



**12. PUBLIC RELEASE.** Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the National Industrial Security Program Operating Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release

Direct  Through (specify):

Office of the System of Systems Integration, SOSI, ATTN: SFAE-SSI-CSC / 515, Warren, MI 48397-5000, who will obtain Public Release approval through the prescribed channels to include the SOSI Security Manager, PCO and PAO.

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)\* for review.  
\*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

**13. SECURITY GUIDANCE.** The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classified assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Block 8 Continued – System of Systems Integration  
 WSMR, NM

System of Systems Integration  
 Ft. Bliss, TX

Access to SOSI technical data by foreign interests is prohibited unless authorized by a valid export authorization.

The following attachments are made part of this DD Form 254:

Attachment “A” – CONTROLLED UNCLASSIFIED INFORMATION (Item 10.j. and Item 10.k.)

Item 11.a - Collateral classified information generated in support of this contract shall be classified in accordance with the source material used (available at the Government site) and protected in accordance with the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M, and this DD Form 254. Government site security rules at the performance location will be followed. Unclassified information will be protected IAW the Attachment A; SOSI OPSEC Plan; and, this DD Form 254.

Item 11.j – OPERATIONS SECURITY (OPSEC) REQUIREMENTS: The contractor will adhere to the site’s SOSI OPSEC Plan.

Item 11.l – INFORMATION SYSTEMS (IS) PROCESSING REQUIREMENTS: For access to Government IS or systems processing US Government information will in IAW AR 25-2.

Block 12 – PUBLIC RELEASE: One (1) electronic copy on disk with full text and graphics must be provided at least fifteen (15) working days prior to the requested release date. If all or part of the information was generated by another organization, their written release authorization must accompany the request.

Reports of loss, compromise or suspected compromise of Controlled Unclassified Information (CUI) or Classified Information shall be provided to the Government SOSI Security Office within 24 hours of the incident, in addition to the reporting requirements outlined in the NISPOM.

**14. ADDITIONAL SECURITY REQUIREMENTS.** Requirements, in addition to NISPOM requirements, are established for this contract. (If, Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.) YES \_\_\_\_\_ NO

**15. INSPECTIONS.** Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.) YES \_\_\_\_\_ NO

**16. CERTIFICATION AND SIGNATURE.** Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this contract effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL Rick Bailey	b. TITLE Warren Site Security Manager System of Systems Integration Directorate	c. TELEPHONE (Include Area Code) (586)-282-9635
d. ADDRESS (Include Zip Code) System of Systems Integration SFAE-SSI-CSC/515 6051 E. 11 Mile Road Warren, MI 48397-5000	17. REQUIRED DISTRIBUTION <input checked="" type="checkbox"/> a. CONTRACTOR <input type="checkbox"/> b. SUBCONTRACTOR <input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR <input type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION <input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER <input type="checkbox"/> f. OTHERS AS NECESSARY	
e. SIGNATURE		

DD Form 254 Reverse, DEC 99

## ATTACHMENT A: CONTROLLED UNCLASSIFIED INFORMATION

**General:** There are types of information that are not classified, but which require protective measures which restrict its distribution for a variety of reasons. This information is known as "Controlled Unclassified Information (CUI)." The types of information considered CUI for this contract are information marked "For Official Use Only" and Technical Data.

**Technical Data Description:** Any recorded information related to experimental, developmental, or engineering works that can be used to define an engineering or manufacturing process or to design, procure, produce, support, maintain, operate, repair, or overhaul program material. The data may be graphic or pictorial delineations in media, such as computer software, drawings or photographs, text in specifications, or related performance or design documents, or computer printouts. Examples of technical data include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, catalog-item identifications, and related information, and computer software documentation.

**FOR OFFICIAL USE ONLY INFORMATION (FOUO) Description:** "For Official Use Only (FOUO)" is a designation that is applied to **unclassified** information that may be exempt from mandatory release to the public under the Freedom of Information Act. FOUO information includes information identified as such in the Security Classification Guide or information from a government document marked FOUO. FOUO shall be applied to any information that is neither approved for public release nor a technical document.

### **CUI Markings**

Marking of FOUO documents will be in accordance with Army Regulation 25-55. ([http://www.apd.army.mil/pdf/AR25\\_55.pdf](http://www.apd.army.mil/pdf/AR25_55.pdf)). Information extracted from an FOUO document will carry the FOUO marking until formally reviewed by the government.

Marking of unclassified Technical Data will, at a minimum include the statements listed below. This does not preclude additional mandated markings as may be required by the contract such as Competition Sensitive Information.

**Distribution Statement:** Unless otherwise directed by the government Security Manager, the below Distribution Statement is required on all Technical Data developed under this contract.

DISTRIBUTION STATEMENT F: Further dissemination only as directed by System of Systems Integration (SOSI) Security Office or higher DoD authority, 1 Oct 2011. Requests to disseminate this document shall be referred to System of Systems Integration Security Office, Attn: SFAE-INT-CSC/mail stop 515, 6501 East Eleven Mile Road, Warren, MI 48397-5000.

**Export Warning Statement:** Technical Data contained in documents not approved for export shall display the appropriate export control caveat on the front cover or title page, as follows:

**"WARNING** - This document contains technical data whose export may be restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq) or the Export Administration Act of 1979, as amended (Title 50, U.S.C., App. 2401 et seq). Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25."

The government Security Manager may require more or less restrictive distribution statements on certain types of CUI information as security needs require.

Preliminary or working drafts shall not be disseminated without a proper security classification review and assignment of a distribution statement.

