Imprimis, Inc. Information Packet: Summary of Changes and Requirements - DFARS Cybersecurity Safeguards

Imprimis, Inc.
5755 Mark Dabling Blvd.,
Suite 250
Colorado Springs, CO 80919-2247

This Paper describes the interim changes and requirements regarding cybersecurity safeguards as prescribed in DFARS subparts:

- 204.73 - Safeguarding Covered Defense Information and Cyber Incident Reporting,
- 202.1 - Definitions,
- 239.76 - Cloud Computing, and
- 212.301(f) - Solicitation provisions and contract clauses for the acquisition of commercial items.

(This page intentionally left blank)

TABLE OF DEFINITIONS
CYBERSECURITY DFARS
SUBPARTS 204.73, 239.76, 212.301

ITEM	DEFINITION
Adequate Security	"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	"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	"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	"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	"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	"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	"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	"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	"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Malicious Software	"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	"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	"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.
Rapid Report	"Rapidly report" means within 72 hours of discovery of any cyber incident
Technical Information	"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— Noncommercial Items, 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.

(This page intentionally left blank)

SUBPART / CLAUSE	TITLE	REQUIREMENTS
204.73 (subpart)	**Safeguarding Covered Defense Information and Cyber Incident Reporting.** *Revised – Sept 21, 2015* *Revised - Oct 21, 2016*	▪ Contractors & Subcontractors must safeguard '***Covered***'[1] defense information that resides in or transits through contractor 'UNCLASSIFIED' information system. ▪ Must rapidly report incidents involving possible loss of covered data to DoD via Dibnet.dod.mil o Will include i) incident report, ii) malicious software, and iii) media ▪ Prescribes: 252.204-7008, -7009, -7012; 252.227-7013
252.204-7012 (clause)	**Safeguarding Covered Defense Information and Cyber Incident Reporting.** *Revised – Sept 21, 2015* *Revised - Dec 30, 2015* *Revised - Oct 21, 2016*	*(a.) Definitions. [Please see Table of Definitions]* *(b.) Adequate security.* ▪ Contractor will implement information systems security protections on all covered contractor 'UNCLASSIFIED' information systems ▪ If operated on behalf of the Government – for Cloud follow DFARS 252.239-7010, Cloud Computing Services - if other than Cloud as specified in contract *(Commonly CNSSI 1253)* ▪ If Contractor Covered Information System – NOT on behalf of Government … ▪ Contractor (Offeror) represents that it will implement security requirements in NIST 800-171 as soon as practical but no 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 ▪ Contractor will apply other information system security measures when the contractor reasonably determines that additional security measures are required. ▪ "Alternative but equal effective" security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection must be submitted in writing to an "authorized representative of the DoD CIO," who will "adjudicate" offeror requests. ▪ If 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 *(c.) Cyber incident reporting requirement.* ▪ Contractor will rapidly report incidents within 72 hours to both the prime contractor and DoD via http://dibnet.dod.mil ▪ Medium Assurance Certificate required *(d.) Malicious software.* ▪ When Contractor discover and isolate malicious software submit the malicious software to DoD Cyber Crime Center (DC3)-not the Contracting Officer. *(e.) Media preservation & protection.* ▪ When a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems and all relevant monitoring/packet capture data for at least 90 days *(f.) Access to additional information or equipment necessary for forensic analysis.* ▪ Upon request, Contractor will provide access to additional data and equipment for forensics *(g.) Cyber incident damage assessment activities.* ▪ If requested, Contractor will provide all damage assessment information. *(h.) DoD safeguarding and use of contractor attributional/proprietary information.* *(i.) Use and release of contractor attributional/proprietary information* ***not created by or for DoD****.* *(j.) Use and release of contractor attributional/proprietary information* ***created by or for DoD****.* *(k.) The Contractor shall conduct activities … in accordance with applicable laws and regulations.* *(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 *(m.) Subcontracts.* ▪ Contractor will include this clause on any subcontracts, or similar contractual instruments, for which subcontractor performance will involve covered defense information … including reporting. ▪ The Contractor shall— 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; 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.

(This page intentionally left blank)

252.204-7008 (provision)	**Compliance with Safeguarding Covered Defense Information Controls.** *New Addition - Aug 26, 2015* *Revised - Dec 30, 2015* *Revised - Oct 21, 2016*	▪ All contractors represent to implement NIST 800-171 as soon as practical, but no later than December 31, 2017 ▪ If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800-171 -the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of— (A) Why a particular security requirement is not applicable; or (B) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection. (ii) An authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP 800-171 requirements in writing prior to contract award. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract.
252.204-7009 (clause)	**Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.** *New Addition – Aug 26, 2015* *Revised - Dec 30, 2015* *Revised - Oct 21, 2016*	*(b.) Restrictions* ▪ The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government, and shall not be used for any other purpose. ▪ The Contractor shall protect the information against unauthorized release or disclosure. ▪ The Contractor shall ensure that its employees are subject to use and non-disclosure obligations. ▪ The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor ▪ A breach of these obligations or restrictions may subject the Contractor to— (i) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and (ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this clause. *(c.) Subcontracts.* ▪ The Contractor shall include this clause in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items, without alteration, except to identify the parties.
252.227-7013 (clause)	**Rights in Technical Data--Noncommercial Items**	▪ The Contractor grants or shall obtain for the Government the following royalty free, world-wide, nonexclusive, irrevocable license rights in technical data other than computer software documentation: o Unlimited rights if on government funds, o Government purpose rights, is mixed funds (government & private) o Limited rights if exclusively private funds.
239.76 (subpart)	**Cloud Computing.** *New Addition – Aug 26, 2015* *Revised - Oct 21, 2016*	▪ For information systems operated on behalf of the government, the contracting officer shall only award a contract to acquire cloud computing services from a cloud service provider (e.g., contractor or subcontractor, regardless of tier) that has been granted provisional authorization by Defense Information Systems Agency, at the level appropriate to the requirement, to provide the relevant cloud computing services in accordance with the Cloud Computing Security Requirements Guide (SRG) ▪ Prescribes 252.239-7009 & -7010
252.239-7009 (provision)	**Representation of Use of Cloud Computing.** *New Addition – Aug 26, 2015* *Revised – Sept 21, 2015*	▪ The Contractor will be required to provide, as a part of its offer, a Representation of Intent to use Cloud Computing Services in performance of the contract.
252.239-7010 (clause)	**Cloud Computing Services.** *New Addition – Aug 26, 2015* *Revised - Oct 21, 2016*	▪ Respresentation at time of offer or written approval by the contracting officer required before using cloud computing. ▪ The Contractor shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG) found at http://iase.disa.mil/cloud_security/Pages/index.aspx, unless notified by the Contracting Officer that this requirement has been waived by the DoD Chief Information Officer. ▪ *Subcontracts*. The Contractor shall include this clause, including this paragraph (l), in all subcontracts that involve or may involve cloud services, including subcontracts for commercial items.
212.301 (f) (clauses & provisions)	**Solicitation provisions and contract clauses for the acquisition of commercial items.** *Revised – Sept 21, 2015* *Revised – Oct 30, 2015* *Revised – Aug 2, 2016*	▪ Identifies Solicitation clauses and provisions to be included in the acquisition of commercial items. ▪ Includes cybersecurity and safeguards identified in the above clauses. ▪ Supply chain risk evaluation required (239.73)
NOTE (1)-Covered Information: Unclassified information that is i) provided to contractor by or on behalf of DoD, ii) Collected, developed, received, transmitted, used, or stored by the contractor, or [information that] falls within the following categories i) Controlled technical information, ii) Critical information (operations security), iii) Export control, iv) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls …		

