Supplemental Requirements for Electronic Processing and Storing of Unclassified and Controlled Unclassified Information

Revision 08/2021

This document establishes requirements applicable to Purchase Orders that involve electronic processing and storing of Unclassified Information and/or Information designated as Controlled Unclassified Information (CUI). The Supplier is responsible for complying with the specific clauses of this document that have been invoked by the Purchase Order. These requirements may be in addition to other contractual requirements identified elsewhere in the Purchase Order. The Supplier is responsible for passing these requirements down to all subcontracts at any tier, to the extent necessary, to ensure the Supplier's compliance with the requirements.

References

(a) NIST SP 800-171, Revision 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
(b) NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
(c) NIST SP 800-88, Revision 1, Guidelines for Media Sanitization

Note: version of the issued document in effect at the time the solicitation is issued or as authorized by the Buyer.

Definitions

1. *Adequate Security* – protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

2. *Controlled Unclassified Information (CUI)* – Information created for or on behalf of the Government that requires safeguarding and/or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended. Controlled Unclassified Information includes but is not limited to Official Use Only (OUO) Information and Personally Identifiable Information (PII). Refer to the National Archives and Records Administration (NARA) CUI Registry (https://www.archives.gov/cui) for additional information.

3. *Data at Rest* – Data at rest refers to data stored on specific components of information systems (e.g., storage devices) or on removable media.

4. *Data in Transit* – Information that is transmitted outside the system boundary or physical control of an organization (note: common transmission methods include: email, file transfers, data exchange web portals and web-based collaboration tools).

5. *Public Information* – Unclassified information created in support of this procurement which has been reviewed and approved by Fluor Marine Propulsion (FMP) for public release.

6. *Unclassified Information Not Approved for Public Release*– Unclassified Information that is generated or acquired in support of the Naval Nuclear Propulsion Program that discloses unique Naval Reactors technologies or processes, designs, analysis, test methods, or Program direction, and (at a minimum) may not be released without obtaining proper approval from FMP.

Clause 1 – General Security Requirements

1.1 Baseline Security Requirements

All Supplier information systems processing and/or storing information in support of the performance of the contract shall be compliant with the following baseline security requirements.

1.1.1 Public Information – Systems that are used to process public information require no specific baseline security requirements.

1.1.2 Unclassified Information Not Approved for Public Release– Systems that are used to process Unclassified Information Not Approved for Public Release require no specific baseline security requirements, but shall provide adequate security on information systems to protect information from public release.

1.1.3 Controlled Unclassified Information (CUI) – Systems that are used to store and/or process CUI shall be subject to the security requirements defined in Reference (a) available via the Internet at http://dx.doi.org/10.6028/NIST.SP.800-171. Note: version of the issued document in effect at the time the solicitation is issued or as authorized by the Buyer.

1.2 General Protection Requirements for CUI

The Supplier may designate specific information systems or system components for the processing, storage, or transmission of CUI in an effort to limit the scope of the CUI security requirements to those particular information systems. Isolation of CUI into its own security domain by applying architectural design principles or concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices) may be the most cost-effective and efficient approach to satisfy the requirements identified in Reference (a) and protect the confidentiality of CUI. Security domains may employ physical separation, logical separation, or a combination of both. This approach can: (i) reasonably provide adequate security for the CUI; and (ii) avoid increasing the security posture to a level beyond which it typically requires for protecting core business operations and assets. The Supplier may choose to use the same CUI infrastructure for multiple government contracts or agreements, as long as the CUI infrastructure meets the safeguarding requirements for all CUI-related contracts/agreements.

Clause 2 – Technical Security Requirements

2.1 Data at Rest Encryption

The confidentiality of data stored on information systems shall be protected. Data at rest refers to electronic information stored on specific components of information systems (e.g., storage devices) or on removable media. The following requirements are applicable for the respective information categories:

2.1.1 Public Information – Systems that are used to process public information require no additional security requirements for encryption of data at rest.

2.1.2 Unclassified Information Not Approved for Public Release– Systems that are used to process Unclassified Information Not Approved for Public Release require no additional security requirements for encryption of data at rest.

