CCR Account Application & Interconnection Security Agreement (ISA)

Between

Central Contracting Registration (CCR)

And

(Connecting Agency Name Here)

INSERT CONNECTING AGENCY'S LOGO HERE

TABLE OF CONTENTS

I. INTERCONNECTION STATEMENT OF REQUIREMENTS

_____ requires an interconnection with CCR for the express purpose of utilizing information contained in the CCR database. This Interconnection Security Agreement (ISA) specifies the security requirements for establishing, operating, and maintaining this interconnection. Guidance for this ISA was taken from National Institute of Standards and Technology (NIST) Special Publications 800-18 and 800-47.

The expected benefit of this interconnection is to (explain):

II. SYSTEM SECURITY CONSIDERATIONS

Data Sensitivity
The information transferred between CCR and _____ is Sensitive but Unclassified (SBU). The types of sensitive data being transmitted include:

FOUO/Non-Proprietary	Yes _____	No _____
Proprietary – Public and Tax information (TINs, SSNs, EINs)	Yes _____	No _____
Sensitive– Public, Proprietary and Banking information (Bank account numbers, Routing Numbers)	Yes _____	No _____
Other (explain) (MPIN, Austin Tetra, BSM)	_____	

If requesting proprietary, sensitive, or other data, please provide justification below:

Method of Interconnection

☐ CCR Extracts (SFTP/HTTPS)

☐ CCR XML (HTTPS)

List the external IP address and/or domain name that will be interconnecting with CCR.

_____

User Community
Users from both parties with access to the interconnection data are U.S. Government employees or contractors working on the behalf of U.S. government employees.

Information Exchange Security
The security of the information being passed on this interconnection is protected through the use of FIPS 140-2 approved encryption mechanisms. The connections at each end are located within controlled access facilities and guarded 24 hours a day. Individual users will not have access to the data except through their system's security software inherent to the operating system. All access is controlled by authentication methods to validate the approved users.

Trusted Behavior Expectations
Both parties are required to protect the other party's information in accordance with the Privacy Act and Trade Secrets Act (18 U.S. Code 1905), the Unauthorized Access Act (18 U.S. Code 2701 and 2710), OMB Policy on Protecting Personally Identifiable Information (PII), and local policies and directives.

Incident Reporting
The party discovering inconsistent or suspicious activity that may affect the confidentiality, integrity, or availability of the other party's information shall report the incident, regardless of confirmation. Each party has established a Computer Security Incidence Response Capability (CSIRC) in accordance with NIST Special Publication 800-3, Establishing a Computer Security Incidence Response Capability (CSIRC), and Federal Computer Incident Response Center (FedCIRC) publications.

Audit Trail Responsibilities
Both parties are responsible for auditing application processes and user activities involving the interconnection. Activities that will be recorded include event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. Audit logs will be retained for one (1) year.

Security Controls
Both parties shall implement reasonable security controls including, but not limited to, firewalls, intrusion detection systems, encryption, scanning and

auditing, penetration testing, patch management, incident response, and access control. These controls will be implemented to protect the confidentiality, integrity, and availability of the connected systems, and the data that will pass between them.

Contingency Planning
Both parties shall have contingency plans covering response and recovery from disasters and other disruptive contingencies that could affect their IT systems. Examples of such contingencies range from the failure of system components to the loss of computing facilities in accordance with NIST Special Publication 800-34, the Contingency Planning Guide for Information Technology Systems.

Security Training and Awareness
Both parties shall have security training and awareness programs in accordance with NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program", for all authorized personnel who will be involved in managing, using, and/or operating the interconnection. The program will ensure that personnel are familiar with IT security policy, procedures, and the rules of behavior associated with the interconnection and will require users to sign an acknowledgement form indicating that they understand their security responsibilities, if appropriate.

III. TOPOLOGICAL DRAWING

Insert a topological drawing or description indicating how _____ will interconnect with the CCR database.

IV. SIGNATORY AUTHORITY

This ISA is valid for one (1) year after the last date on either signature below. At the end of the period of validity, it will be updated, reviewed, and reauthorized. Either party may terminate this agreement upon 30 days' advance notice in writing or in the event of a security incident that necessitates an immediate response.

CCR Program Manager	Agency Official Title
Date	Date

CENTRAL CONTRACTOR REGISTRATION (CCR) RENEWAL

V. SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

Please fax completed form to DSN 661-4728, or commercial (269) 961-4728.

PRIVACY ACT STATEMENT

AUTHORITY:	Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act
PRINCIPAL PURPOSE:	To record names, signatures, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Government systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
ROUTINE USES:	None.
DISCLOSURE:	Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay, or prevent further processing of this request.

