ATTACHMENT A

ADDITIONAL GUIDELINES FOR CONTROLLED UNCLASSIFIED INFORMATION

General: There are types of information that are not classified but that require application of access and distribution controls and protective measures for a variety of reasons. This information is known as "controlled unclassified information (CUI)." The types of information considered CUI are U.S. Government technical information and information listed at the CUI registry (https://www.archives.gov/cui/registry/category-list). When handling CUI material, all personnel are to comply with these requirements and follow their company policy and/or applicable Non-Disclosure Agreement (NDA) concerning the protection of proprietary information in situations not clearly stated herein.

Technical Information Description: Any recorded information related to experimental, developmental, or engineering works that can be used to define an engineering or manufacturing process, or can be used to design, procure, produce, support, maintain, operate, repair, or overhaul program material. The data may be graphic or pictorial delineations in media (e.g., computer software, drawings, or photographs), text in specifications, related performance or design documents, or computer printouts. Examples of technical information 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.

CUI Information Description: Unclassified Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide or "LRGWP" policies but is not classified under EO 13526, (Classified National Security Information).

CUI Markings All documents containing CUI will carry the CUI markings in accordance with DoDI 5200.48. Discontinue all use of legacy or other markings not permitted or included in either the CUI Registry or DoDI 5200.48. Marking of Technical Information will include the statement provided in the Security Classification Guide. If the contents of the technical document require more than one Distribution Statement, apply the most restrictive statement. This does not preclude additional mandated markings as may be required by the contract.

Protection of CUI Information

Access: In accordance with (IAW) DoDI 5200.48, Controlled Unclassified Information (CUI), July 2023, all contractors supporting this contract who receive, store, or generate CUI are required to take the DoD Mandatory CUI training available on the Security Awareness Hub at : https://securityawareness.usalearning.gov/cui/index.html. Per DoDI 5200.48 and pursuant to all contractual requirements, DoD contractors require initial CUI training and annual CUI refresher training. CUI may be released only to an individual who has a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose. Further dissemination of such information will be at the discretion of the Government Security Manager. All personnel supporting this contract shall sign a CUI Non-disclosure Agreement prior to gaining access to the information. Personnel no longer requiring access to CUI must dispose (see "Disposal" below) or surrender any in their possession and terminate future access to it.

Storing/Handling: During working hours, take reasonable steps to minimize risk of access to CUI by unauthorized personnel. After working hours, when not in physical possession of the owner, all CUI (whether hardcopy or optical media (e.g., DVDs, CDs) that contain CUI) must be afforded a reasonable degree of physical protection to prevent theft of program information (e.g., store CUI information in locked desks or file cabinets, locked rooms, cable lock laptops, storing in a trunk, storing out of site or similar means). Do not display CUI in public places (e.g., airports, airplanes, restaurants). Electronic storing and processing of CUI shall be in accordance with DFARS 252.204-7012 Safeguarding Controlled Defense Information and Cyber Incident Reporting. Do not process CUI on public computers (e.g., those available for use by the general public in kiosks, hotel business centers), public wireless networks or computers that do not have access control. Personally owned computers and personally owned devices are not authorized to process CUI. Portable electronic devices (e.g., smartphones, laptop computers, tablets), non-portable computers, and removable media (e.g., external hard drives, flash drives, USB drives; not including optical media) must be physically and electronically protected as described in this instruction, DFARS 252.204-7012 and DoDI 8582.01.

Dissemination: CUI printed documents and material may be transmitted through mail channels, commercial carrier or hand-carried without formal courier orders. CUI information may be disseminated to DoD personnel and DoD contractors to conduct official business for the program. If dissemination is required outside of DoD personnel or DoD contractors, contact the Government Security Manager for approval. Technical information will follow the release instructions identified in the Distribution Statement. Use secure communications whenever possible; however, land-line telephones are more secure than cellular telephones and should be used whenever available for

discussions involving CUI. Transmit voice and facsimile transmissions only when you have a reasonable assurance that only authorized recipients will have access to the transmission. Digital transmission shall comply with the below:

All transmission and/or dissemination of CUI (i.e., email and file transfers) must use NIST/NIAP-approved cryptographic products/algorithms, e.g., DoD-approved Public Key Infrastructure Certification or DoD Safe Exchange at https://safe.apps.mil/. These are available at http://iase.disa.mil/pki/eca or http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm. This encryption requirement includes communications that contain passcodes to teleconferences or web conferences where there is a reasonable expectation that CUI may be discussed. When encryption is not available, a government collaborative suite (aka Integrated Digital Environment [IDE]) must be used to transmit CUI.

- Contractor-hosted collaborative suites may be used for digital transmission and/or dissemination of CUI by personnel not located on a government backbone (e.g., NIPRNET), provided the following conditions apply: 1) Use only NIST/NIAP-approved cryptographic products/algorithms. The latest validation lists may be obtained at http://iase.disa.mil/pki/eca or http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm; and, 2) Use an internally hosted service that does not use a third-party collaborative suite service provider.

- Do not post CUI to web pages that are publicly available or have access limited only by domain/IP restrictions. As permitted by other contract provisions, CUI may be posted to web pages that control access through the use of a DoD approved Public Key Infrastructure Certification and that provide protection via use of secure sockets, or other equivalent technologies. These are available at http://iase.disa.mil/pki/eca.

- As new technologies become available in the electronics arena, care should be given to providing a reasonable degree of protection from known vulnerabilities.

- The Internet is “Public Access”. CUI must be reviewed and officially approved by the TACOM Public Affairs Officer 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: The contractor shall ensure any covered defense information provided by the Government under this contract is destroyed or sanitized from contractor-owned media and reported in accordance with (IAW) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, Revision 1: Guidelines for Media Sanitization (December 2014) (NIST SP 800-88, rev 1), destruction methods, or any destruction method approved for Classified National Security Information (32 CFR 2001.47) unless the CUI category's authority mandates other destruction methods (CUI Specified categories). Agencies must also use destruction methods specifically required by law, regulation, or Government-wide policy for CUI Specified categories. Destroy CUI documents in a manner that makes it unreadable, indecipherable, and irrecoverable (32 CFR 2002.14(f)(2)). For paper documents, Reference CUI Notice 2019-03: Destroying of Controlled Unclassified Information (CUI) in paper form.

Report of Loss of CUI: Report any loss of CUI to the Government Security Manager. Initial reports shall be made as expeditiously as possible in all cases within 72 hours of discovery. If additional information is required after submission and review of the initial report, guidance will be provided at that time. 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 or lost, and its potential impact on government programs