5. CONTRACT BILLING: The payment office shall make payment using the ACRN funding of the line item being billed. Contractor billings submitted for payment shall identify the specific accounting classifications cited in this contract. The Contractor shall submit billings by Line Item, Sub Line Item, and ACRN level as identified on the Financial Accounting Data Sheet(s) attached to this contract. Billings submitted to the paying offices that do not identify billing amounts by the ACRN level will be returned to the Contractor for proper identification.

6. PROGRESS REPORTS: The contractor will provide Progress Reports at the SubCLIN level and shall provide progress to the Project Manager at the Weekly Progress Meetings with the Government. **NOTE**: This is not the same progress as the total progress; however, the SubCLINs will be equal to the total delivery order progress.

CLAUSES INCORPORATED BY REFERENCE

52.245-1	Government Property	SEP 2021
252.245-7003	Contractor Property Management System Administration	JAN 2025
252.245-7005	Management and Reporting of Government Property	JAN 2024

CLAUSES INCORPORATED BY FULL TEXT

252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (MAY 2024)

(a) Definitions. As used in this clause--

Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

Contractor attributional/proprietary information means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

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. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

Covered contractor information system means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

Covered defense information means 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 Governmentwide policies, and is--

(1) 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

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

Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

Forensic analysis means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Malicious software means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

Media means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

Operationally critical support means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

Rapidly report means within 72 hours of discovery of any cyber incident.

Technical information means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data--Other Than Commercial Products and Commercial Services, regardless of whether or not the clause is incorporated in this solicitation or contract. 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.

(b) Adequate security. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an information technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.

(ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at https://csrc.nist.gov/publications/sp800) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii)(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

(C) If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/documents-templates/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

(c) Cyber incident reporting requirement.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall--

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify

compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.

(2) Cyber incident report. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at https://dibnet.dod.mil.

(3) Medium assurance certificate requirement. In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.

(d) Malicious software. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(e) Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) DoD safeguarding and use of contractor attributional/proprietary information. The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) Use and release of contractor attributional/proprietary information not created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD--

(1) To entities with missions that may be affected by such information;

(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(3) To Government entities that conduct counterintelligence or law enforcement investigations;

(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or

(5) To a support services contractor (“recipient”) that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) Use and release of contractor attributional/proprietary information created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) Other safeguarding or reporting requirements. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) Subcontracts. The Contractor shall--

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial products or commercial services, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to--

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

(End of clause)

C-204-H001 USE OF NAVY SUPPORT CONTRACTORS FOR OFFICIAL CONTRACT FILES (NAVSEA) (OCT 2018)

(a) NAVSEA may use a file room management support contractor, hereinafter referred to as "the support contractor", to manage its file room, in which all official contract files, including the official file supporting this procurement, are retained. These official files may contain information that is considered a trade secret, proprietary,

business sensitive or otherwise protected pursuant to law or regulation, hereinafter referred to as “protected information”. File room management services consist of any of the following: secretarial or clerical support; data entry; document reproduction, scanning, imaging, or destruction; operation, management, or maintenance of paper-based or electronic mail rooms, file rooms, or libraries; and supervision in connection with functions listed herein.

(b) The cognizant Contracting Officer will ensure that any NAVSEA contract under which these file room management services are acquired will contain a requirement that:

(1) The support contractor not disclose any information;

(2) Individual employees are to be instructed by the support contractor regarding the sensitivity of the official contract files;

(3) The support contractor performing these services be barred from providing any other supplies and/or services, or competing to do so, to NAVSEA for the period of performance of its contract and for an additional three years thereafter unless otherwise provided by law or regulation; and,

(4) In addition to any other rights the contractor may have, it is a third party beneficiary who has the right of direct action against the support contractor, or any person to whom the support contractor has released or disclosed protected information, for the unauthorized duplication, release, or disclosure of such protected information.

(c) Execution of this contract by the contractor is considered consent to NAVSEA's permitting access to any information, irrespective of restrictive markings or the nature of the information submitted, by its file room management support contractor for the limited purpose of executing its file room support contract responsibilities.

(d) NAVSEA may, without further notice, enter into contracts with other contractors for these services. Contractors should enter into separate non-disclosure agreements with the file room contractor. Contact the Procuring Contracting Officer for contractor specifics. However, any such agreement will not be considered a prerequisite before information submitted is stored in the file room or otherwise encumber the government.

(End of text)

C-223-H004 MANAGEMENT AND DISPOSAL OF HAZARDOUS WASTE (NAVSEA) (MAY 2023)

(a) General

(1) The Contractor shall comply with the Resource Conservation and Recovery Act (RCRA), the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (CERCLA), 10 U.S.C. 8681 and all other applicable Federal, State and local laws, codes, ordinances and regulations for the management and disposal of hazardous waste.

