holds a credential issued by a federal agency after background screening through OPM, the contractor may provide documentation supporting this status to the COTR. CNCS security officials will determine if the existing clearance can be accepted without further investigation.

2.5 Badges/credentials issued upon satisfactory completion of a preliminary National Agency Check (NAC) may be revoked if the subsequent NAC with Inquiries (NACI) investigation produces an unfavorable determination. Individuals who do not pass the background investigation cannot be permitted to hold a building pass, allowed entry into the building for contract work, or permitted access to CNCS systems (whether remote or on-site). In such cases, the Contractor will be required to sign (or have their subcontractor sign) a notification form indicating that their employee has been informed of the results of the background check. The Government is the final authority in determining access privileges. The Government's exercise of its right to

grant and revoke " the access of particular individual(s) to its facilities, systems, or parts thereof shall not constitute a breach or change to the Contract, regardless of its impact on any individual's ability to perform work under the Contract.

2.6 During all operations on Government premises, contractor personnel shall comply with the rules and regulations governing the conduct of personnel and the operation of the facility. Government-issued identity credentials must be worn upon entry and displayed at all times while on federally controlled property, unless otherwise instructed by the COTR.

2.7 The Government reserves the right to require a re-submission of clearance forms and a new background investigation at any time. Failure to provide the documents within the specified time period will result in removal of the employee until such time that the documents are submitted and clearance granted. Should removal be necessary, salary/wages and other costs associated with the removed employee are not allowable or allocable under this contract. If removal would result in understaffing or non-performance of contract requirements, the Contractor shall provide a qualified and cleared replacement. Failure to do so will entitle to Government to a downward adjustment in price reflecting the reduced level of performance.

2.8 When any of their personnel leaves the company's employ, is reassigned to other work, or otherwise no longer requires access to CNCS facilities or CNCS computer systems, the contractor shall immediately advise the CNCS COTR so that those user accounts and credentials can be cancelled. The contractor will ensure that the ID badge and facility access keys (if any) are retrieved and promptly returned to the COTR. The COTR must be notified in advance of any potentially unfriendly termination of an employee; or subcontractor.

2.9 The contractor will report any lost keys or badges to the COTR within 24 hours. The COTR will relay the information to the responsible building security officials. All badges and keys shall be returned to the COTR at the completion of this contract.

2.10 The requirements of this clause must be included in any subcontracts in which subcontract workers will need building or unsupervised system access.

3. Access to Government facilities

   During the life of the contract, the rights of ingress and egress to and from the Government facility for service technicians shall be made available as required. During all operations on Government premises, service technicians shall comply with the rules and regulations governing the conduct of personnel and the operation of the facility. The Government reserves the right to require service technicians to display photographic identification card (such as driver's license) and sign in upon ingress to and sign out upon egress from the Government facility.

4. Availability of IT Security Standards, Guides, and Other Publications

   The documents relating to Information Technology (IT) security are located at websites operated by NIST and CNCS. The IT security guidance located at those websites are incorporated by reference into each CNCS task/contract as appropriate. The following are the urls for the security guidance documents:

   - NIST Special publications: http://csrc.nist.gov/publications/nistpubs/
   - Federal Information Processing Standards: http://csrc.nist.gov/publications/fips/
   - CNCS information security policies and procedures: http://www.cns.gov/home/infosec_policy.

5. Confidentiality, Privacy and Sensitive Information

5.1 To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies and/or CNCS internal planning or procurement sensitive source selection data, which, if released to third parties may give unfair business, technical, or competitive advantages. As long as such data remains propriety or confidential, the contractor shall protect such data from unauthorized use and disclosure and agrees not to use it to compete with such companies or for any purpose other than performance of this contract.

5.2 This data may be in various forms, such as documents, raw photographic films, magnetic or digital media, photographic prints, computer system data, or it may be interpretative results derived from analysis, investigative, or study effort. Regardless of the form of this data, the contractor agrees that neither it nor any of its employees will disclose to third parties any such data, or derivatives thereof, except as may be required in the performance of this contract. Further, the contractor will not copy any of this data, or derivatives thereof, other than as necessary for the performance of this contract.

5.3 The contractor will establish policies and procedures to implement the substance of this clause at the individual employee level which will assure that affected employees made aware of the contract provision and the contractor's implementing policies and procedures. Particular attention will be given to keeping employees advised of statutes and regulations applicable to the handling of Privacy Act, third party confidential or financial data.

5.4 Prior to receiving access to CNCS computers, contractor employees shall be required to sign non-disclosure, Rules of Behavior, or other system security agreements, depending on the systems to be used and level of access granted. The required non-disclosure agreement will be similar to the attached but may be customized, as needed, to reflect the data involved.

5.5 This clause does not preclude the contractor and/or its employees from independently acquiring and using data from legitimate sources outside of this contract, or from performing and using independent analysis of data so acquired, provided that the contractor and/or its employees fully document the source of such data, and the independence of any such analysis.

5.6 The Contractor shall immediately notify, in writing, the Contracting Officer in the event that the Contractor determines or has reason to suspect breach of this requirement.

5.7 The contractor will insert the substance of this clause in each subcontract hereunder (other than for purchase of supplies or equipment) unless the Contracting Officer has waived this requirement, in writing, as to particular subcontracts or classes of subcontracts.

5.8 Contractor employees shall complete CNCS-defined Information Systems Security Awareness course before being granted system access and must renew the training annually. Failure to complete training within the required timeframe may result in loss of system access for that user. The Contractor shall also provide Contract employees with significant IT security responsibilities appropriate specialized role-based security training. The Contractor shall provide a summary of such training provided to the COTR on a quarterly basis.