(This page intentionally left blank)

DFARS Subpart 204.73

Safeguarding Covered Defense Information and Cyber Incident Reporting.

Revised – Sept 21, 2015

Revised – Oct 21, 2016

http://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm

Previously known as *"Safeguarding Unclassified Controlled Technical Information."*

www.i2ComplianceTools.com
866-471-0145

SUBPART 204.73—SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

(Revised October 21, 2016)

204.7300 Scope.

(a) This subpart applies to contracts and subcontracts requiring contractors and subcontractors to safeguard covered defense information that resides in or transits through covered contractor information systems by applying specified network security requirements. It also requires reporting of cyber incidents.

(b) This subpart does not abrogate any other requirements regarding contractor physical, personnel, information, technical, or general administrative security operations governing the protection of unclassified information, nor does it affect requirements of the National Industrial Security Program.

204.7301 Definitions.

As used in this subpart—

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

"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.

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

"Media" means physical devices or writing surfaces including, but 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.

"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-Non Commercial Items, 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.

204.7302 Policy.

(a) Contractors and subcontractors are required to provide adequate security on all covered contractor information systems.

(b) Contractors and subcontractors are required to rapidly report cyber incidents directly to DoD at http://dibnet.dod.mil. Subcontractors provide the incident report number automatically assigned by DoD to the prime contractor. Lower-tier subcontractors likewise report the incident report number automatically assigned by DoD to their higher-tier subcontractor, until the prime contractor is reached.

(1) If a cyber incident occurs, contractors and subcontractors submit to DoD—

(i) A cyber incident report;

(ii) Malicious software, if detected and isolated; and

(iii) Media (or access to covered contractor information systems and equipment) upon request.

(2) Contracting officers shall refer to PGI 204.7303-4(c) for instructions on contractor submissions of media and malicious software.

(c) Information shared by the contractor may include contractor attributional/

proprietary information that is not customarily shared outside of the company, and that

the unauthorized use or disclosure of such information could cause substantial competitive harm to the contractor that reported the information. The Government shall protect against the

unauthorized use or release of information that includes contractor attributional/proprietary information.

(d) A cyber incident that is reported by a contractor or subcontractor shall not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate security on their covered contractor information systems, or has otherwise failed to meet the requirements of the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. When a cyber incident is reported, the contracting officer shall consult with the DoD component Chief Information Officer/cyber security office prior to assessing contractor compliance (see PGI 204.7303-3(a)(3)). The contracting officer shall consider such cyber incidents in the context of an overall assessment of a contractor's compliance with the requirements of the clause at 252.204-7012.

(e) Support services contractors directly supporting Government activities related to safeguarding covered defense information and cyber incident reporting (e.g., forensic analysis, damage assessment, or other services that require access to data from another contractor) are subject to restrictions on use and disclosure of reported information.

204.7303 Procedures.

Follow the procedures relating to safeguarding covered defense information at PGI 204.7303.

204.7304 Solicitation provision and contract clauses.

(a) Use the provision at 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items.

(b) Use the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Information, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting.

(c) Use the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts solely for the acquisition of COTS items.

DFARS 252.204-7012

Safeguarding Covered Defense Information and Cyber Incident Reporting.

New Addition – Sept 21, 2015
Revised – Dec 30, 2015
Revised – Sept 21, 2016

http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012

www.i2ComplianceTools.com
866-471-0145

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016)

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.

As prescribed in 204.7304(c), use the following clause:

(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—Noncommercial Items, 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 http://dx.doi.org/10.6028/NIST.SP.800-171) 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/resources/documents/) 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 http://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 http://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 http://iase.disa.mil/pki/eca/Pages/index.aspx.

(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 items, 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)

(This page intentionally left blank)

DFARS 252.204-7008

Compliance with Safeguarding Covered Defense Information Controls.

New Addition – Aug 26, 2015
Revised – Dec 30, 2015
Revised – Oct 21, 2016

http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7008

www.i2ComplianceTools.com
866-471-0145

COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (OCT 2016)

252.204-7008 Compliance with Safeguarding Covered Defense Information Controls.

As prescribed in 204.7304(a), use the following provision:

(a) *Definitions*. As used in this provision—

"Controlled technical information," "covered contractor information system," "covered defense information," "cyber incident," "information system," and "technical information" are defined in clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

(b) The security requirements required by contract clause 252.204-7012, shall be implemented for all covered defense information on all covered contractor information systems that support the performance of this contract.

(c) For covered contractor information systems that are not part of an information technology service or system operated on behalf of the Government (see 252.204-7012(b)(2)—

(1) By submission of this offer, the Offeror 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://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 contracting officer not later than December 31, 2017.

(2)(i) If the Offeror 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 Contracting Officer, the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of—

(A) Why a particular security requirement is not applicable; or

(B) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.

(ii) An authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP 800-171 requirements in writing prior to contract award. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract.

