CUSTOMER CONTRACT REQUIREMENTS
A-1387
CUSTOMER CONTRACT A-1387

CUSTOMER CONTRACT REQUIREMENTS

The following customer contract requirements apply to this contract to the extent indicated below. If this contract is for the procurement of commercial items under a Government prime contract, as defined in FAR Part 2.101, see Section 3 below.

1. Prime Contract Special Provisions The following prime contract special provisions apply to this purchase order

A-1387 A-1387 .

Proprietary Data – Data Rights Assertions Table

If Seller proposal or purchase contract involves proprietary data, please complete the Proprietary Data – Data Rights Assertions Table provided by Buyer. If a table has not been provided, please request Buyer provide one.

Non-traditional Defense Contractor Warranties and Representations

If Seller is a non-traditional defense contractor, please complete the Non-traditional Defense Contractor Warranties and Representations form provided by Buyer. If form has not been provided, please request Buyer provide one.

Organizational Conflict of Interest

Please complete the Organizational Conflict of Interest Disclosure Form for this effort. If the form has not been provided, please request Buyer provide one.

Program A-1387 Security Classification Guide (SCG)

Sellers are required to comply with the A-1387 SCG's that are part of this program effort. Buyer may provide copies of A-1387 SCG documents upon request.

Data Rights

(a) For the purposes of this Article, "Parties" means the Buyer, Seller, and Government where collectively identified and "Party" where each entity is individually identified. This is a Data Rights Clause specifically tailored for this contract to address respective rights of the Government and Buyer and Seller.

(1) Definitions

(i) "Commercial Computer Software" as used in the Article is defined in DFARS 252- 227-7014(a)(1) (Jun 1995).

(ii) "Commercial Computer Software License" means the license terms under which commercial computer software and Data (as defined in this OTA) is sold or offered for sale, lease or license to the general public.

(iii) "Computer Data Base" as used in this Base Agreement, means a collection of data recorded in a form capable of being processed by a computer. The term does not include computer software.

(iv) "Computer program" as used in this Base Agreement means a set of instructions, rules, or routines in a form that is capable of causing a computer to perform a specific operation or series of operations.
(v) "Computer software" as used in this Base Agreement means computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae and related material that would enable the software to be reproduced, recreated or recompiled. Computer software does not include computer data bases or computer software documentation.

(vi) "Computer software documentation" means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide
instructions for using the software.

(vii) Reserved.

(viii) "Form, fit and function data" means technical data that describes the required overall physical, functional and performance characteristics (along with the qualification requirements, if applicable) of an item, component, or process to the extent necessary to permit identification of physically and functionally interchangeable items.

(ix) "Government purpose" means any activity in which the United States Government is a party, including cooperative agreements with international or multi-national defense organizations, or sales or transfers by the United States Government to foreign governments or international organizations. Government purposes include competitive procurement, but do not include the rights to use, modify, reproduce, release, perform, display, or disclose technical data for commercial purposes or authorize others to do so

(x) "Government purpose rights" means the rights to

(i) Use, modify, reproduce, release, perform, display, or disclose technical data within the Government without restriction; and

(ii) Release or disclose technical data outside the Government and authorize persons to whom release or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose that data for United States government purposes.

Under this Base Agreement, the period of a Government Purpose Rights license shall be no less than five (5) years. In the event that the Data subject to this Government Purpose Rights license is used to perform an additional Prototype Project during this five (5) year period, the Government Purpose Rights license
shall be extended an additional five (5) years starting from completion of the additional Prototype Project.

(xi) "Limited rights" as used in this Article is as defined in DFARS 252.227-7013(a)(14) (Feb 2 0 1 4).

(xii) "Restricted rights" as used in this Article is as defined in DFARS 252.227-7014(a)(15) (Feb 2014).

(xiii) "Specially Negotiated License Rights" are those rights to Data that have been specifically negotiated between the Government and the Buyer on behalf of the contractor/subcontractor whose proposal is selected by the Government under a Request for Prototype Proposals issued under the OT Agreement.

(xiv) "Technical data" means recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software.

(xv) "Unlimited rights" means rights to use, modify, reproduce, perform, display, release, or disclose technical data in whole or in part, in any manner, and for any purpose whatsoever, and to have or authorize others to do so.

