CYBERSECURITY CDI/CUI SAFEGUARDS STATEMENT

IT systems owned or controlled by federal contractors like Trident must be compliant with safeguards required by the U.S. DoD, NASA and GSA relative to Covered Defense Information (CDI) and Controlled Unclassified Information (CUI).

RATIONALE:

Under a joint Department of Defense (DoD), NASA, and General Services Administration (GSA) rule virtually all future federal contracts may require contractors to implement a set of cybersecurity measures to attain the "basic safeguarding" of contractor systems that process, store, or transmit a newly defined category of "federal contract information." The result is that many IT systems owned or controlled by federal contractors will need to be compliant with the rules set of required safeguards. Controls mandated by the rule for covered contractor systems include limiting information system access to the types of transactions and functions that authorized users are permitted to execute; monitoring, controlling, and protecting organizational communications. Once a contractor or subcontractor accepts a contract containing FAR 52.204-21, it must comply with the following 15 (fifteen) safeguarding controls:

1. Limit access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

2. Limit information system access to the types of transactions and functions that authorized users are allowed to execute.

3. Verify and control/limit connections to and use of external information systems.

4. Control information posted or processed on publicly accessible information systems.

5. Identify information system users and processes action on behalf of users or devices.

6. Authenticate (or verify) the identities of users, processes, or devices prior to allowing access to an information system.

7. Sanitize or destroy information system media containing Federal contract information before disposal or release for reuse.

8. Limit physical access to organization information systems, equipment, and operating environments to authorized individuals.

9. Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

10. Monitor, control, and protect organizational communications at external boundaries and key internal boundaries of the information systems.

11. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

12. Identify, report, and correct information and information system flaws in a timely manner.

13. Provide protection from malicious code at appropriate locations within organizational information systems.

14. Update malicious code protection mechanisms when new releases are available.

15. Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

POLICY STATEMENT:

PURPOSE:

The purpose of this policy is to ensure that Trident Maritime Systems (TMS) maintains a controlled environment (BOTH Physical and Electronic) in the handling, storing and transmission of Covered Defense Information (CDI) and Controlled Unclassified Information (CUI)

- Covered Defense Information (CDI) means unclassified controlled technical information

- The CUI registry identifies the categories and sub-categories of protected Government information

    - 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

    - Examples of Controlled Technical Information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets,

studies and analyses and related information, and computer software executable code and source code

- Export Control is defined as 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

- All CDI/CUI should be marked as such. A description of such information can be found in the Appendix A CDI – Document Types

- Any CDI/CUI that Trident creates must be treated in accordance with this policy/procedure

- The receipt of Controlled Information is limited to company associates who have been approved as Approved Recipients (AR) of Controlled Information

- The creation of CDI/CUI by Trident can only be done by an AR

- Approved Recipients submissions are communicated to IT by senior management who are empowered to do so. Such senior management will be approved by Executive Management

- The sharing of Controlled information is performed by Approved Recipients

- Controlled information can only be shared with Approved Recipients and 3rd parties who have certified themselves as DFARS compliant

- 3rd Parties who receive controlled information must provide Trident with a current signed Certification of Safeguarding Covered Defense Information and Cyber Reporting document prior to receiving Controlled Information

- Approved Recipients are required to read and understand this document and its references and to certify as such by signing the Approved Recipient Certification document, prior to being approved

- Controlled Information is stored in a Secured File Server accessible only to Approved Recipients

- Approved Recipients are required to use Multi-Factor Authentication and encrypted hard drives where they are accessing electronic information

- Approved Recipients who do not access electronic information do not require to have Multi-factor authentication, but are required to safeguard all hard copy documents in a secure location. The distribution and handling of hard copy must be recorded in a log which will be submitted to IT

- The transmission of controlled information is effected using Trident's Citrix ShareFile or the 3rd Party's secure encryption method if agreed upon

- Controlled information should NOT be shared via any electronic method other than aforementioned. Any other methods of sharing must be approved by Information Technology for logging / tracking purposes

- Approved ARs are only authorized to access controlled information required to perform their function. ARs can only share controlled information with other ARs on the AR/ 3rd party approved list maintained by IT, on a need to know basis