(2) Nothing contained in this special contract requirement shall relieve the Contractor from complying with applicable Federal, State, and local Laws, codes, ordinances, and regulations, including obtaining licenses and permits, giving notices and submitting reports, in connection with hazardous waste management and disposal in the performance of this contract. Nothing contained herein shall serve to alter either party's liability or responsibility under CERCLA.

(3) Materials contained in ship systems are not waste until after removal from the system.

(b) Identification of Hazardous Wastes - 998-41-001 of this contract identifies the types and amounts of hazardous wastes that are required to be removed by the Contractor, or that are expected to be generated, during the performance of work under this contract.

(c) Generator Identification Numbers

(1) Documentation related to hazardous waste generated solely by the physical actions of ship's force or Navy employees on board the vessel shall only bear a generator identification number issued to the Navy pursuant to applicable law.

(2) Documentation related to hazardous waste generated solely by the physical actions of Contractor personnel shall only bear a generator identification number issued to the Contractor pursuant to applicable law. Regardless of the presence of other materials in or on the shipboard systems or structures which may have qualified a waste stream as hazardous, where the Contractor performs work on a system or structure using materials (whether or not the use of such materials was specified by the Navy) which by themselves would cause the waste from such work to be a hazardous waste, documentation related to such waste shall only bear a generator identification number issued to the Contractor.

(3) Documentation related to hazardous waste generated by the combined physical actions of Navy and Contractor personnel shall bear a generator identification number issued to the Contractor pursuant to applicable law and shall also cite in the remarks block a generator identification number issued to the Navy pursuant to applicable law.

(4) Notwithstanding paragraphs (c)(1) - (c)(3) above, hazardous wastes are considered to be co-generated in cases where: (a) the Contractor merely drains a system and such drainage creates hazardous waste or (b) the Contractor performs work on a system or structure using materials which by themselves would not cause the waste from such work to be hazardous waste but such work nonetheless creates a hazardous waste. Documentation related to such co-generated waste shall bear a generator identification number in accordance with the provisions of paragraph (c)(3) above.

(5) In the event of a failure by the parties to agree to the assignment of a generator identification number to any hazardous waste as set forth in paragraphs (c)(1) through (c)(4) above, the Government may direct which party or parties shall provide generator identification numbers for the waste and such number(s) shall be used on all required documentation. Any disagreement with this direction shall be a dispute within the meaning of clause of this contract entitled "Disputes" (FAR 52.233-1). However, the Contractor shall not stop any work but shall continue with performance of all work under this contract as specified in the "DISPUTES" clause.

(6) Hazardous Waste Manifests - For wastes described in (c)(2), (c)(3), and (c)(4) above (and (c)(5) as applicable), the Contractor shall sign the generator certification on the Uniform Hazardous Waste Manifest whenever use of the Manifest is required for disposal. The Contractor shall obtain concurrence with the categorization of wastes under paragraphs (c)(3) and (c)(4) above before completion of the manifest. Manifests prepared pursuant to paragraph (c)(1) above shall be presented to the techncial POC for completion after the hazardous waste has been identified.

(7) For purposes of paragraphs (c)(2) and (3) herein, if the Contractor, while performing work at a Government facility, cannot obtain a separate generator identification number from the State in which the availability will be performed, the Contractor shall notify the technical POC within 3 business days of receipt of written notification by the State. After obtaining approval, the Contractor shall use the Navy site generator identification number and insert in the remarks block the contractor generator identification number issued for the site where his main facilities are located. For purposes of paragraph (c)(1) herein, if the work is being performed at a contractor facility and the Government cannot obtain a separate generator identification number for the State, the Government shall use the Contractor site generator identification number and shall cite in the remarks block a Navy generator identification

number. In both instances described above, the Contractor shall prepare the Uniform Hazardous Waste Manifest described in paragraph (c)(6) above and present it to the technical POC for completion.

(End of Text)

C-223-W002 ON-SITE SAFETY REQUIREMENTS (NAVSEA) (OCT 2018)

(a) The contractor shall ensure that each contractor employee reads any necessary safety documents within 30 days of commencing performance at any Government facility. Required safety documents can be obtained from the respective safety office. Contractors shall notify the Safety office points of contact below to report completion of the required training via email. The email shall include the contractor employee's name, work site, and contract number.

(b) It is expected that contractor employees will have received training from their employer on hazards associated with the areas in which they will be working and know what to do in order to protect themselves. Contractors are required to adhere to the requirements of 29 CFR 1910, 29 CFR 1926 and applicable state and local requirements while in Government spaces. The contractor shall ensure that all on-site contractor work at the Government facility is in accordance with any local safety instructions as provided via the COR. The contractor shall report all work-related injuries/illnesses that occurred while working at the Government site to the COR.