(2) Data Categories

I) Category A is the Data developed and paid for totally by private funds or IR&D funds and it is Data to which the Seller retains all rights. Category A Data shall include, but not be limited to,

a. Data or other material provided by under this contract which was not developed in the performance of work under that project, and for which the Seller retains all rights.

b. (B) Any initial Data or technical, marketing, or financial Data provided at the onset of the project by Seller. Such Data shall be marked "Category A" and any rights to be provided under a specific Prototype Project shall be as identified in the proposal submitted and included into the issued Prototype Awards.

(II) Category B is any Data developed under this contract with mixed funding, i.e. development was accomplished partially with costs charged to indirect cost pools and/or costs not allocated under this contract, and partially with Government funding under the this contract.

(iii) Category C is any Data developed exclusively with Government funds under this contract. Research and Development performed was not accomplished exclusively or partially at private expense. Under this category,

(A) the Government will have Government Purpose Rights in Data developed exclusively with Government funds under a Prototype Project funded under this Base Agreement that is:

(i) Data pertaining to an item, component, or process which has been or will be developed exclusively with Government funds;

(ii) Studies, analyses, test data, or similar data produced for this contract, when the study, analysis, test, or similar work was specified as an element of performance;

(iii) Data created in the performance of the Base Agreement that does not require the development, manufacture, construction, or production of items, components, or processes;

(iv) Form, fit, and function data;

(v) Data necessary for installation, operation, maintenance, or training purposes (other than detailed manufacturing or process data);

(vi) Corrections or changes to technical data furnished to the Buyer by the Government;

The Government can only order such Data as is developed under the Prototype Project where the order request is made within one (1) year following Prototype Project completion or for an alternate duration specified in the Prototype Award. In the event the Government orders such Data, it shall pay Seller, directly or via the Buyer, the reasonable costs for all efforts to deliver such requested Data, including but not limited to costs of locating such Data, formatting, reproducing, shipping, and associated administrative costs.

(B) The Government shall have unlimited rights in Data that is:

(i) Otherwise publicly available or that has been released or disclosed by the Seller without restrictions on further use, release or disclosure, other than a release or disclosure resulting from the sale, transfer, or other assignment of interest in the Data to another party or the sale or transfer of some or all of a business entity or its assets to another party;

(ii) Data in which the Government has obtained unlimited rights under another Government contract or as a result of negotiations; or

(iii) Data furnished to the Government, under this contract or any other Government contract or subcontract thereunder, with-

(1) Government Purpose Rights or limited rights and the restrictive condition(s) has/have expired; or

(2) Government purpose rights and the Seller's exclusive right to use such Data for commercial purposes under such contract or subcontract has expired.

(C) However, any Data developed outside of this contract whether or not developed with any Government funding in whole or in part under a Government agreement, contract or subcontract shall have the rights negotiated under such prior agreement, contract or subcontract; the Government shall get no additional rights in such Data.

(D) Further, the Government's rights to Commercial Computer Software and Data licensed under a Commercial Computer Software License under this OTA, and the treatment of Data relating thereto, shall be as set forth in the Commercial

Computer Software License.

(iv) The Seller shall stamp all documents in accordance with this Article and that the Freedom of Information Act (FOIA) and Trade Secrets Act (TSA) apply to Data.

(3). Allocation of Principal Rights

(i) The Government shall have no rights to Category A Data.

(ii) The Government shall have immediate Government Purpose Rights to Category B or C Data upon delivery or Prototype Project completion (whichever is earlier), except that

(A) The Buyer, at the request of small business or any other than small business Seller, may request on such Seller's behalf a delay of the start of Government Purpose Rights in Category B or C Data for a period not to exceed five (5) years from Prototype Project completion. Such requests will only be made in those cases where the Seller through the Buyer has provided information from the affected actual or prospective Seller demonstrating the need for this additional restriction on Government use and shall be submitted to the USG for approval, which approval shall not be unreasonably withheld.
(B) for Article 28 (2)(iii)(C) Category C Data, the Government shall have only the rights established under prior agreements.

(C) for Article 28(2)(iii)(D) Category C Data, the Government shall only have the rights set forth in the Commercial Computer Software Data license agreement.

(iii) Data that will be delivered, furnished, or otherwise provided to the Government as specified in a specific Prototype Award funded under this contract, in which the Government has previously obtained rights, shall be delivered, furnished, or provided with the pre-existing rights, unless (a) the Parties have agreed otherwise, or (b) any restrictions on the Government's rights to use, modify, reproduce, release, perform, display, or disclose the data have expired or no longer apply.

