Control and Protection of Unclassified Information Not Approved for Public Release

Revision 08/2021

Unclassified Information Not Approved for Public Release is any information 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 Fluor Marine Propulsion (FMP). The Supplier may only exchange this Information with FMP and/or organizations and individuals who are authorized employees of suppliers with whom FMP or the Supplier maintains an established contractual relationship (Note: the controls prescribed within this document only apply to Unclassified Information Not Approved for Public Release. Additional protection requirements for Official Use Only, Unclassified Controlled Nuclear Information or Unclassified Naval Nuclear Propulsion Information are provided separately from this document). Regardless of the performer of the work, the Supplier is responsible for compliance with the protection requirements for Unclassified Information Not Approved for Public Release. 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. The Supplier shall ensure that the following minimum protection requirements are followed:

1. Protection in Use. Reasonable precautions must be taken to prevent access to documents that contain Unclassified Information Not Approved for Public Release associated with this contract by persons who do not require the information to perform their jobs or other authorized activities (e.g., don't read a document in a public place, such as a cafeteria, on public transportation, etc.).

2. Protection in Storage. Documents associated with this contract that contain Unclassified Information Not Approved for Public Release may be stored in unlocked receptacles such as file cabinets, desks, or bookcases when Government or Government-contractor internal building security is provided during nonduty hours. When such internal building security is not provided, comparable measures should be taken, such as storing the documents in a locked room or other locked receptacle (e.g., a locked file cabinet, desk, bookcase, or briefcase).

3. Reproduction. Documents associated with this contract that contain Unclassified Information Not Approved for Public Release may be reproduced without the permission of the originator to the minimum extent necessary to carry out official activities. Copies must be protected in the same manner as originals. Copy machine malfunctions must be cleared and all paper paths checked for papers. Excess paper must be destroyed as described below.

4. Destruction. Documents associated with this contract that contain Unclassified Information Not Approved for Public Release must be destroyed by using a strip-cut shredder that produces strips no more than 1/4-inch wide or by any other means that provides a similar level of destruction as approved by the local security office. The decision to dispose of any document containing Unclassified Information Not Approved for Public Release must be consistent with the policies and procedures for records disposition.

5. Requirements for Information Systems. Suppliers must ensure that information systems used to process, store and transmit Unclassified Information Not Approved for Public Release are protected from unauthorized access. The following requirements are provided:

a. Data in Transit. Transmission of Unclassified Information Not Approved for Public Release via the Internet is subject to interception. As a result, unencrypted transmission of Unclassified Information Not Approved for Public Release via the Internet must be considered a public release of information and is therefore not authorized unless that data in transit is encrypted with a FIPS 140-2 certified encryption solution to protect the confidentiality and integrity of the information. This includes all Unclassified Information Not Approved for Public Release that is transmitted outside the system boundary or physical control of an organization (e.g. via email, file transfers,

web portals and Internet collaboration tools). Note: Unclassified Information that has been approved for public release requires no protective measures (e.g. encryption) when transmitted.

b. Email Communications. Internet based email communications that originate from FMP and contain Unclassified Information Not Approved for Public Release is securely encrypted (utilizing a FIPS 140-2 certified encryption solution) and includes the following disclaimer statement:

"This email contains information that has not been approved for Public Release and may only be sent to those authorized to receive such information as defined per contract or other formal agreement."

Suppliers who receive email from FMP personnel that contains Unclassified Information Not Approved for Public Release must ensure that when replying to and/or forwarding an e-mail containing Unclassified Information Not Approved for Public Release, that the information is protected (e.g. encrypted utilizing a FIPS 140-2 certified solution) when transmitted.

c. Data at Rest. Data at rest refers to data stored on specific components of information systems (e.g., storage devices) or on removable media. Systems used to process Unclassified Information Not Approved for Public Release require no additional security requirements for encryption of data at rest.

d. Data Destruction. Upon successful completion of the contract, the Supplier shall ensure that all information and data associated with the contract is deleted and 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. Devices that are unable to have data deleted must be physically destroyed. The Supplier maintains responsibility for sanitizing or destroying all 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.