PART 1 – REQUESTER INFORMATON

1. TYPE OF REQUEST (If modification or deactivation, then provide your user ID.)
☐ MODIFICATION ☐ DEACTIVATE USER ID _____

2. SYSTEM REQUESTING ACCESS TO
☐ CCR EXTRACT ☐ FEDREG EXTRACT

3. INFORMATION REQUESTED (Request for proprietary and sensitive information may take up to two weeks to process.)

4. JUSTIFICATION FOR ACCESS (Explanation for the need of data requested)

5. NAME (Last, First, Middle Initial)		6. SOCIAL SECURITY NUMBER (LAST 6 DIGITS)
7. ORGANIZATION / AGENCY	8. OFFICE OR DEPARTMENT	9. PHONE (DSN or Commercial)
10. OFFICIAL E-MAIL ADDRESS	11. JOB TITLE AND GRADE/RANK	
12. OFFICIAL MAILING ADDRESS	13. CITIZENSHIP ☐ US ☐ FN ☐ OTHER	14. DESIGNATION OF PERSON ☐ GOV ☐ CIVILIAN ☐ CONTRACTOR

USER AGREEMENT

I accept the responsibility for the information and Federal Government system to which I am granted access and will not exceed my authorization level of system access. I understand that my access may be revoked or terminated for non-compliance with Government security policies. I accept responsibility to safeguard the information contained in these systems from unauthorized or inadvertent modification, disclosure, destruction, and use. I understand and accept that my use of the system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems. I agree to notify the appropriate organization that issued my account(s) when access is no longer required.

15. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS
I have completed Annual Information Awareness Training. ☐ DATE OF COMPLETION _____

16. USER SIGNATURE	17. DATE (YYYYMMDD)

PART 2 - ENDORSEMENT OF ACCESS BY USER SUPERVISOR OR GOVERNMENT SPONSOR		
18. VERIFICATION OF NEED TO KNOW I certify this user requires access as requested. ☐	19. EXPIRATION DATE OF ACCESS (If less than 1 year)	
20. NAME *(Print name)*	21. SIGNATURE	22. DATE
23. OFFICE OR DEPARTMENT	24. E-MAIL ADDRESS	25. PHONE NUMBER

PART 3 – SECURITY MANAGER VALIDATES BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION		
26. TYPE OF INVESTIGATION		27. CLEARANCE LEVEL
28. IT LEVEL DESIGNATION	29. DATE	30. TYPE OF DESIGNATION
31. VERIFIED BY (Print name)	32. SIGNATURE	33. DATE

CCR INTERNAL USE ONLY

COMPLETION BY AUTHORIZED STAFF CONDUCTING SECURITY REVIEW		
AFTER REVIEWING THIS ACCESS REQUEST, I RECOMMEND THE FOLLOWING ACTION TO BE TAKEN:		
☐ Approve access	☐ Deny access	Signature and date

DECISION OF CCR DATA OWNER		
AFTER REVIEWING THIS ACCESS REQUEST, I DIRECT THE FOLLOWING ACTION TO BE TAKEN:		
☐ Approve access	☐ Deny access	Signature and date

INSTRUCTIONS

PART 1 - The following information is supplied by the requester when establishing or modifying his or her account.

(1) Indicate if you are requesting new access or updating or removing existing access. If you are updating or removing access, then provide your User ID.
(2) Indicate the CCR system you wish to access.
(3) List the information you are requesting to obtain from the system. Examples include financial data, tax information, etc.
(4) Provide the reason you need this information to perform your official duties.
(5) Name.
(6) Social Security Number (Last 6 digits).
(7) Organization Agency. User's current organization (i.e. DOD/Army, DoD/DLA, DoT, DHS)
(8) Office or department. Office symbol or department within your organization or agency.
(9) Phone number, DSN is preferred.
(10) Official e-mail address. Do not use free ISP accounts such as hotmail, yahoo, or gmail.
(11) Job Title , Grade / Rank. Civilian job title such as Systems Analyst, GS-15, Pay Clerk, GS-5)/military rank (COL, US Army, CMSgt, USAF) or "CONT" if user is a contractor.
(12) Official Mailing Address
(13) Citizenship. US citizen, foreign national, or other.
(14) Designation. Government, civilian, or contractor.
(15) Awareness training. Indicate whether or not you have had annual IA awareness training and the date it was completed.
(16) Signature.
(17) Date signed.

PART 2 - If the requester is a government employee, then this section must be completed by a supervisor. If the requester is a contractor, then this section must be completed by the government sponsor.

(18) Verification of need to know. You are certifying that the requester requires this access to perform their official duties.
(19) Expiration date of access. If less than one year, then indicate that date. All accounts expire no later than one year from activation.
(20) Name. Supervisor or government sponsor's printed name.
(21) Signature. Supervisor or government sponsor's signature.
(22) Date. Date of signature of supervisor or government sponsor.
(23) Office or department. Office symbol or department within your organization or agency.
(24) E-mail address. Do not use free ISP accounts such as hotmail, yahoo, or gmail.
(25) Phone number. DSN is preferred.

PART 3 - Security manager validates background investigation or clearance information.