PROCEDURES:

1. **Approved Recipient set up (Permission to Receive, Store/Retrieve and Transmit controlled information)**

    a. Senior Management submits the Approved Recipient Certification document, Appendix B to Human Resources

    b. Human Resources validates that the associate can indeed access controlled information due to nationality or other such type restrictions and then forwards the document to IT

    c. Information Technology grants appropriate permissions and configures a fob (smart card technology) for each AR if they need to access electronic information

    d. Information Technology encrypts the AR's hard drive

    e. IT adds the AR to the AR/ 3rd party approved list

2. **Approved 3rd Party set up (Permission to Receive, Store/Retrieve and Transmit controlled information)**

    a. Purchasing or other others secure a signed copy of the "Certification of Safeguarding Covered Defense Information and Cyber Incident Reporting" document and submit it to Senior Management, Appendix C for approval and forwarding to IT

b. IT adds the 3rd Party to the AR/ 3rd party approved list

3. Receipt and Storing of Controlled Information from 3rd Parties

a. 3rd Party Sender notifies Trident in writing that they want to share controlled information

b. Trident and 3rd Party Sender agree in writing on the method of secure transmission (e.g. Citrix ShareFile)

i. Email and Email attachments are NOT an acceptable means of receiving controlled information and is not authorized

ii. Hard copy documents, including faxes, are NOT an acceptable means of receiving controlled information documents and is not authorized

c. Trident notifies Sender of the AR contact name to receive the controlled information

d. AR receives the controlled information and reviews it for appropriate markings

i. Banner Marking is mandatory at the top of the page denoting CDI/CUI

ii. All CDI/CUI must indicate the agency of designation (a best practice is also to include the contact information of the agency)

iii. Archives.gov Markings Introduction: https://www.archives.gov/files/cui/documents/marking-introduction-20170906.pdf

iv. If the controlled information is unmarked the AR will notify the Sender immediately

e. AR stores the controlled information document(s) on the Secure File Server

f. AR enters the transaction in the Controlled Information log

g. Security Information and Event Management (SIEM – pronounced SIM) Reports are produced, reviewed and compared to the Controlled Information log for approved recipient control

4. **Retrieval of Controlled Information from the Secure File Server (CDI/CUI)**

    a. AR retrieves controlled information documents from the Secure File Server to their encrypted hard drive if necessary

    b. AR logs the retrieving of controlled information

5. **Sharing of Controlled Information (CDI/CUI) with 3rd party Receivers**

    a. AR and Receiver (Trident associate or 3rd party) agree in writing to share controlled information

    b. AR and Receiver agree in writing on the method of secure transmission (e.g. Citrix ShareFile)

        i. AR and receiver ensure a "Certification of Safeguarding Covered Defense Information and Cyber Reporting" form has been executed by the Receiver

    c. AR retrieves controlled information documents from the Secure File Server

    d. AR logs the retrieving of controlled information

    e. AR transmits the controlled information via the agreed to secure method

        i. Email and Email attachments are NOT an acceptable means of sending controlled information documents and is not authorized

        ii. Hard copy documents, including faxes, are NOT an acceptable means of sending controlled information documents and is not authorized

    f. AR enters the transaction in the Controlled Information log

    g. Security Information and Event Management (SIEM – pronounced SIM) Reports are produced, reviewed and compared to the Controlled Information log for approved recipient control

6. **Sharing of Controlled Information (CDI/CUI) with other Approved Recipients**

a. Prior to sharing controlled information internally, the AR ensures that the receiving AR is on the AR/ 3rd party approved list

b. AR enters the transaction in the Controlled Information log if hard copy sharing is involved

7. Printing and safeguarding hardcopy controlled information

a. AR prints controlled information to a secure printer and retrieves the hard copy immediately

b. AR ensures that the hard copy is kept in his control or stored in a secure area