2.1.3 Controlled Unclassified Information – Systems that are used to process CUI shall ensure that data at rest is encrypted with a FIPS 140-2 certified encryption solution to protect the confidentiality and integrity of the information. This includes all CUI data on non-volatile memory (including, but not limited to: magnetic hard drive, solid state drives, flash memory, camera memory, laptops, copiers, MFDs, CDs, DVDs, Blu-Ray discs). CUI Data that are not encrypted to these standards shall be treated, handled, and protected as unencrypted data. CUI data in access restricted storage areas directly supporting servers is exempt from this requirement. All CUI data at rest on removable media shall be encrypted with FIPS 140-2 certified encryption solution.

2.2 Data in Transit Encryption

The confidentiality of transmitted information from information systems shall be protected. Data in transit refers to information that is transmitted outside the system boundary or physical control of an organization Protection requirements apply to both internal and external networks and all types of information system components from which information can be transmitted (e.g., clients, servers, mobile devices, printers, multifunction devices, etc.). The following requirements are applicable for the respective information categories:

2.2.1 Public Information – Systems that are used to transmit public information require no additional security requirements for encryption of data at rest.

2.2.2 Unclassified Information Not Approved for Public Release– Systems that are used to transmit Unclassified Information Not Approved for Public Release shall ensure that data in transit is encrypted with a FIPS 140-2 certified encryption solution to protect the confidentiality and integrity of the information.

2.2.3 Controlled Unclassified Information – Systems that are used to transmit CUI (e.g. email, file transfers, collaboration tools, etc.) shall ensure that data in transit is encrypted with a FIPS 140-2 certified encryption solution to protect the confidentiality and integrity of the information.

2.3 Data Destruction

Unless otherwise notified, upon successful completion of the contract, the Supplier shall ensure that all information and data associated with the contract is deleted and take action to ensure that no data remains on the Supplier’s information systems and/or networks. All backups maintained (offline) by the respective Supplier containing information and data associated with the contract must also be deleted. The Supplier shall produce a completed certification of non-possession that all data has been deleted or made logically inaccessible by “purging” all data on devices prior to decommissioning, disposal, reuse, or transfer, in accordance with Reference (c). Note that when there is any doubt to the success of the cleared or purged process, the storage device must be destroyed. Devices that are unable to be cleared or purged must be physically destroyed, as defined in Reference (c). The Supplier remains responsible for sanitizing or destroying all storage devices that held Buyer information and data at the hardware's end-of-life. The Supplier may not reuse or dispose of storage hardware until all Buyer data has been successfully removed.

2.4 Data Spills

Data spills involving information associated with the contract shall be immediately reported to the Buyer and remediated or "cleaned" by sanitizing affected hardware to ensure that reconstruction of spilled data is impossible or impractical. Upon discovery of a data spill, sanitization methods must at a minimum be conducted using a process that is compliant with Reference (c).

2.5 Incident Response/Breach Notification

The Supplier shall notify the Buyer of any security relevant incident within eight (8) hours of discovery (for events involving information associated with the contract). The effective execution plan for incidents within each stage of the incident handling process: detection/analysis, notification, containment, eradication and recovery shall be documented by the Supplier using organizationally defined procedures.

Clause 3 – Administrative Requirements

3.1 Obtaining Concurrence for CUI (Information System Processing and Storing)

Suppliers requesting Buyer concurrence for processing and storing CUI on information systems shall complete the following documentation and submit to the Buyer within 30 days of contract placement:

□ Completed copy of the Naval Reactors Program – DFARS 252.204-7012 System Security Plan, (available upon request) documenting compliance with requirement 3.12.4 of reference (a), and assertion to applicable security controls identified in references (a) and (b).

□ Copy of a Network Topology/Data Flow Diagrams that provide a pictorial view of information systems and their respective interconnections (e.g. system components to include: servers, clients, printers, switches, routers), externally connected information systems/components, the logical flow of data protocols between information system components and those associated with interconnections.

□ Copy of any Plans of Actions and Milestones (POAMs) for implementing reference (a) requirements not met at the time of production use of the system to processes and/or store CUI.

Concurrence for processing and storing CUI on information systems is assumed (subject to Buyer comments) upon submission of the aforementioned documentation. Significant changes to the system and/or details of implementation which affect controls required for CUI protections necessitate Buyer notification by the Supplier via updating of the previously submitted supporting documentation.

3.2 Contract Completion

Upon completion of the contract, the Supplier shall ensure that all Buyer data is deleted in accordance with requirements specified in paragraph 2.3. The Supplier shall sign a “Certification of Removal of Buyer Data from Information Systems” declaring that all Buyer data has been irretrievably removed from all Supplier information systems.