(End of provision)

DFARS 252.204-7009

Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

New Addition – Aug 26, 2015
Revised – Dec 30, 2015
Revised – Sept 21, 2016

http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7009

www.i2ComplianceTools.com
866-471-0145

LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (OCT 2016)

252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

As prescribed in 204.7304(b), use the following clause:

(a) *Definitions*. As used in this clause—

"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.

"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 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.

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

"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.

"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-Noncommercial Items, 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) *Restrictions*. The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party's reporting of a cyber incident pursuant to DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (or derived from such information obtained under that clause):

(1) The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to clause 252.204-7012, and shall not be used for any other purpose.

(2) The Contractor shall protect the information against unauthorized release or disclosure.

(3) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.

(4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of this clause.

(5) A breach of these obligations or restrictions may subject the Contractor to—

(i) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and

(ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this clause.

(c) *Subcontracts*. The Contractor shall include this clause, including this paragraph (c), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items, without alteration, except to identify the parties.

(End of clause)

(This page intentionally left blank)

DFARS Subpart 202.1

Definitions.

New Addition – Aug 26, 2015
Revised -- Oct 30, 2015
Revised -- Oct 21, 2016

http://www.acq.osd.mil/dpap/dars/dfars/html/current/202_1.htm

SUBPART 202.1--DEFINITIONS

(Revised October 21, 2016)

202.101 Definitions.

"Authorized aftermarket manufacturer" means an organization that fabricates an electronic part under a contract with, or with the express written authority of, the original component manufacturer based on the original component manufacturer's designs, formulas, and/or specifications.

"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.

"Congressional defense committees" means—

(1) In accordance with 10 U.S.C. 101(a)(16), except as otherwise specified in paragraph

(2) of this definition or as otherwise specified by statute for particular applications—

(i) The Committee on Armed Services of the Senate;

(ii) The Subcommittee on Defense of the Committee on Appropriations of the Senate;

(iii) The Committee on Armed Services of the House of Representatives; and

(iv) The Subcommittee on Defense of the Committee on Appropriations of the House of Representatives.

(2) For use in subpart 217.1, see the definition at 217.103.

"Contract administration office" also means a contract management office of the Defense Contract Management Agency.

"Contract manufacturer" means a company that produces goods under contract for another company under the label or brand name of that company.

"Contracting activity" for DoD also means elements designated by the director of a defense agency which has been delegated contracting authority through its agency charter. DoD contracting activities are listed at PGI 202.101 (DFARS/PGI view).

"Contracting officer's representative" means an individual designated and authorized in writing by the contracting officer to perform specific technical or administrative functions.

"Contractor-approved supplier" means a supplier that does not have a contractual agreement with the original component manufacturer for a transaction, but has been identified as trustworthy by a contractor or subcontractor.

"Counterfeit electronic part" means an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

"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.

"Departments and agencies," as used in DFARS, means the military departments and the defense agencies. The military departments are the Departments of the Army, Navy, and Air Force (the Marine Corps is a part of the Department of the Navy). The defense agencies are the Defense Advanced Research Projects Agency, the Defense Commissary Agency, the Defense Contract Management Agency, the Defense Finance and Accounting Service, the Defense Information Systems Agency, the Defense Intelligence Agency, the Defense Logistics Agency, the Defense Security Cooperation Agency, the Defense Security Service, the Defense Threat Reduction Agency, the Missile Defense Agency, the National Geospatial-Intelligence Agency, the National Security Agency, the United States Special Operations Command, and the United States Transportation Command.

"Department of Defense (DoD)," as used in DFARS, means the Department of Defense, the military departments, and the defense agencies.

"Electronic part" means an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly (section 818(f)(2) of Pub. L. 112-81).

"Executive agency" means for DoD, the Department of Defense, the Department of the Army, the Department of the Navy, and the Department of the Air Force.

"General public" and "non-governmental entities," as used in the definition of "commercial item" at FAR 2.101, do not include the Federal Government or a State, local, or foreign government (Pub. L. 110-181, section 815(b)).

"Head of the agency" means, for DoD, the Secretary of Defense, the Secretary of the Army, the Secretary of the Navy, and the Secretary of the Air Force. Subject to the direction of the Secretary of Defense, the Under Secretary of Defense (Acquisition, Technology, and Logistics), and the Director of Defense Procurement and Acquisition Policy, the directors of the defense agencies have been delegated authority to act as head of the agency for their respective agencies (i.e., to perform functions under the FAR or DFARS reserved to a head of agency or agency head), except for such actions that by terms of statute, or any delegation, must be exercised within the Office of the Secretary of Defense. (For emergency acquisition flexibilities, see 218.270.)

"Information technology" (see 40 U.S.C 11101(6)) means, in lieu of the definition at FAR 2.1, any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

(1) For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires—

(i) Its use; or

(ii) To a significant extent, its use in the performance of a service or the furnishing of a product.

(2) The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

(3) The term "information technology" does not include any equipment acquired by a contractor incidental to a contract.

"Major defense acquisition program" is defined in 10 U.S.C. 2430(a).

"Obsolete electronic part" means an electronic part that is no longer available from the original manufacturer or an authorized aftermarket manufacturer.

"Original component manufacturer" means an organization that designs and/or engineers a part and is entitled to any intellectual property rights to that part.

"Original equipment manufacturer" means a company that manufactures products that it has designed from purchased components and sells those products under the company's brand name.

"Original manufacturer" means the original component manufacturer, the original equipment manufacturer, or the contract manufacturer.

"Procedures, Guidance, and Information (PGI)" means a companion resource to the DFARS that—

(1) Contains mandatory internal DoD procedures. The DFARS will direct compliance with mandatory procedures using imperative language such as "Follow the procedures at..." or similar directive language;

(2) Contains non-mandatory internal DoD procedures and guidance and supplemental information to be used at the discretion of the contracting officer. The DFARS will point to non-

mandatory procedures, guidance, and information using permissive language such as "The contracting officer may use..." or "Additional information is available at..." or other similar language;

(3) Is numbered similarly to the DFARS, except that each PGI numerical designation is preceded by the letters "PGI"; and

(4) Is available electronically at http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html.

"Senior procurement executive" means, for DoD—

Department of Defense (including the defense agencies)--Under Secretary of Defense (Acquisition, Technology, and Logistics);

Department of the Army--Assistant Secretary of the Army (Acquisition, Logistics and Technology);

Department of the Navy--Assistant Secretary of the Navy (Research, Development and Acquisition);

Department of the Air Force--Assistant Secretary of the Air Force (Acquisition).