(iv) Each Proposal submitted by the Buyer in response to a Government call for proposals under
shall include a list of the Category A, B and C Data to be used or developed if selected. Any proposal that includes information to be provided with Limited Rights, Restricted Rights, or Specially Negotiated License Rights shall include supporting detail and rationale. Rights in such Data shall be as established under the terms of this contract, unless otherwise asserted in the proposal and agreed to by the Government in the Prototype Award. The Buyer and USG will incorporate the list of Category A, B and C Data and the identified rights therefor in the Prototype Award.

Following issuance of a PM and subsequent CM issuance of the Prototype Award to the Government selected contractor, the Buyer & Seller shall update the list to identify any additional, previously unidentified, Data if such Data will be used or generated in the performance of the funded work. Rights in such Data shall be as established under the terms of this contract, unless otherwise asserted in a supplemental listing and agreed to by the Government.

(4). Marking of Data

Except for Data delivered with unlimited rights, Data to be delivered under this contract subject to restrictions on use, duplication or disclosure shall be marked with the following legends:

Category A use company proprietary statement.

Category B and C use legend at DFARS 252.227-7013 (f)(2).

It is not anticipated that any Category A Data will be delivered to the Government under this contract.
In the event commercial computer software and Data is licensed under a commercial computer software license under this contract a Special License rights marking legend shall be used as agreed to by the parties.

The Government shall have unlimited rights in all unmarked Data. In the event that Buyer or Seller learns of a release to the Government of its unmarked Data that should have contained a restricted legend, the they will have the opportunity to cure such omission going forward by providing written notice within three (3) months of the erroneous release.

(5). Copyright

The Seller reserve the right to protect by copyright original works developed under this Contract.. All such copyrights will be in the name of the individual Seller. The Seller hereby grants to the Buyer and U.S. Government a nonexclusive, non-transferable, royalty-free, fully paid-up license to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, for governmental purposes, any copyrighted materials developed under this agreement, and to authorize others to do so.

In the event Data is exchanged with a notice indicating that the Data is protected under copyright as a published, copyrighted work and it is also indicated on the Data that such Data existed prior to, or was produced outside of this contract, the Party receiving the Data and others acting on its behalf may reproduce, distribute, and prepare derivative works for the sole purpose of carrying out that Party's responsibilities under this Contract. or Prototype Award with the written permission of the Copyright holder.

Copyrighted Data that existed or was produced outside of this contract and is unpublished - having only
been provided under licensing agreement with restrictions on its use and disclosure - and is provided under this contract shall be marked as unpublished copyright in addition to the appropriate license rights legend restricting its use, and treated in accordance with such license rights legend markings restricting its use.

The Seller is responsible for affixing appropriate markings indicating the rights of the Government on all Data delivered under this contract.

The Government agrees not to remove any copyright notices placed on Data and to include such notices on all reproductions of the Data.

(6). Data First Produced by the Government:

As to Data first produced by the Government in carrying out the Government's responsibilities under this contract and which Data is privileged or confidential if obtained from Buyer, such Data will, to the extent permitted by law, be appropriately marked with a suitable notice or legend and maintained in confidence by the party to whom disclosed for three (3) years after the development of the information, with the express understanding that during the aforesaid period such Data may be disclosed and used by or on behalf of the Government for Government purposes only.

(7). Prior Technology

(i) Government Prior Technology: In the event it is necessary for the Government to furnish Data which existed prior to, or was produced outside of the contract, and such Data is so identified with a suitable notice or legend, the Data will be maintained in confidence and disclosed and used only for the purpose of carrying out their responsibilities under this contract. Data protection will include proprietary markings and handling, compliance, Proprietary Information, and the signing of non-disclosure agreements by subcontractors of any tier and their respective employees) to whom such Data is provided for use under the contract. Upon completion of activities under this contract, such Data will be disposed of as requested by the Government or Buyer.

(ii) n the event it is necessary to furnish the Government with Data which existed prior to, or was produced outside of the contract, and such Data embodies trade secrets or comprises commercial or financial information which is privileged or confidential, and such Data is so identified with a suitable notice or legend, the Data will be maintained in confidence and disclosed and used by the Government and such Government Contractors or contract employees that the Government may hire on a temporary or periodic basis only for the purpose of carrying out the Government's responsibilities under the contract. Data protection will include proprietary markings and handling, and the signing of nondisclosure agreements by such Government Contractors or contract employees. Seller shall not be obligated
to provide Data that existed prior to, or was developed outside of this contract to the Government.
Upon completion of activities under this contract, such Data will be disposed of as requested.

