INTEGRATED RESEARCH & DEVELOPMENT FOR ENTERPRISE SOLUTIONS
REQUEST FOR BIDDERS' LIBRARY AND DOCUMENT HANDLING AND SAFEGUARDING PROCEDURES AGREEMENT (v2.2)

Section 1: Form Purpose, Instructions, and Background Information

Purpose: Interested parties must use this form to request a copy of the Integrated Research & Development for Enterprise Solutions (IRES) bidders' library and acknowledge document handling and safeguarding procedures.

Instructions: Complete Section 2 of the form and return the completed form to the MDA via email to IRESCoreTeam@mda.mil (include "IRES Library Request" in the subject line) or via facsimile to 719-721-9575.

Information: Interested parties may request the IRES bidders' library at any time by returning a copy of the completed form to the MDA. In order to be eligible to receive the library, companies must have a facility clearance and an active Joint Certification Program (JCP) certification. When available, the library CD/DVD ROM will be mailed to the name and physical address associated with the JCP certification and will include a copy of this form. Requests from interested parties that do not yet have the facility clearance and JCP certification will be accepted, but the CD/DVD ROM will not be mailed until the MDA can confirm these requirements have been met. (Additional information regarding application for the JCP certification is available at the Defense Logistics Agency (DLA) Logistics Information Service (DLIS) JCP homepage at http://www.dlis.dla.mil/jcp/Default.aspx.)

Section 2: Requestor Acknowledgments and Data

By submitting this request, the requestor acknowledges the following:

- Your company will use the IRES bidders' library content only for the purpose of pursuing the IRES acquisition.
- As a minimum and regardless of whether or not marked, the IRES bidders' library CD/DVD ROM (or alternate transmission media) and all individual content are considered Controlled Unclassified Information (CUI) and shall be handled and safeguarded as For Official Use Only (FOUO); all technical data are considered export controlled technical data. Additionally, your company will comply with any and all notices and restrictive markings on the individual documents.
- The CD/DVD ROM and all individual content will be protected as FOUO/CUI and export controlled material in accordance with the attached For Official Use Only/Controlled Unclassified Information Handling Instructions and U.S. DoD Directive 5230.25.
- Compliance with the security controls as specified in paragraph (b) and reporting of cyber incidents as specified in paragraph (c) of DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting (Dec 2015)*, is in effect for all IRES bidders' library content resident on or transiting contractor unclassified information systems.
- Further distribution of the CD/DVD ROM and any of its content shall only be as authorized or directed by Missile Defense Agency/DAC(J) or higher DoD authority.
- Your company will immediately report a failure to comply with any of the document handling and safeguarding procedures identified herein to the IRES contracting officer.

Company name: _____ Request date: _____

Requestor name: _____

Requestor email address: _____ Requestor telephone # _____

DUNS #_____ CAGE code: _____

JCP certification number and expiration date: _____

Requestor comments (if any):

Section 3: IRES Librarian Record (Internal MDA Use Only)

Date request received:_____

Facility clearance, JCP certification, CAGE code, address, and SAM exclusions verified (date and initials): _____

Date library sent:_____ Version library sent: _____

Comments:

Approved for Public Release 15-MDA-8410 (22 September 15)

REQUEST FOR BIDDERS' LIBRARY AND DOCUMENT HANDLING AND SAFEGUARDING PROCEDURES AGREEMENT

FOR OFFICIAL USE ONLY/CONTROLLED UNCLASSIFIED INFORMATION SUPPLEMENT

1. Definitions.

a. Controlled Unclassified Information (CUI). Unclassified information which requires access and distribution limitations prior to appropriate coordination and an official determination by cognizant authority approving clearance of the information for release to one or more foreign governments or international organizations, or for official public release. Per DoD Manual 5200.01, Volume 4 it includes the following types of information: "For Official Use Only" (FOUO); "Sensitive But Unclassified" (State Department information); "DEA Sensitive Information" (Drug Enforcement Agency information); "DoD Unclassified Controlled Nuclear Information"; "Sensitive Information" as defined in the Computer Security Act of 1987; and information contained in technical documents (i.e., Technical Data) as discussed in DoD 5230.24, 5230.25, International Traffic in Arms Regulation (ITAR), and the Export Administration Regulations (EAR).

b. Controlled Technical Information (CTI). "Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

c. Covered Defense Information. "Covered defense information" means unclassified information that:

(1) Is—

(a) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

(b) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and

(2) Falls in any of the following categories:

(a) Controlled technical information.