### **Sharing Distribution Statement F material outside the SOSI**

The holder of the document is not authorized to release the information in any form to anyone other than the SOSI. Sharing of Distribution Statement F documents with non-SOSI participants requires authorization from the government Security Manager and/or a change to the Distribution Statement.

### **Protection of CUI Information**

**Access:** CUI is restricted to individuals who are a U.S. Citizen and with a valid need to know for the information. Unless public release authorization has been obtained, information, in any media format is prohibited from further dissemination. The need to know restricts the use or dissemination of CUI data to those individuals or organizations with direct affiliation

with the given program or project. Further dissemination of such information will be at the discretion of the government Security Manager. Personnel no longer requiring access to CUI must delete or surrender any in their possession and terminate future access to it.

**Storing/Handling:** During working hours, reasonable steps should be taken to minimize risk of access to CUI by unauthorized personnel (for example, janitorial staff). After working hours, CUI information shall be stored in locked desks, file cabinets, bookcases, locked rooms, or similar means. CUI may not be displayed in public places, such as airports, airplanes, restaurants, etc. Computers used for processing CUI do not need to be accredited for classified use. Do not process DoD information on public computers (e.g. those available for use by the general public in kiosks, hotel business centers or the like) or computers that do not have access control. Personally owned computers and Portable Electronic Devices (PEDs) are not authorized for processing CUI. CUI stored electronically on all devices such as company issued laptops, Portable Electronic Devices (PEDs), and removable media, are to be physically protected or protected using cryptographic products that are either NIST/NIAP approved. Protect CUI by at least one physical or electronic barrier when not under direct individual control.

**Dissemination:** CUI printed documents and material may be transmitted through mail channels or handcarried without formal courier orders. Use of secure communications whenever possible; however, land-line communications for telephone conversations are more secure than cellular and should be utilized whenever available for program CUI discussions. Voice and fax transmissions will be transmitted only when the sender has a reasonable assurance that only authorized recipients will have access to the transmission. Digital transmission will be by the NISP/NIAP approved encrypted email or Army Knowledge Online (AKO) collaborative suites. However when AKO is not feasible (e.g., foreign suppliers, non-program associated personnel, etc.) the following guidelines apply:

- Collaborative suites may be used by personnel not located on a government backbone (i.e., NIPRNET) without Government Security Office approval provided all of the following requirements apply:

- Use only NIST/NIAP approved cryptographic vendors and algorithms. The latest validation lists may be obtained at: <http://csrc.nist.gov/cryptval/> and,
- An internally hosted service (does not use third-party collaborative suite service provider) and, (excluding currently approved collaborative tools pending final Government determination).

- Personnel with access to NIPRNET require Enterprise Designated Approving Authority (DAA) approval prior to participation in any collaborative suite that requires installation of mobile code on the local NIPRNET connected system.

- All computers containing program CUI must be protected by either physical isolation from all personnel without a valid need for the information or protected using Data At Rest (DAR) cryptographic products that are NIST/NIAP approved. Discretionary access control measures must be used to grant authorized users access to CUI data. After working hours, when not in physical possession of the owner, all computers and PEDs containing program CUI must be afforded a reasonable degree of physical protection to prevent theft of program information i.e. locking up laptops or cable locking them to a stationary base.

- All transmission/dissemination of CUI identified with a Distribution Statement or marked FOUO (i.e. email and file transfers) must use applications utilizing NIST/NIAP approved cryptographic vendors and algorithms. The latest validation lists may be obtained at: <http://csrc.nist.gov/cryptval/>. This encryption requirement includes passcodes to teleconferences or webconferencing where there is a reasonable expectation that CUI may be discussed. When encryption is not available, AKO must be used to transmit/disseminate CUI.

- Do not post CUI to web pages that are publically available or have access limited only by domain/IP restrictions.
- As new technologies become available in the electronics arena care should be given to providing a reasonable degree of protection to program information from known vulnerabilities.
- Internet shall be equated with "Public Access". Therefore, CUI must be reviewed and officially approved for public release before placing on the Internet. This is not applicable when the internet is used for e-mail transmissions and encryption is used as noted above.

**Disposal:** CUI documents shall be destroyed by cross-cut shredding or equivalent method so as not to be easily reconstructed. Removable media and computing devices may also be disposed of by providing them to a company's internal organization responsible for destruction. Sanitize CUI IAW NSA/CSS Policy Manual 9-12, 13 March 2006 before sale, transfer, or reassignment to those not authorized and requiring access to data stored thereon.

**Report of Loss of CUI:** Any loss of CUI or loss of unencrypted CUI from an information system shall be reported to the government Security Manager and to their supporting counterintelligence office. Initial reports shall be made as

expeditiously as possible in all cases within 72 hours of discovery. Additional information may be required after submission and review of the initial report, guidance will be provided at that time. Mark any reports For Official Use Only, identifying exemptions 2 and 5 apply. Initial report content shall include the following information as available.

- Applicable dates, including dates of compromise and dates of discovery
- Threat methodology, including all known resources used (e.g. IP addresses, domain names, software tools)
- Account of what actions the threat(s) may have taken on victim system/network
- What information may have been compromised, exfiltrated, or lost and its potential impact on government programs

**Report of Cyber Intrusions:** Upon confirmation of cyber intrusions that result in compromise of CUI, contractors will inform the DoD-DIB Common Information Sharing Environment (DCISE). The contractor will also notify the government Security Manager and their supporting counterintelligence office of any cyber compromises. Refer to Report of Loss of CUI for what needs to be reported, when and how.