(c) Contractors whose employees perform work within Government spaces in excess of 1000 hours per calendar quarter during a calendar year shall submit the data elements on OSHA Form 300A, Summary of Work Related Injuries and Illnesses, for those employees to the safety office, via the COR by 15 January for the previous calendar year, even if no work related injuries or illnesses occurred. If a contractor's injury/illness rates are above the Bureau of Labor Statistics industry standards, a safety assessment may be performed by the Safety Office to determine if any administrative or engineering controls can be utilized to prevent further injuries/illnesses, or if any additional Personal Protective Equipment or training will be required.

(d) Any contractor employee exhibiting unsafe behavior may be removed from the Government site. Such removal shall not relieve the contractor from meeting its contractual obligations and shall not be considered an excusable delay as defined in FAR 52.249-14.

(e) The Safety Office points of contacts are as follows:

Frank Walker (757) 400-0106

(End of text)

C-245-H004 INFORMATION AND DATA FURNISHED BY THE GOVERNMENT--BASIC (NAVSEA) (MAY 2019)

(a) Contract Specifications. The Government will furnish, if not included as an attachment to the contract, any unique contract specifications set forth in Section C.

(b) Contract Drawings and Data. The Government will furnish contract drawings, design agent drawings, ship construction drawings, and/or other design or alteration data cited or referenced in Section C or in the contract specification as mandatory for use or for contract performance.

(c) Government Furnished Information (GFI). GFI is defined as that information essential for the installation, test, operation, and interface support of all Government Furnished Material identified in an attachment in Section J. The Government shall furnish only the GFI identified in an attachment in Section J. The GFI furnished to the contractor need not be in any particular format. Further, the Government reserves the right to revise the listing of GFI as follows:

(1) The Contracting Officer may at any time by written order:

(i) delete, supersede, or revise, in whole or in part, data identified in an attachment in Section J; or
(ii) add items of data or information to the attachment identified in Section J; or
(iii) establish or revise due dates for items of data or information in the attachment identified in Section J.

(2) If any action taken by the Contracting Officer pursuant to subparagraph (1) immediately above causes an increase or decrease in the costs of, or the time required for, performance of any part of the work under this contract, the contractor may be entitled to an equitable adjustment in the contract amount and delivery schedule in accordance with the procedures provided for in the "CHANGES" clause of this contract.

(d) Except for the Government information and data specified by paragraphs (a), (b), and (c) above, the Government will not be obligated to furnish the Contractor any specification, standard, drawing, technical documentation, or other publication, notwithstanding anything to the contrary in the contract specifications, the GFI identified in an attachment in Section J, the clause of this contract entitled "Government Property" (FAR 52.245-1) or "Government Property Installation Operation Services" (FAR 52.245-2), as applicable, or any other term or condition of this contract.

(e) Referenced Documentation. The Government will not be obligated to furnish Government specifications and standards, including Navy standard and type drawings and other technical documentation, which are referenced directly or indirectly in the contract specifications set forth in Section C and which are applicable to this contract as specifications. Such referenced documentation may be obtained:

(1) From the ASSIST database via the internet at https://assist.dla.mil/online/start/; or
(2) By submitting a request to the

Department of Defense Single Stock Point (DoDSSP)
Building 4, Section D
700 Robbins Avenue
Philadelphia, Pennsylvania 19111-5094
Telephone (215) 697-6396
Facsimile (215) 697-9398.

Commercial specifications and standards, which may be referenced in the contract specification or any sub-tier specification or standard, are not available from Government sources and should be obtained from the publishers.

(End of Text)

C-245-H006 ADDITIONAL REQUIREMENTS RELATING TO GOVERNMENT PROPERTY (NAVSEA) (OCT 2018)

(a) For purposes of paragraph (h) of the clause entitled "Government Property" (FAR 52.245-1) in addition to those items of property defined in that clause as Government Property, the following shall also be included within the definition of Government Property:

(1) the vessel;
(2) the equipment on the vessel;
(3) movable stores;
(4) cargo; and
(5) other material on the vessel

(b) For purposes of paragraph (b) of the clause entitled "Government Property", notwithstanding any other requirement of this contract, the following shall not be considered Government Property:

(1) the vessel;
(2) the equipment on the vessel;
(3) movable stores; and
(4) other material on the vessel

(End of text)

C-245-H010 GOVERNMENT SURPLUS PROPERTY (NAVSEA) (JAN 2019)

No former Government surplus property or residual inventory resulting from terminated Government contracts shall be furnished under this contract unless such property is approved in writing by the contracting officer. The Contractor agrees that all such property shall comply in all respects with the specifications contained herein.

(End of text)