(b) Critical information (operations security). Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(c) Export control. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

(d) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies (e.g., privacy, proprietary business information).

d. Dual Citizenship. A dual citizen is a citizen of two nations. For the purposes of this document, an individual must have taken an action to obtain or retain dual citizenship. Citizenship gained as a result of birth to non-U.S. parents or by birth in a foreign country to U.S. parents thus entitling the individual to become a

citizen of another nation does not meet the criteria of this document unless the individual has taken action to claim and to retain such citizenship.

e. For Official Use Only (FOUO). FOUO is a dissemination control applied by the DoD to unclassified information that may be withheld from public disclosure under one or more of the nine exemptions of the Freedom of Information Act (FOIA) (See DOD 5400.7-R). FOUO is not a form of classification to protect U.S. national security interests.

f. National of the United States. Title 8, U.S.C. Section 1101(a)(22), defines a National of the U.S. as:

(1) A citizen of the United States, or,

(2) A person who, but not a citizen of the U.S., owes permanent allegiance to the U.S.

NOTE: 8 U.S.C. Section 1401, paragraphs (a) through (g), lists categories of persons born in and outside the U.S. or its possessions that may qualify as Nationals and Citizens of the U.S. This subsection should be consulted when doubt exists as to whether or not a person can qualify as a National of the U.S.

g. U.S. Person. Any form of business enterprise or entity organized, chartered, or incorporated under the laws of the United States or its possessions and trust territories and any person who is a citizen or national (see National of the United States) of the United States, or permanent resident of the United States under the Immigration and Nationality Act.

2. Access.

a. Access to FOUO/CUI must be limited to U.S. Persons that have a current U.S. security clearance (minimum interim SECRET clearance); or have been the subject of a favorably completed National Agency Check with Inquiries (NACI) or a more stringent personnel security investigation. Access approval by MDA/Special Security is pending completion of a favorable NACI or Contractor equivalent.

(1) Contractor Equivalent: Contractor equivalent includes various background checks such as those performed by employers during hiring process. Minimum checks shall include Citizenship, Personal Identification (Social Security Number), Criminal, and Credit. Contractors shall submit a request for approval on company letter head to MDA/Special Security.

(2) Contractor personnel with dual citizenship that have an active U.S. security clearance (interim Secret or higher) can have access to FOUO/CUI material.

(3) Contractor personnel with dual citizenship that do not have an active U.S. security clearance (interim Secret or higher), the following actions will be completed prior to authorizing access to FOUO/CUI material:

(a) The dual citizen shall surrender the foreign passport to the security office

(b) The Contractor Company shall provide a signed letter to the dual citizen informing them that if they request their passport be returned to them, or they obtain a new foreign passport, they will be immediately removed from the MDA program. The dual citizen shall acknowledge by signing and dating the letter.

(c) The MDA Program Manager and MDA/Special Security shall be notified and will provide written approval.

b. Non-Sensitive Positions (ADP/IT-III positions). Non-sensitive positions associated with FOUO/CUI are found at Contractor facilities processing such information on their (Contractor's) unclassified computer systems. Personnel nominated to occupy ADP/IT-III designated positions (applies to any individual that may have access to FOUO/CUI on the Contractor's computer system) must have at least a National Agency Check with Inquiries (NACI) or Contractor equivalent (company hiring practices reviewed and approved by MDA/Special Security). When "Contractor equivalent" option is NOT authorized and there is no record of a valid investigation, the Contractor shall contact MDA/Special Security at mdasso@mda.mil, and provide the requested information.

MDA/Special Security will assist the Contractor complete the SF85, Position of Trust Questionnaire, and fingerprints.

3. Identification Markings. FOUO/CUI shall be marked in accordance with DoDM 5200.01, Volume 4, Enclosure 3, Section 2.c.

4. Handling. Storage of FOUO/CUI outside of Contractor facilities (i.e. residence, telework facility, hotel, etc.) shall be in a locked room, drawer, filing cabinet, briefcase, or other storage device. Continuous storage of FOUO/CUI outside of a Contractor facility shall not exceed 30 days unless government approval is granted.