8. Creation and Storage of Controlled Information (CDI/CUI) by Trident

a. AR creates a document that may be considered CDI/CUI

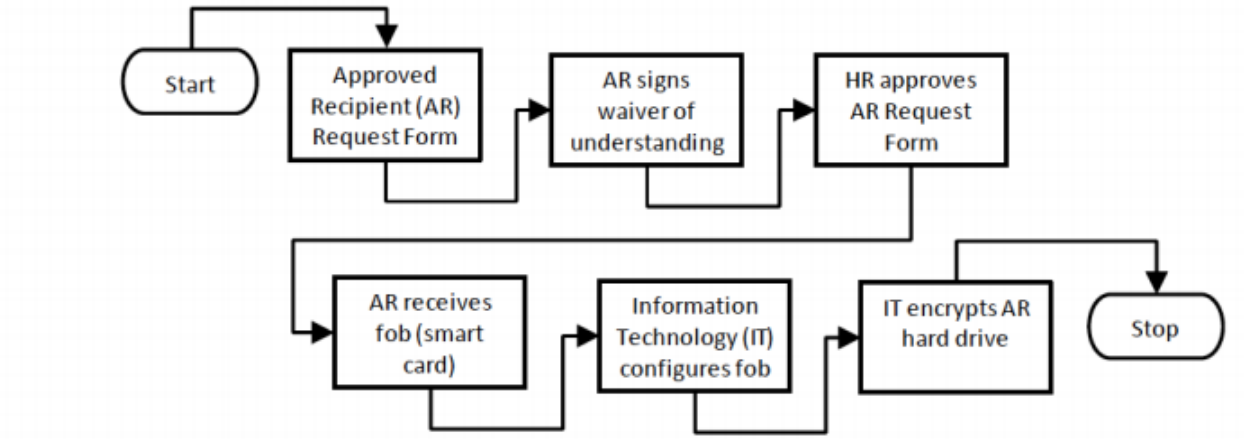
b. AR marks the document as CDI/CUI and saves it to the Pending Classification area on the Secure File Server

c. AR notifies another AR who validates that the document is indeed CDI/ CUI and that it is marked correctly

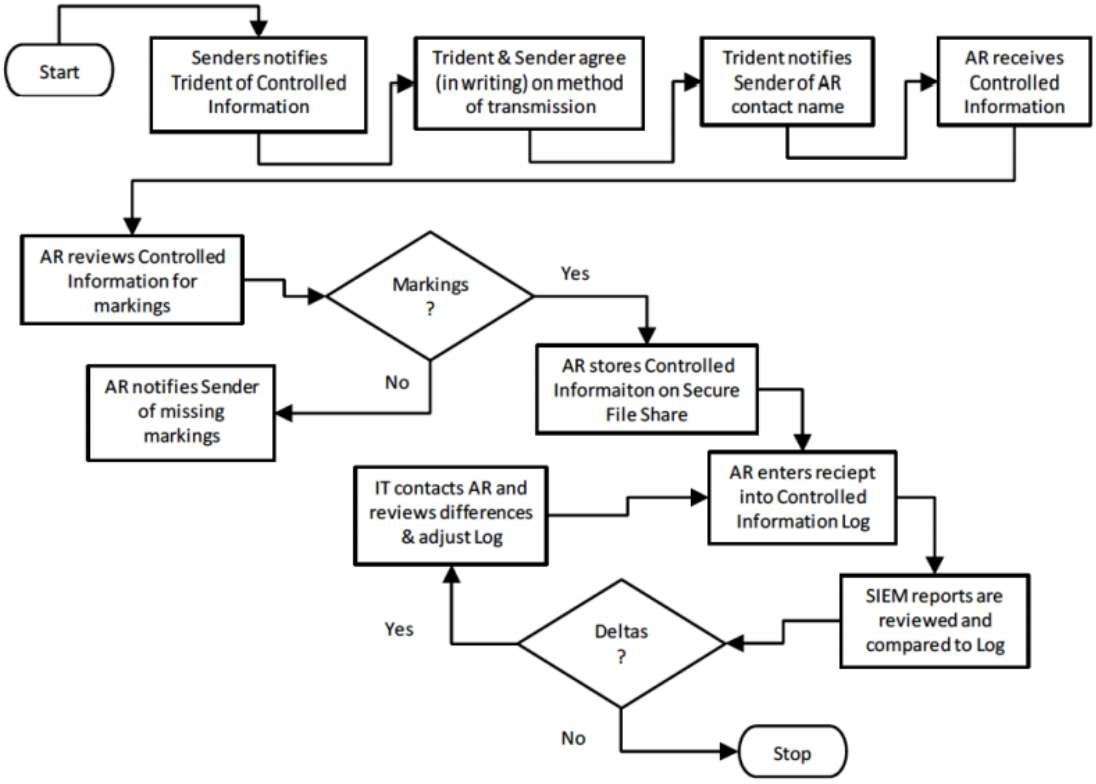
d. AR moves the document to its permanent location on the Secure File Server