(iii) Oral and Visual Information: If information considered to embody trade secrets or to comprise commercial or financial information which is privileged or confidential is expressly disclosed orally or visually directly to the Government, the exchange of such information must be memorialized in tangible, recorded form and marked with a suitable notice or legend, and furnished to the Government within thirty (30) calendar days after such oral or visual disclosure, or the Government shall have no duty to limit or restrict, and shall not incur any liability for any disclosure and use of such information. Upon Government request, additional detailed information about the exchange will be provided subject to restrictions on use and disclosure.

(iv) Disclaimer of Liability: Notwithstanding the above, the Government shall not be restricted in, nor incur any liability for, the disclosure and use of:

(A) Data not identified with a suitable notice or legend as set forth in this Article; nor

(B) Information contained in any Data for which disclosure and use is restricted, if such information is or becomes generally known without breach of the above, is properly known to the Government or is generated by the Government independent of carrying out responsibilities under the contract, is rightfully received from a third party without restriction, or is included in data furnished, or is required to furnish to the Government without restriction on disclosure and use.

(v) Marking of Data: Any Data delivered under this contract shall be marked with a suitable notice or legend.

(8). Notwithstanding the Paragraphs in this Article, differing rights in Data may be negotiated among the Parties to each individual project on a case-by-case basis.

(9). Lower Tier Agreements

The Seller shall include this Article, suitably modified to identify the parties, in all Prototype Awards, subcontracts or lower tier agreements, regardless of tier, or experimental, developmental, or research work.

(10). Survival Rights

Provisions of this Article shall survive termination of this contract. Notwithstanding the terms of this Article, differing rights in data may be negotiated among the Parties to each individual Prototype Award on a case-by-case basis.

CYBERSECURITY AND INFORMATION PROTECTION

For the purposes of this Article, “Parties” means the Buyer, Seller, and, or, Government where collectively identified and “Party” where each entity is individually identified.

(a) Definitions applicable to this Article

"Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.
"Cloud computing," means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software- as-a-service, infrastructure-as-a-service, and platform-as-a-service.

"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.
"Parties attributional/proprietary information" means information that identifies the Parties, whether directly or indirectly, by the grouping of information that can be traced back to the Parties (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 <http://www.archives.gov/cui/registry/category- list.html>.archives.gov/cui/registry/category-list.html>
<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-

(1) Marked or otherwise identified in the Prototype Award and provided to the Parties by or on behalf of DoD in support of the performance of the Prototype Award; or

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

"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.

"Safeguarding" means measures or controls that are prescribed to protect information systems.

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013 <http://www <http://www.acq.osd.mil/dpap/dars/dfars/html/current/252227.htm>.acq.osd.mil/dpap/dars/dfars/html/ current/252227.htm <http://www.acq.osd.mil/dpap/dars/dfars/html/current/252227.htm>>; Rights in Technical Data-Noncommercial Items, regardless of whether or not the clause is incorporated in the Request for Prototype Proposal or Base Agreement. 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) Compliance with this Article is only required when the prototype award explicitly require compliance. The Government or Buyer will clearly mark solicitations where the resulting contract is anticipated to include covered defense information. In such instances, Seller's will confirm in their white paper/Proposal either compliance or requirement to comply prior to award.

(c) This article applies to the extent that prime contract or Prototype Award (PA) involves a covered contractor information system that processes, stores or transmits Covered Defense Information (CDI) as determined by the Buyer.

(1) By submission of an offer, the Seller represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see<http://d <http://dx.doi.org/10.6028/NIST.SP.800-171>x.doi.org/10.6028/NIST.SP.800-171> <http://dx.doi.org/10.6028/NIST.SP.800-171>) that are in effect at the time the solicitation is issued or as authorized by the Agreements Officer (AO).

(2) If the Seller proposes to vary from any of the security requirements specified by NIST SP 800- 171 that are in effect at the time the solicitation is issued or as authorized by the AO, the Seller shall submit to the AO through the Buyer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of why a particular security requirement is not applicable; or how an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection. An authorized representative of the DoD CIO will adjudicate Seller requests to vary from NIST SP 800- 171 requirements in writing prior to Prototype Award . Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting PA.