5.9 No portion of the services to be performed hereunder may be performed outside the United States without the express written permission of the Contracting Officer.

5.10 Any unauthorized disclosure of information may result in termination of this contract for cause.

5.11 To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

6. Special IT Security Provisions

6.1 Internet Logon Banner

Web-based applications developed or maintained under this contract must contain a CNCS approved logon banner.

6.2 Incident Reporting

Contractor employees must report any suspected computer security incidents (viruses, intrusion attempts, system compromises, offensive e-mail, information security policy violations, etc.) which may affect Government data, systems, and reports, or access to that data or systems. Contractors shall report computer security incidents to the CNCS help desk, information systems security officer (ISSO), or local system administrator. Contractor employees will support CNCS investigation and resolution of reported security incidents as required.

6.3 Malicious Code

The Contractor shall institute controls as appropriate to ensure that software products delivered are free from malicious code.

6.4 Confidentiality of Security Safeguards

The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.

6.5 Changes in Threats or Vulnerabilities

If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

7. Rights In Data-Special Works

(A) Definitions.

"Data," as used in this clause, means recorded information regardless of form or the medium on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing or management information.

"Unlimited rights," as used in this clause, means the right of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose whatsoever, and to have or permit others to do so.

(B) Allocation of Rights

(1) The Government shall have-

(i) Unlimited rights in all data delivered under this contract, and in all data first produced in the performance of this contract, except as provided in paragraph (c) of this clause for copyright.
(ii) The right to limit exercise of claim to copyright to data first produced in the performance of this contract, and to obtain assignment of copyright in such data, in accordance with subparagraph (C)(l) of this clause.
(iii) The right to limit the release and use of certain data in accordance with paragraph (d) of this clause.

(2) The Contractor shall have, to the extent permission is granted in accordance with subparagraph (C)(l) of this clause, this right to establish claim to copyright subsisting in data first produced in the performance of this contract.

(C) Copyright

(1) Data first produced in the performance of this contract.

(i)The Contractor agrees not to assert, establish, or authorize others to assert or establish, any claim to copyright subsisting in any data first produced in the performance of this contract without prior written permission of the Contracting Officer. When claim to copyright is made, the Contractor shall affix the appropriate copyright notice of 17 U.S.C. 401 or 402 and acknowledgment of Government ownership (including contract number) to such data when delivered to the Government, as well as when the data are published or deposited for registration as a published work in the U.S. Copyright Office. The Contractor grants to the Government and others acting on its behalf, a paid-up nonexclusive, irrevocable, worldwide license for all such data to reproduce, prepare derivative

works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.
(ii) If the Government desires to obtain copyright in data first produced in the performance of this contact and permission has not been granted as set forth in subdivision (C)(l)(i) of this clause, the Contracting Officer may direct the Contractor to establish, or authorize the establishment of, claim to copyright in such data and to assign, or obtain the assignment of, such copyright to the Government or its designated assignee.

(2) Data not first produced in the performance of this contract. The Contractor shall not, without prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract and which contain the copyright notice of 17 U.S.C. 401 or 402, unless the Contractor identifies such data and grants to the Government, or acquires on its behalf, a license of the same scope as set forth in subparagraph (C)(1)of this clause.

(D) Release and use restrictions. Except as otherwise specifically provided for in this contract, the Contractor shall not use for purposes other than the performance of this contract, nor shall the Contractor release, reproduce, distribute, or publish any data first produced in the performance of this contract, nor authorize others to do so, without written permission of the Contracting Officer.

(E) Indemnity. The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability, including costs and expenses, incurred as the result of the violation of trade secrets, copyrights, or right of privacy or publicity, arising out of the creation, delivery, publication, or use of any data furnished under this contract; or any libelous or other unlawful matter contained in such data. The provisions of this paragraph do not apply unless the Government provides notice to the Contractor as soon as practicable of any claim or suit, affords the Contractor opportunity under applicable laws, rules, or regulations to participate in the defense thereof, and obtains the Contractor's consent to the settlement of any suit or claim other than as required by final decree of a court of competent jurisdiction; nor do these provisions apply to material furnished to the Contractor by the Government and incorporated in data to which this clause applies.

CONTRACTOR EMPLOYEE NON-DISCLOSURE AGREEMENT

It is understood that as part of my official duties under Contract No. _____ I may come in contact with Government sensitive information (e.g., data subject to protection under the Privacy Act of 1974 as amended) or proprietary business information from other contractors (e.g., cost data), I certify that I will not disclose, publish, divulge, release, or make known, in any manner or to any extent, to any individual other than an appropriate or authorized Government employee, the content of any sensitive information provided during the course of my employment. I further certify that I will use sensitive information provided only for official purposes in the performance of Contract No. _____, and will disclose such information only to those individuals who have a specific need to know in performance of their official duties. I hereby agree not to disclose to others any sensitive information, including, but not limited to, proprietary information, trade secrets, and financial data, and technical proposals, pre-decisional data, information related to individuals which may be presented to me by a Government Official or which I may come into contact. I specifically will not disclose any sensitive information to employees of my company or any other contractor employees who have not signed this agreement. I will take all reasonable precautions to prevent the unauthorized disclosure and use of such information.

I hereby certify that I have read the non-disclosure agreement described above and I am familiar with the directives and policies governing the disclosure of procurement sensitive information. I will fully and completely observe these directives and will not disclose such information to any unauthorized person, or use any information obtained for private use or gain at any time, including subsequent to the performance of duties under Contract No. _____.

Name (Printed)	Signature	Date