PROCESS MAPS:

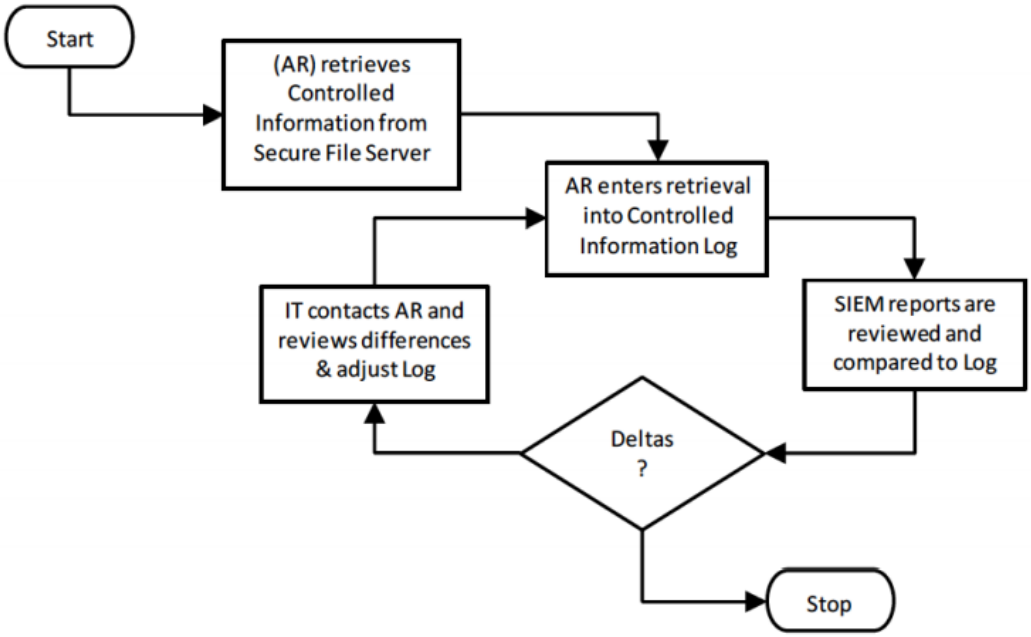
1. Approved Recipient



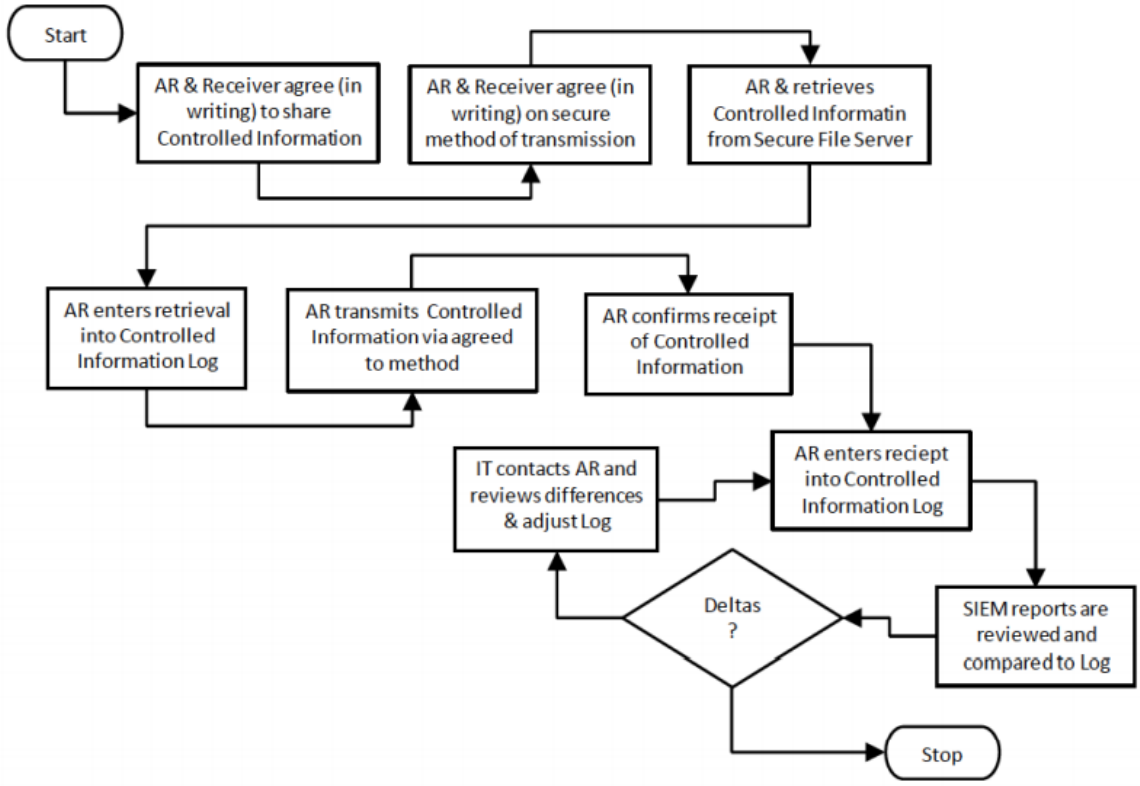
2. Receipt and Storing of Controlled Information



3. Retrieval of Controlled Information



4. Sharing of Controlled Information



GLOSSARY

- **CONTROLLED UNCLASSIFIED INFORMATION (CUI**) – Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see definition above) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways:

    - Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic

    - Requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified

    - Requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.

- **COVERED DEFENSE INFORMATION (CDI)** – Unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/ registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies, and is:

    - Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

    - Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

- **CONTROLLED TECHNICAL INFORMATION (CTI)** – 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 is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions.

"Technical Information" means: technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

- **APPROVED RECIPIENT (AR)** – Trident associate that has been approved to receive, store and transmit documents containing controlled information.

- **3RD PARTY RECIPIENT** – 3rd party who has provided Trident with a Certification of Safeguarding Covered Defense Information and Cyber Incident Reporting document.

- **SIEM** – Security Information and Event Management (pronounced SIM) is an approach to security management that seeks to provide a holistic view of an organization's information technology security.

- **EXPT** – or Export Controlled; 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 the munitions list; license applications; and sensitive nuclear technology information. Further information: https://www.archives.gov/cui/registry/category-detail/export-control.html