The directors of the defense agencies have been delegated authority to act as senior procurement executive for their respective agencies, except for such actions that by terms of statute, or any delegation, must be exercised by the Under Secretary of Defense (Acquisition, Technology, and Logistics).

"Suspect counterfeit electronic part" means an electronic part for which credible evidence (including, but not limited to, visual inspection or testing) provides reasonable doubt that the electronic part is authentic.

"Tiered evaluation of offers," also known as "cascading evaluation of offers," means a procedure used in negotiated acquisitions, when market research is inconclusive for justifying limiting competition to small business concerns, whereby the contracting officer—

(1) Solicits and receives offers from both small and other than small business concerns;

(2) Establishes a tiered or cascading order of precedence for evaluating offers that is specified in the solicitation; and

(3) If no award can be made at the first tier, evaluates offers at the next lower tier, until award can be made.

(End of definitions)

(This page intentionally left blank)

DFARS Subpart 239.76

Cloud Computing.

New Addition- Aug 26, 2015
Revised -- Oct 21, 2016

http://www.acq.osd.mil/dpap/dars/dfars/html/current/239_76.htm

SUBPART 239.76—CLOUD COMPUTING

(Revised October 21, 2016)

239.7600 Scope of subpart.
239.7601 Definitions.
239.7602 Policy and responsibilities.
239.7602-1 General.
239.7602-2 Required storage of data within the United States or outlying areas.
239.7603 Procedures.
239.7604 Solicitation provision and contract clause.

239.7600 Scope of subpart.

This subpart prescribes policies and procedures for the acquisition of cloud computing services.

239.7601 Definitions.

As used in this subpart—

"Authorizing official," as described in DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), means the senior Federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

"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.

"Government data" means any information, document, media, or machine readable material regardless of physical form or characteristics, that is created or obtained by the Government in the course of official Government business.

"Government-related data" means any information, document, media, or machine readable material regardless of physical form or characteristics that is created or obtained by a contractor through the storage, processing, or communication of Government data. This does not include a contractor's business records (e.g., financial records, legal records, etc.) or data such as operating procedures, software coding, or algorithms that are not uniquely applied to the Government data.

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

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

239.7602 Policy and responsibilities.

239.7602-1 General.

(a) Generally, DoD shall acquire cloud computing services using commercial terms and conditions that are consistent with Federal law, and an agency's needs, including those requirements specified in this subpart. Some examples of commercial terms and conditions are license agreements, End User License Agreements (EULAs), Terms of Service (TOS), or other similar legal instruments or agreements. Contracting officers shall incorporate any applicable service provider terms and conditions into the contract by attachment or other appropriate mechanism. Contracting officers shall carefully review commercial terms and conditions and consult counsel to ensure these are consistent with Federal law, regulation, and the agency's needs.

(b) (1) Except as provided in paragraph (b)(2) of this section, the contracting officer shall only award a contract to acquire cloud computing services from a cloud service provider (e.g., contractor or subcontractor, regardless of tier) that has been granted provisional authorization by Defense Information Systems Agency, at the level appropriate to the requirement, to provide the relevant cloud computing services in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at the time the solicitation is issued or as authorized by the contracting officer) found at http://iase.disa.mil/cloud_security/Pages/index.aspx.

(2) The contracting officer may award a contract to acquire cloud computing services from a cloud service provider that has not been granted provisional authorization when—

(i) The requirement for a provisional authorization is waived by the DoD Chief Information Officer; or

(ii) The cloud computing service requirement is for a private, on-premises version that will be provided from U.S. Government facilities. Under this circumstance, the cloud service provider must obtain a provisional authorization prior to operational use.

(c) When contracting for cloud computing services, the contracting officer shall ensure the following information is provided by the requiring activity:

(1) Government data and Government-related data descriptions.

(2) Data ownership, licensing, delivery and disposition instructions specific to the relevant types of Government data and Government-related data (e.g., DD Form 1423, Contract Data Requirements List; work statement task; line item). Disposition instructions shall provide

for the transition of data in commercially available, or open and non-proprietary format (and for permanent records, in accordance with disposition guidance issued by National Archives and Record Administration).

(3) Appropriate requirements to support applicable inspection, audit, investigation, or other similar authorized activities specific to the relevant types of Government data and Government-related data, or specific to the type of cloud computing services being acquired.

(4) Appropriate requirements to support and cooperate with applicable system-wide search and access capabilities for inspections, audits, investigations.

239.7602-2 Required storage of data within the United States or outlying areas.

(a) Cloud computing service providers are required to maintain within the 50 states, the District of Columbia, or outlying areas of the United States, all Government data that is not physically located on DoD premises, unless otherwise authorized by the authorizing official, as described in DoD Instruction 8510.01, in accordance with the SRG.

(b) The contracting officer shall provide written notification to the contractor when the contractor is permitted to maintain Government data at a location outside the 50 States, the District of Columbia, and outlying areas of the United States.

239.7603 Procedures.

Follow the procedures relating to cloud computing at PGI 239.7603 (DFARS/PGI view).

239.7604 Solicitation provision and contract clause.

(a) Use the provision at 252.239-7009, Representation of Use of Cloud Computing, in solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial item, for information technology services.

(a) Use the clause at 252.239-7010, Cloud Computing Services, in solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial item, for information technology services.

DFARS 252.239-7009

Representation of Use of Cloud Computing.

New Addition – Aug 26, 2015
Revised – Sept 21, 2015

http://www.acq.osd.mil/dpap/dars/dfars/html/current/252239.htm#252.239-7009

REPRESENTATION OF USE OF CLOUD COMPUTING (SEP 2015)

252.239-7009 Representation of Use of Cloud Computing.

As prescribed in 239.7604(a), use the following provision:

(a) *Definition*. "Cloud computing," as used in this provision, 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.

(b) The Offeror shall indicate by checking the appropriate blank in paragraph (c) of this provision whether the use of cloud computing is anticipated under the resultant contract.

(c) *Representation*. The Offeror represents that it—

_____ Does anticipate that cloud computing services will be used in the performance of any contract or subcontract resulting from this solicitation.