5. Transmission/Dissemination/Reproduction.

a. Subject to compliance with official distribution statements, FOUO markings (e.g., Export Control, Proprietary Data) and/or Non-Disclosure Agreements which may apply to individual items in question; authorized Contractors, consultants and grantees may transmit/disseminate FOUO/CUI information to each other, other DoD Contractors and DoD officials who have a legitimate need to know in connection with any DoD authorized contract, solicitation, program or activity. The government Procuring Contracting Officer (PCO) will confirm with the Contracting Officer's Representative or Task Order Monitor "legitimate need to know" when required. The MDA/Chief Information Officer has determined that encryption of external data transmissions of FOUO/CUI are now practical. The MDA/Chief Information Officer has stated that Public Key Infrastructure (PKI) and Public Key (PK) enabling technologies are available and cost effective. The following general guidelines apply:

(1) In accordance with DoD Manual 5200.01, Volume 4, “Controlled Unclassified Information (CUI),” Enclosure 3, external electronic data transmissions of CUI/FOUO shall be only over secure communications means approved for transmission of such information. Encryption of e-mail to satisfy this requirement shall be in accordance with MDA Directive 8190.01, Electronic Collaboration with Commercial, Educational, and Industrial Partners, May 12, 2009, being accomplished by use of DoD approved Public Key Infrastructure Certification or by the company’s participation in the “Federal Bridge.”

(2) The MDA/Chief Information Officer (CIO), PKI Common Access Card (CAC) point of Contact is, Ms. Ingrid Weecks (719-721-7040).

b. Failure of the Contractor to encrypt FOUO/CUI introduces significant risks to the BMDS mission. It is essential for the Contractor to understand that mitigation options that are available. The Contractor must understand that failure to encrypt FOUO/CUI carries with it certain risks to the mission. These risks can be mitigated with the thoughtful application of processes, procedures, and technology. Some of the available mitigation tools include:

(1) Approved DoD PKI/CAC hardware token certificates or DoD trusted software certificates for encrypting data in transport.

(2) Industry best practice of Virtual Private Network (VPN) Internet Protocol Security (IPSEC) for intra-organization transport.

(3) Industry best practice of Secure Sockets Layer Portal Web Services for document sharing and storage.

(4) Approved DoD standard solutions for encrypting data at rest.

(5) Approved DoD E-Collaboration services via MDA Portal or Defense Information Systems Agency (DISA) Network Centric Enterprise Services (NCES).

(6) Any FIPS 140-2 validated encryption [e.g., IPSEC, Secure Socket Layer/Transport Layer Security (SSL/TLS), Secure/Multipurpose Internet Mail Extensions (S/MIME)].

(7) Procure and employ Secure Telephone Equipment (STE).

(8) Procure and employ secure facsimile (FAX) capability.

(9) Utilize secure VTC capabilities.

(10) Hand-carry FOUO/CUI.

(11) Utilize mailing through U.S. Postal Service.

(12) Utilize overnight express mail services.

c. FOUO/CUI shall be processed and stored internally on Automated Information Systems (AIS) or networks 1) when distribution is to an authorized recipient and 2) if the receiving system is protected by either physical isolation or a password protection system. Holders shall not use general, broadcast, or universal e-mail addresses to distribute FOUO/CUI. Discretionary access control measures may be used to preclude access to FOUO/CUI files by users who are authorized system users, but who are not authorized access to FOUO/CUI. External transmission of FOUO/CUI shall be secured using NIST-validated encryption. FOUO/CUI cannot be placed on any publically-accessible medium.

d. Reproduction of FOUO/CUI may be accomplished on unclassified copiers within designated government or Contractor reproduction areas.

6. Storage. During working hours, reasonable steps shall be taken to minimize the risk of access by unauthorized personnel (e.g., not reading, discussing, or leaving FOUO/CUI information unattended where unauthorized personnel are present). After working hours, FOUO/CUI information may be stored in unlocked containers, desks, or cabinets if contract building security is provided. If such building security is not provided or is deemed inadequate, the information shall be stored in locked desks, file cabinets, bookcases, locked rooms, etc.

7. Disposition.

a. When no longer required, but no later than 60 days after award of the IRES contract, FOUO/CUI shall be returned to the MDA office that provided the information or destroyed by any of the means approved for the destruction of classified information or by any other means that would make it difficult to recognize or reconstruct the information.

b. Removal of the FOUO/CUI status can only be accomplished by the government originator. The MDA COR shall review and/or coordinate with proper authority the removal of FOUO/CUI status for information in support of contract activity.