- **SSEL** – or Source Selection; Refers to the process of evaluating a competitive bid or proposal to enter into a Government procurement https://www.archives.gov/cui/registry/categorydetail/source-selection

APPENDIX A

*This list is not limited to only these types of documents.

Document Type	CDI	CUI	CTI	EXPT	SSEL	None	SB Notes
RFP/RFQ	X	X			X		*Usually public information, but could contain CUI. Depends on Gov verbiage in RFP/RFQ*
Specs	X	X	X				*If the specs are for the client deliverable, per the contract.*
Proposal	X	X	X		X		*If the proposal lists client deliverables.*
Pricing					X		*Could fall under Source Selection.*
Drawings (uncontrolled/not licensable)	X	X	X				*If the drawings are for the client deliverable, per the contract.*
Bill of Materials (BOM's)							
Work Instructions	X	X	X				*Tech Manuals/Work Instructions can fall under the CTI Subcategory.*
Test Reports	X	X	X				
Licensable Data (EAR/ITAR)	X	X		X			*Would fall under Export Control subcategory of CUI.*
Contract T/C's etc.	X	X			X		*If it lists Gov information, it would be CDI/CUI. If it's more vague and just lists "services/deliverables will be complete by 12/15/2017 date," it would not be CDI/CUI.*
Delivery destinations and dates					X		*None, unless it has specific deliverable information, per the client.*
Supplier Information (single source/competitive/location [countr	X	X		X			*Potentially falls under Export Control subcategory of CUI.*
Purchase Orders					X		*None, unless it has specific deliverable information, per the client.*
General maintenance data	X	X	X	X			*Who Owns it? If it's a deliverable to the Gov, it's CUI.*
Repair Manual, CMM, etc.	X	X	X				
Maintenance Instructions for Government Property	X	X	X				*Anything your company uses that is Government property will be CDI/CUI, and potentially CTI.*
Xray	X	X		X			

SB: Other document types will depend on the work performed/delivered to the Gov. If there is ever any concern, always ask the Gov contract office you're working with, or the Prime POC.