_____ Does not anticipate that cloud computing services will be used in the performance of any contract or subcontract resulting from this solicitation.

(End of provision)

DFARS 252.239-7010

Cloud Computing Services.

New Addition –Aug 26, 2015
Revised –Oct 21, 2016

http://www.acq.osd.mil/dpap/dars/dfars/html/current/252239.htm#252.239-7010

www.i2ComplianceTools.com
866-471-0145

252.239-7010 Cloud Computing Services.

As prescribed in 239.7604(b), use the following clause:

CLOUD COMPUTING SERVICES (OCT 2016)

(a) *Definitions*. As used in this clause—

"Authorizing official," as described in DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), means the senior Federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

"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.

"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.

"Government data" means any information, document, media, or machine readable material regardless of physical form or characteristics, that is created or obtained by the Government in the course of official Government business.

"Government-related data" means any information, document, media, or machine readable material regardless of physical form or characteristics that is created or obtained by a contractor through the storage, processing, or communication of Government data. This does not include contractor's business records e.g. financial records, legal records etc. or data such as operating procedures, software coding or algorithms that are not uniquely applied to the Government data.

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

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

"Spillage" security incident that results in the transfer of classified or controlled unclassified information onto an information system not accredited (i.e., authorized) for the appropriate security level.

(b) *Cloud computing security requirements*. The requirements of this clause are applicable when using cloud computing to provide information technology services in the performance of the contract.

(1) If the Contractor indicated in its offer that it "does not anticipate the use of cloud computing services in the performance of a resultant contract," in response to provision 252.239-7009, Representation of Use of Cloud Computing, and after the award of this contract, the Contractor proposes to use cloud computing services in the performance of the contract, the Contractor shall obtain approval from the Contracting Officer prior to utilizing cloud computing services in performance of the contract.

(2) The Contractor shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at the time the solicitation is issued or as authorized by the Contracting Officer) found at http://iase.disa.mil/cloud_security/Pages/index.aspx, unless notified by the Contracting Officer that this requirement has been waived by the DoD Chief Information Officer.

(3) The Contractor shall maintain within the United States or outlying areas all Government data that is not physically located on DoD premises, unless the Contractor receives written notification from the Contracting Officer to use another location, in accordance with DFARS 239.7602-2(a).

(c) *Limitations on access to, and use and disclosure of Government data and Government-related data.*

(1) The Contractor shall not access, use, or disclose Government data unless specifically authorized by the terms of this contract or a task order or delivery order issued hereunder.

(i) If authorized by the terms of this contract or a task order or delivery order issued hereunder, any access to, or use or disclosure of, Government data shall only be for purposes specified in this contract or task order or delivery order.

(ii) The Contractor shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations.

(iii) These access, use, and disclosure prohibitions and obligations shall survive the expiration or termination of this contract.

(2) The Contractor shall use Government-related data only to manage the operational environment that supports the Government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

(d) *Cloud computing services cyber incident reporting*. The Contractor shall report all cyber incidents that are related to the cloud computing service provided under this contract. Reports shall be submitted to DoD via http://dibnet.dod.mil/.

(e) *Malicious software*. The Contractor or subcontractors that discover and isolate malicious software in connection with a reported cyber incident shall submit the malicious software in accordance with instructions provided by the Contracting Officer.

(f) *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 the cyber incident report (see paragraph (d) 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.

(g) *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.

(h) *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 (f) of this clause.

(i) *Records management and facility access.*

(1) The Contractor shall provide the Contracting Officer all Government data and Government-related data in the format specified in the contract.

(2) The Contractor shall dispose of Government data and Government-related data in accordance with the terms of the contract and provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures.

(3) The Contractor shall provide the Government, or its authorized representatives, access to all Government data and Government-related data, access to contractor personnel involved in performance of the contract, and physical access to any Contractor facility with Government data, for the purpose of audits, investigations, inspections, or other similar activities, as authorized by law or regulation.

(j) *Notification of third party access requests*. The Contractor shall notify the Contracting Officer promptly of any requests from a third party for access to Government data or

Government-related data, including any warrants, seizures, or subpoenas it receives, including those from another Federal, State, or local agency. The Contractor shall cooperate with the Contracting Officer to take all measures to protect Government data and Government-related data from any unauthorized disclosure.

(k) *Spillage*. Upon notification by the Government of a spillage, or upon the Contractor's discovery of a spillage, the Contractor shall cooperate with the Contracting Officer to address the spillage in compliance with agency procedures.

(l) *Subcontracts*. The Contractor shall include this clause, including this paragraph (l), in all subcontracts that involve or may involve cloud services, including subcontracts for commercial items.

(End of clause)

(This page intentionally left blank)

DFARS Subpart 212.3

Solicitation provisions and contract clauses for the acquisition of commercial items.

Revised – Sept 21, 2015

Revised – Aug 2, 2016

http://www.acq.osd.mil/dpap/dars/dfars/html/current/212_3.htm

SUBPART 212.3--SOLICITATION PROVISIONS AND CONTRACT CLAUSES FOR THE ACQUISITION OF COMMERCIAL ITEMS

(Revised August 2, 2016)

212.301 Solicitation provisions and contract clauses for the acquisition of commercial items.
212.302 Tailoring of provisions and clauses for the acquisition of commercial items.

212.301 Solicitation provisions and contract clauses for the acquisition of commercial items.

See DoD Class Deviation 2013-O0019, Commercial Item Omnibus Clause for Acquisitions Using the Standard Procurement System, issued September 25, 2013. This class deviation allows the contracting officer to use the SPS clause logic capability to automatically select the clauses that are applicable to the specific solicitation and contract. The contracting officer shall ensure that the deviation clause is incorporated into these solicitations and contracts because the deviation clause fulfills the statutory requirements on auditing and subcontract clauses applicable to commercial items. The deviation also authorizes adjustments to the deviation clause required by future changes to the clause at 52.212-5 that are published in the FAR. This deviation is effective for five years, or until otherwise rescinded.

(c) Include an evaluation factor regarding supply chain risk (see subpart 239.73) when acquiring information technology, whether as a service or as a supply, that is a covered system, is a part of a covered system, or is in support of a covered system, as defined in 239.7301.

(f) The following additional provisions and clauses apply to DoD solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items. If the offeror has completed any of the following provisions listed in this paragraph electronically as part of its annual representations and certifications at https://www.acquisition.gov, the contracting officer shall consider this information instead of requiring the offeror to complete these provisions for a particular solicitation.