(26) Type of investigation. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).
(27) Clearance level. The user's current clearance level (i.e., Secret or Top Secret).
(28) IT level designation. The user's ADP level designation (ADP1, ADP2, etc.).
(29) Date. Date of last investigation.
(30) Type of designation. The user's ADP level designation (ADP1, ADP2, etc.).
(31) Verified by. The security manager or representative prints his or her name to indicate that the above clearance and investigation information has been verified.
(32) Signature. The security manager or representative signs his or her name to indicate that the above clearance and investigation information has been verified.
(33) Date. Date form was signed by security managers or representative.

VI. CCR/FEDREG SYSTEMS INTERCONNECT AGREEMENT DESCRIPTIONS

1. DOCUMENT	Interconnection Security Agreement (ISA)
2. INFORMATION DESCRIPTION	CCR Data
3. RECEIVING AGENCY	Receiving Agency Name
4. RECEIVING SYSTEM	Receiving System Name
5. RECEIVING SYSTEM LOCATION	Receiving System Location
6. SENDING AGENCY	Defense Business Transformation Agency (BTA)
7. SENDING SYSTEM	Central Contractor Registration (CCR)
8. SENDING SYSTEM LOCATION	DLIS / Battle Creek, MI
9. PRIVACY ACT INFORMATION	N/A
10. FORMAT	XML/Text
11. CLASSIFICATION	Sensitive Unclassified
12. FREQUENCY	XML – Real time, Extract - Daily
13. MEDIA	SFTP/HTTPS
14. PROTECTION	Encryption (SFTP, HTTPS) Authentication (Password)

VII.CCR NON-DISCLOSURE AGREEMENT

CCR NON-DISCLOSURE AGREEMENT
FOR {Receiving Agency Acronym} INFORMATION ACCESS

1. To carry out its duties, {Receiving Agency Acronym} may disclose information to authorized representatives of the United States (U.S.) Government. This Non-Disclosure Agreement ("Agreement") covers information provided to the Department of Defense (DoD) under a mandate for federal contractors as described in 48 CFR, Parts 204, 212, and 252 and the Debt Collection Improvement Act of 1996, Public Law 104-134. The disclosure of such information to the public or outside of the government shall be in accordance with all conditions and limitations set forth herein.

2. This Agreement is entered into this ___ day of _____, 20___, between **{Receiving Agency Acronym}** and _____, (hereinafter "Data Receiver"), with a duration of one year. The Data Receiver has a requirement for such data to perform certain tasks on behalf of the U.S. Federal Government. Because of this requirement, the Data Receiver is considered "authorized" for the purpose of this Agreement.

3. {Receiving Agency Acronym} hereby determines that disclosure of information described in paragraphs 1 and 2 is necessary so that the Data Receiver may perform the duties required of them by the U.S. Federal Government.

4. {Receiving Agency Acronym} shall grant access to information described in paragraphs 1 and 2 for each year that a completed Non-Disclosure form is submitted until the Data Receiver requests termination of access or {Receiving Agency Acronym} terminates access. ** This Non-Disclosure Agreement must be renewed each year.

5. The Data Receiver accepts the obligations contained in this Agreement in consideration of being granted access to the information described in paragraphs 1 and 2. The Data Receiver acknowledges that all obligations imposed by this agreement concerning the use and disclosure of such information apply for the duration of the requirement and at all times thereafter.

6. The Data Receiver agrees that it shall use the information described in paragraphs 1 and 2 only for the purpose of the work required by the U.S. Federal Government and shall not use such data for commercial purposes.

7. The Data Receiver agrees it shall not disclose or provide access to information described in paragraphs 1 and 2 to anyone unless it has verified that the recipient has been properly authorized to receive such information.

8. The Data Receiver agrees to adopt operating procedures and physical security measures to properly safeguard such information from unauthorized use and from disclosure or release to unauthorized third parties.

9. The Data Receiver agrees to return to {Receiving Agency Acronym} all copies of any abstracts or extracts of data described in paragraphs 1 and 2, of which it has possession pursuant to this Agreement, upon request of {Receiving Agency Acronym} or the completion or termination of the tasks set forth by the U.S. Federal Government, whichever comes first.

10. The Data Receiver hereby acknowledges that any violation or breach of this Agreement shall constitute grounds for termination of access to such information; suit for damages; suit to enforce the Agreement—including, but not limited to, application for a court order prohibiting disclosure or use of information in violation or breach of this Agreement; and/or suit for civil fines or penalties. The Data Receiver further acknowledges that the unauthorized use, disclosure, or retention of the information may constitute a violation of the U.S. criminal laws, including provisions of sections 641, 793, 794, and 1905, title 18 U.S. Code, and that nothing in this Agreement constitutes a waiver by the U.S. of the right to prosecute for any statutory violation.

11. The Data Receiver agrees that any data received will not be used for testing purposes or in a testing environment. Real time user data is not to be used for system testing in any way.

Acknowledging Party

Signature: _____

Printed Name: _____

Title: _____

Service/Agency: _____

Office/Dept: _____

Project: _____

Commercial Phone: _____ DSN: _____

Email Address: _____

Date: _____

Agency Registration Official Verification

Verification of ARO for requester named above:

Signature of ARO: _____

Printed: _____

Title: _____ Date: _____

Commercial Phone: _____ DSN: _____