(3) The Seller shall indicate in its proposal whether the use of cloud computing is anticipated at any level under the resultant contract. After the award of a contract, if the Seller proposes to use cloud computing services in the performance of the contract at any level, the Seller shall obtain approval from the Buyer prior to utilizing cloud computing services.

(d) The Seller shall provide adequate security on all covered contractor information systems. To provide adequate security, the Seller shall implement, at a minimum, the following safeguarding and information security protections:

(1) The Seller shall apply the following basic safeguarding requirements and procedures:

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

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, and devices.

(vi) Authenticate (or verify) the identities of those users, processes, and devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

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

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

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

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

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

(2) 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 http://dx.doi.org/10.6028/NIST.SP.800-171), within 30 days of agreement award, of any security requirements specified by NIST SP 800-171 not implemented at the time of Prototype Award.

(3) Apply additional information systems security measures when the Buyer reasonably determines that information systems security measures 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.

(e) The Seller shall notify the DoD Chief Information Officer (CIO) via the Buyer, within thirty (30) days of Prototype Award, of any security requirements specified by NIST SP 800-171 not implemented at the time of Prototype Award.

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

(2) If the DoD CIO has previously adjudicated the Seller’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 through the Buyer to the AO when requesting its recognition under this agreement.

(3) If the Seller intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this agreement, the Seller 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/resources/documents/ <http://www.fedramp.gov/resources/documents/>>) and that the cloud service provider complies with requirements of this Article 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.

(f) When the Seller discovers a cyber incident that affects a covered contractor information system (including internal or external cloud computing services) or the covered defense information residing therein, or that affects the Seller's ability to perform the requirements of the agreement that are designated as operationally critical support and identified in the agreement, the Seller shall-

(1) 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 Seller'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 Seller's ability to provide operationally critical support; and

(2) Rapidly report cyber incidents to Buyer and to the DoD at <http://dib <http://dibnet.dod.mil/>net.dod.mil/>. <http://dibnet.dod.mil/> The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil. In order to report cyber incidents in accordance with this article, the Seller or subperformer 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 <http://iase.
<http://iase.disa.mil/pki/eca/Pages/index.aspx>disa.mil/pki/eca/Pages/index.aspx
<http://iase.disa.mil/pki/eca/Pages/index.aspx>>.

(g) When the Seller or subperformers discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to Buyer and the DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the AO. Do not send the malicious software to the AO.

(h) When a Seller discovers a cyber incident has occurred, the Seller shall preserve and protect images of all known affected information systems identified in paragraph (d)(1) of this article and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow Buyer and DoD to request the media or decline interest.

(i) Upon request by Buyer or DoD, the Seller shall provide the Buyer or DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(j) If DoD elects to conduct a damage assessment, the AO or Buyer will request that the Seller provide all of the damage assessment information gathered in accordance with paragraph (f) of this clause.

(k) The Government shall protect against the unauthorized use or release of information obtained from the Seller (or derived from information obtained from the Seller) under this Article that includes Parties attributional/proprietary information, including such information submitted in accordance with paragraph (f). To the maximum extent practicable, the Seller shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the Parties 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.

(l) Information that is obtained from the Buyer (or derived from information obtained from the Buyer) under this article 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 contract ("recipient") that is directly supporting Government activities under a contract that includes the clause at DFARS 252.204-7009 <http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm>.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm <http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm>>, Limitations on the Use or Disclosure of Third-Party PLP Reported Cyber Incident Information.

(m) Information that is obtained from the Buyer (or derived from information obtained from the Buyer) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (f) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (l) 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.

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

(o) The safeguarding and cyber incident reporting required by this article in no way abrogates the Seller’s responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable articles of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(p) Reserved

(q) Reserved

(r) The Parties shall include this Article, including this paragraph (r), in subagreements, or agreements for which subperformer performance will involve covered defense information, including subagreements for commercial items, without alteration, except to identify the parties. The Parties shall determine if the information required for subperformer performance retains its identity as covered defense information and will require protection under this article, and, if necessary, consult with the AO through the Buyer; and require subperformers to notify the Buyer (or next highertier subperformer) when submitting a request to vary from a NIST SP 800-171 security requirement to the AO, in accordance with paragraph (c)(2) of this clause; and provide the incident report number, automatically assigned by DoD, to the Buyer (or next higher-tier subperformer) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (f) of this Article.