(i) *Part 203—Improper Business Practices and Personal Conflicts of Interest.*

(A) Use the FAR clause at 52.203-3, Gratuities, as prescribed in FAR 3.202, to comply with 10 U.S.C. 2207.

(B) Use the clause at 252.203-7000, Requirements Relating to Compensation of Former DoD Officials, as prescribed in 203.171-4(a), to comply with section 847 of Pub. L. 110-181.

(C) Use the clause at 252.203-7003, Agency Office of the Inspector General, as prescribed in 203.1004(a), to comply with section 6101 of Pub. L. 110-252 and 41 U.S.C. 3509.

(D) Use the provision at 252.203-7005, Representation Relating to Compensation of Former DoD Officials, as prescribed in 203.171-4(b).

(ii) *Part 204—Administrative Matters.*

(A) Use the provision at 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls, as prescribed in 204.7304(a).

(B) Use the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Information, as prescribed in 204.7304(b).

(C) Use the provision at 252.204-7011, Alternative Line Item Structure, as prescribed in 204.7109(b).

(D) Use the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, as prescribed in 204.7304(c).

(E) Use the provision at 252.204-7013, Limitations on the Use or Disclosure of Information by Litigation Support Offerors, as prescribed in 204.7403(a), to comply with 10 U.S.C. 129d.

(F) Use the clause at 252.204-7014, Limitations on the Use or Disclosure of Information by Litigation Support Contractors, as prescribed in 204.7403(b), to comply with 10 U.S.C. 129d.

(G) Use the clause at 252.204-7015, Notice of Authorized Disclosure of Information for Litigation Support, as prescribed in 204.7403(c), to comply with 10 U.S.C. 129d.

(iii) *Part 205—Publicizing Contract Actions.*

Use the clause at 252.205-7000, Provision of Information to Cooperative Agreement Holders, as prescribed in 205.470, to comply with 10 U.S.C. 2416.

(iv) *Part 211—Describing Agency Needs.*

(A) Use the clause at 252.211-7003, Item Unique Identification and Valuation, as prescribed in 211.274-6(a)(1).

(B) Use the provision at 252.211-7006, Passive Radio Frequency Identification, as prescribed in 211.275-3.

(C) Use the clause at 252.211-7007, Reporting of Government-Furnished Property, as prescribed in 211.274-6.

(D) Use the clause at 252.211-7008, Use of Government-Assigned Serial Numbers, as prescribed in 211.274-6(c).

(v) *Part 213—Simplified Acquisition Procedures.*

Use the provision at 252.213-7000, Notice to Prospective Suppliers on Use of Past Performance Information Retrieval System—Statistical Reporting in Past Performance Evaluations, as prescribed in 213.106-2-70.

(vi) *Part 215—Contracting by Negotiation.*

(A) Use the provision at 252.215-7003, Requirements for Submission of Data Other Than Certified Cost or Pricing Data—Canadian Commercial Corporation, as prescribed at 215.408(3)(i).

(B) Use the clause at 252.215-7004, Requirement for Submission of Data other Than Certified Cost or Pricing Data—Modifications—Canadian Commercial Corporation, as prescribed at 215.408(3)(ii).

(C) Use the provision at 252.215-7007, Notice of Intent to Resolicit, as prescribed in 215.371-6.

(D) Use the provision 252.215-7008, Only One Offer, as prescribed at 215.408(4).

(vii) *Part 219—Small Business Programs.*

(A) Use the clause at 252.219-7003, Small Business Subcontracting Plan (DoD Contracts), to comply with 15 U.S.C. 637.

(*1*) Use the basic clause as prescribed in 219.708(b)(1)(A)(*1*).

(*2*) Use the alternate I clause as prescribed in 219.708(b)(1)(A)(*2*).

(B) Use the clause at 252.219-7004, Small Business Subcontracting Plan (Test Program), as prescribed in 219.708(b)(1)(B), to comply with 15 U.S.C. 637 note.

(C) Use the provision at 252.219-7000, Advancing Small Business Growth, as prescribed in 219.309(1), to comply with 10 U.S.C. 2419.

(viii) *Part 222—Application of Labor Laws to Government Acquisitions.*

Use the provision at 252.222-7007, Representation Regarding Combating Trafficking in Persons, as prescribed in 222.1771.

(ix) *Part 223—Environment, Energy and Water Efficiency, Renewable Energy Technologies, Occupational Safety, and Drug-Free Workplace.*

Use the clause at 252.223-7008, Prohibition of Hexavalent Chromium, as prescribed in 223.7306.

(x) *Part 225—Foreign Acquisition.*

(A) Use the provision at 252.225-7000, Buy American—Balance of Payments Program Certificate, to comply with 41 U.S.C. chapter 83 and Executive Order 10582 of December 17, 1954, Prescribing Uniform Procedures for Certain Determinations Under the Buy-American Act.

(*1*) Use the basic provision as prescribed in 225.1101(1)(i).

(*2*) Use the alternate I provision as prescribed in 225.1101(1)(ii).

(B) Use the clause at 252.225-7001, Buy American and Balance of Payments Program, to comply with 41 U.S.C. chapter 83 and Executive Order 10582 of December 17, 1954, Prescribing Uniform Procedures for Certain Determinations Under the Buy-American Act.

(*1*) Use the basic clause as prescribed in 225.1101(2)(ii).

(*2*) Use the alternate I clause as prescribed in 225.1101(2)(iii).

(C) Use the clause at 252.225-7006, Acquisition of the American Flag, as prescribed in 225.7002-3(c), to comply with section 8123 of the DoD Appropriations Act, 2014 (Pub. L. 113-76, division C, title VIII), and the same provision in subsequent DoD appropriations acts.

(D) Use the clause at 252.225-7008, Restriction on Acquisition of Specialty Metals, as prescribed in 225.7003-5(a)(1), to comply with 10 U.S.C. 2533b.

(E) Use the clause at 252.225-7009, Restriction on Acquisition of Certain Articles Containing Specialty Metals, as prescribed in 225.7003-5(a)(2), to comply with 10 U.S.C. 2533b.