APPENDIX B

CDI APPROVED RECIPIENT CERTIFICATION

In the course of your duties you are required to access Covered Defense Information (CDI).

In order to access CDI, you must agree to handle the CDI in accordance with the requirements of the DFARS clause and in accordance with Trident's applicable policies and procedures.

In addition, you are required to read and understand the following documents and sign this document to indicate that you have done so.

In addition to any general required employee training, the following documents are provided to you to ensure that you are familiar with your responsibilities as an Approved Recipient of CDI. The documents that have been provided to you are:

- The CDI/CUI Policy and Procedure effective 12/31/17
- The Corporate Information Technology Policy

By the signing below you certify that you have read and understand the responsibilities stated in the policies and procedures referred to above.

Associate Name (Printed) _____

Associate Signature _____

Human Resources

Name/Signature _____

Manager Name /Signature_____

Date

APPENDIX C

CERTIFICATION OF SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

You (Seller-offeror) are receiving this certification form because you may receive Covered Defense Information (CDI) subject to the requirements of DFARS 252.204-7012, Safeguarding Covered Defense Information (CDI) and Cyber Incident Reporting (the "DFARS clause"), in support of bid and proposal activities of Trident Maritime Systems, LLC.

In order to receive CDI, you must agree to handle the CDI in accordance with the requirements of the DFARS clause. If you are selected as a subcontractor/vendor/ supplier to Trident Maritime Systems, LLC under a related U.S. Government contract, the subcontract is expected to contain the DFARS clause as a mandatory flow down. Should you not receive CDI, then the requirements spelled out in this memorandum are not applicable to you.

The DFARS clause requires that all contractors at every tier under a government prime contract implement "adequate security measures" (as defined in the DFARS clause) to safeguard CDI, which is defined to include unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies.

The DFARS clause also requires that contractors and subcontractors report to https://dibnet.dod.mil/portal/intranet/ within 72 hours of discovery certain "cyber incidents" that result in an actual or potentially adverse effect on CDI.

To submit such reports, you must acquire and maintain a DoD-approved medium assurance certificate. Information on obtaining a DoD-approved medium assurance certificate is available at: http://iase.disa.mil/pki/eca/Pages/index.aspx or https://www.identrust.com.

You agree to the following notification requirements as an express condition of receiving CDI from Trident Maritime Systems, LLC:

- Within 30 days of award of an Order from Trident Maritime Systems, LLC, you agree to notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, with a copy to Trident Maritime Systems authorized representative, of any security requirements specified by NIST SP 800-171 not implemented at the time of Order award.

- You agree to notify Trident Maritime Systems, LLC in writing when submitting any request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, for consideration by the DoD CIO.

- You agree to immediately inform Trident Maritime Systems, LLC in writing if, after the date this certification was executed, there is any change in your company's circumstances that causes this certification to be untrue, inaccurate, or misleading.

CERTIFICATION

By the signature of its authorized representative below, Seller-offeror certifies that either (i) it has implemented adequate security as required by the DFARS Clause on its information systems that, at a minimum, complies with the security requirements of the current revision to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, OR (ii) it is in the process of and will complete implementation of adequate security as soon as practical, but not later than December 31, 2017. If Seller-offeror is not selected as a subcontractor to perform the work for which it received the CDI, Seller-offeror agrees to dispose/destroy any CDI it received from Trident Maritime Systems, LLC in a manner consistent with the requirements of the DFARS clause.

Company Name of Seller-Offeror_____

Company Name of Seller-Offeror_____

Name of Authorized Representative (Type)_____

Title of Authorized Representative (Type)_____

Signature_____

Date