(F) Use the provision at 252.225-7010, Commercial Derivative Military Article—Specialty Metals Compliance Certificate, as prescribed in 225.7003-5(b), to comply with 10 U.S.C. 2533b.

(G) Use the clause at 252.225-7012, Preference for Certain Domestic Commodities, as prescribed in 225.7002-3(a), to comply with 10 U.S.C. 2533a.

(H) Use the clause at 252.225-7015, Restriction on Acquisition of Hand or Measuring Tools, as prescribed in 225.7002-3(b), to comply with 10 U.S.C. 2533a.

(I) Use the clause at 252.225-7016, Restriction on Acquisition of Ball and Roller Bearings, as prescribed in 225.7009-5, to comply with section 8065 of Pub. L. 107-117 and the same restriction in subsequent DoD appropriations acts.

(J) Use the clause at 252.225-7017, Photovoltaic Devices, as prescribed in 225.7017-5(a), to comply with section 858 of Public Law 113-291.

(K) Use the provision at 252.225-7018, Photovoltaic Devices—Certificate, as prescribed in 225.7017-5(b), to comply with section 858 of Public Law 113-291.

(L) Use the provision at 252.225-7020, Trade Agreements Certificate, to comply with 19 U.S.C. 2501-2518 and 19 U.S.C. 3301 note. Alternate I also implements section 886 of the National Defense Authorization Act for Fiscal Year 2008 (Pub. L. 110-181).

(*1*) Use the basic provision as prescribed in 225.1101(5)(i),

(*2*) Use the alternate I provision as prescribed in 225.1101(5)(ii).

(M) Use the clause at 252.225-7021, Trade Agreements to comply with 19 U.S.C. 2501-2518 and 19 U.S.C. 3301 note.

(*1*) Use the basic clause as prescribed in 225.1101(6)(i).

(*2*) Use the alternate II clause as prescribed in 225.1101(6)(ii).

(N) Use the provision at 252.225-7023, Preference for Products or Services from Afghanistan, as prescribed in 225.7703-4(a), to comply with section 886 of the National Defense Authorization Act for Fiscal Year 2008 (Pub. L. 110-181).

(O) Use the clause at 252.225-7024, Requirement for Products or Services from Afghanistan, as prescribed in 225.7703-4(b), to comply with section 886 of the National Defense Authorization Act for Fiscal Year 2008 (Pub. L. 110-181).

(P) Use the clause at 252.225-7026, Acquisition Restricted to Products or Services from Afghanistan, as prescribed in 225.7703-4(c), to comply with section 886 of the National Defense Authorization Act for Fiscal Year 2008 (Pub. L. 110-181).

(Q) Use the clause at 252.225-7027, Restriction on Contingent Fees for Foreign Military Sales, as prescribed in 225.7307(a), to comply with 22 U.S.C. 2779.

(R) Use the clause at 252.225-7028, Exclusionary Policies and Practices of Foreign Governments, as prescribed in 225.7307(b), to comply with 22 U.S.C. 2755.

(S) Use the clause at 252.225-7029, Acquisition of Uniform Components for Afghan Military or Afghan National Police, as prescribed in 225.7703-4(d).

(T) Use the provision at 252.225-7031, Secondary Arab Boycott of Israel, as prescribed in 225.7605, to comply with 10 U.S.C. 2410i.

(U) Use the provision at 252.225-7035, Buy American—Free Trade Agreements—Balance of Payments Program Certificate, to comply with 41 U.S.C. chapter 83 and 19 U.S.C. 3301 note. Alternates II, III, and V also implement section 886 of the National Defense Authorization Act for Fiscal Year 2008 (Pub. L. 110-181).

(*1*) Use the basic provision as prescribed in 225.1101(9)(i).

(*2*) Use the alternate I provision as prescribed in 225.1101(9)(ii).

(*3*) Use the alternate II provision as prescribed in 225.1101(9)(iii).

(*4*) Use the alternate III provision as prescribed in 225.1101(9)(iv).

(*5*) Use the alternate IV provision as prescribed in 225.1101(9)(v).

(*6*) Use the alternate V provision as prescribed in 225.1101(9)(vi).

(V) Use the clause at 252.225-7036, Buy American--Free Trade Agreements-- Balance of Payments Program to comply with 41 U.S.C. chapter 83 and 19 U.S.C. 3301 note. Alternates II, III, and V also implement section 886 of the National Defense Authorization Act for Fiscal Year 2008 (Pub. L. 110-181).

(*1*) Use the basic clause as prescribed in 225.1101(10)(i)(A).

(*2*) Use the alternate I clause I as prescribed in 225.1101(10)(i)(B).

(*3*) Use the alternate II clause as prescribed in 225.1101(10)(i)(C).

(*4*) Use the alternate III clause as prescribed in 225.1101(10)(i)(D).

(*5*) Use the alternate IV clause as prescribed in 225.1101(10)(i)(E).

(*6*) Use the alternate V clause as prescribed in 225.1101(10)(i)(F).

(W) Use the provision at 252.225-7037, Evaluation of Offers for Air Circuit Breakers, as prescribed in 225.7006-4(a), to comply with 10 U.S.C. 2534(a)(3).

(X) Use the clause at 252.225-7038, Restriction on Acquisition of Air Circuit Breakers, as prescribed in 225.7006-4(b), to comply with 10 U.S.C. 2534(a)(3).

(Y) Use the clause at 252.225-7039, Defense Contractors Performing Private Security Functions Outside the United States, as prescribed in 225.302-6, to comply with section 2 of Pub. L. 110-181, as amended.

(Z) Use the clause at 252.225-7040, Contractor Personnel Supporting U.S. Armed Forces Deployed Outside the United States, as prescribed in 225.371-5(a).

(AA) Use the clause at 252.225-7043, Antiterrorism/Force Protection Policy for Defense Contractors Outside the United States, as prescribed in 225.372-2.

(BB) Use the provision at 252.225-7049, Prohibition on Acquisition of Commercial Satellite Services from Certain Foreign Entities—Representations, as prescribed at 225.772-5, to comply with 10 U.S.C. 2279.

(CC) Use the provision at 252.225-7050, Disclosure of Ownership or Control by the Government of a Country that is a State Sponsor of Terrorism, as prescribed in 225.771-5, to comply with 10 U.S.C. 2327(b).

(xi) *Part 226--Other Socioeconomic Programs.*

Use the clause at 252.226-7001, Utilization of Indian Organizations, Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns, as prescribed in 226.104, to comply with section 8021 of Pub. L. 107-248 and similar sections in subsequent DoD appropriations acts.

(xii) *Part 227—Patents, Data, and Copyrights.*

(A) Use the clause at 252.227-7013, Rights in Technical Data–Noncommercial Items, as prescribed in 227.7103-6(a). Use the clause with its Alternate I as prescribed in 227.7103-6(b)(1). Use the clause with its Alternate II as prescribed in 227.7103-6(b)(2), to comply with 10 U.S.C. 7317 and 17 U.S.C. 1301, et. seq.

(B) Use the clause at 252.227-7015, Technical Data–Commercial Items, as prescribed in 227.7102-4(a)(1), to comply with 10 U.S.C. 2320. Use the clause with its Alternate I as prescribed in 227.7102-4(a)(2), to comply with 10 U.S.C. 7317 and 17 U.S.C. 1301, et. seq.

(C) Use the clause at 252.227-7037, Validation of Restrictive Markings on Technical Data, as prescribed in 227.7102-4(c).

(xiii) *Part 229—Taxes.*

(A) Use the clause at 252.229-7014, Taxes—Foreign Contracts in Afghanistan, as prescribed at 229.402-70(k).

(B) Use the clause at 252.229-7015, Taxes—Foreign Contracts in Afghanistan (North Atlantic Treaty Organization Status of Forces Agreement), as prescribed at 229.402-70(l).

(xiv) *Part 232—Contract Financing.*

(A) Use the clause at 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports, as prescribed in 232.7004, to comply with 10 U.S.C. 2227.

(B) Use the clause at 252.232-7006, Wide Area WorkFlow Payment Instructions, as prescribed in 232.7004(b).

(C) Use the clause at 252.232-7009, Mandatory Payment by Governmentwide Commercial Purchase Card, as prescribed in 232.1110.

(D) Use the clause at 252.232-7010, Levies on Contract Payments, as prescribed in 232.7102.

(E) Use the clause at 252.232-7011, Payments in Support of Emergencies and Contingency Operations, as prescribed in 232.908.

(F) Use the provision at 252.232-7014, Notification of Payment in Local Currency (Afghanistan), as prescribed in 232.7202.

(xv) *Part 237—Service Contracting.*

(A) Use the clause at 252.237-7010, Prohibition on Interrogation of Detainees by Contractor Personnel, as prescribed in 237.173-5, to comply with section 1038 of Pub. L. 111-84.

(B) Use the clause at 252.237-7019, Training for Contractor Personnel Interacting with Detainees, as prescribed in 237.171-4, to comply with section 1092 of Pub. L. 108-375.

(xvi) *Part 239--Acquisition of Information Technology.*

(A) Use the provision 252.239-7009, Representation of Use of Cloud Computing, as prescribed in 239.7604(a).

(B) Use the clause 252.239-7010, Cloud Computing Services, as prescribed in 239.7604(b).

(C) Use the provision at 252.239-7017, Notice of Supply Chain Risk, as prescribed in 239.7306(a), to comply with section 806 of Pub. L. 111-383.

(D) Use the clause at 252.239-7018, Supply Chain Risk, as prescribed in 239.7306(b), to comply with section 806 of Pub. L. 111-383.

(xvii) *Part 243—Contract Modifications.*

Use the clause at 252.243-7002, Requests for Equitable Adjustment, as prescribed in 243.205-71, to comply with 10 U.S.C. 2410.

(xviii) *Part 244—Subcontracting Policies and Procedures.*

Use the clause at 252.244-7000, Subcontracts for Commercial Items, as prescribed in 244.403.

(xix) *Part 246—Quality Assurance.*

(A) Use the clause at 252.246-7003, Notification of Potential Safety Issues, as prescribed in 246.371(a).

(B) Use the clause at 252.246-7004, Safety of Facilities, Infrastructure, and Equipment for Military Operations, as prescribed in 246.270-4, to comply with section 807 of Pub. L. 111-84.

(C) Use the clause at 252.246-7008, Sources of Electronic Parts, as prescribed in 246.870-3(b), to comply with section 818(c)(3) of Pub. L. 112-81, as amended by section 817 of the National Defense Authorization Act for Fiscal Year 2015 (Pub. L. 113-291).

(xx) *Part 247—Transportation.*

(A) Use the clause at 252.247-7003, Pass-Through of Motor Carrier Fuel Surcharge Adjustment to the Cost Bearer, as prescribed in 247.207, to comply with section 884 of Pub. L. 110-417.

(B) Use the provision at 252.247-7022, Representation of Extent of Transportation by Sea, as prescribed in 247.574(a).

(C) Use the basic or one of the alternates of the clause at 252.247-7023, Transportation of Supplies by Sea, as prescribed in 247.574(b), to comply with the Cargo Preference Act of 1904 (10 U.S.C. 2631(a)).

(*1*) Use the basic clause as prescribed in 247.574(b)(1).

(*2*) Use the alternate I clause as prescribed in 247.574(b)(2).

(*3*) Use the alternate II clause as prescribed in 247.574(b)(3).

(D) Use the clause at 252.247-7024, Notification of Transportation of Supplies by Sea, as prescribed in 247.574(c).

(E) Use the clause 252.247-7025, Reflagging or Repair Work, as prescribed in 247.574(d), to comply with 10 U.S.C. 2631(b).

(F) Use the provision at 252.247-7026, Evaluation Preference for Use of Domestic Shipyards – Applicable to Acquisition of Carriage by Vessel for DoD Cargo in the Coastwise or Noncontiguous Trade, as prescribed in 247.574(e), to comply with section 1017 of Pub. L. 109-364.

(G) Use the clause at 252.247-7027, Riding Gang Member Requirements, as prescribed in 247.574(f), to comply with section 3504 of the National Defense Authorization Act for Fiscal Year 2009 (Pub. L. 110-417).

(H) Use the clause at 252.247-7028, Application for U.S Government Shipping Documentation/Instructions, as prescribed in 247.207.

212.302 Tailoring of provisions and clauses for the acquisition of commercial items.

(c) *Tailoring inconsistent with customary commercial practice*. The head of the contracting activity is the approval authority within the DoD for waivers under FAR 12.302(c).

(End of provision and clause)

(This page intentionally left blank)