(Billing Code 5001-06)

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Parts 202, 204, 212, 239, and 252

[Docket No. DARS-2015-0039]

RIN 0750-AI61

Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)

AGENCY: Defense Acquisition Regulations System, Department of Defense (DoD).

ACTION: Interim rule.

SUMMARY: DoD is issuing an interim rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a section of the National Defense Authorization Act for Fiscal Year 2013 and a section of the National Defense Authorization Act for Fiscal Year 2015, both of which require contractor reporting on network penetrations. Additionally, this rule implements DoD policy on the purchase of cloud computing services.

DATES: Effective **[Insert date of publication in the FEDERAL REGISTER].**

Comment date: Comments on the interim rule should be submitted in writing to the address shown below on or before **[Insert date 60 days after date of publication in the FEDERAL REGISTER]** to be considered in the formation of a final rule.

ADDRESSES: Submit comments identified by DFARS Case 2013-D018, using any of the following methods:

o Regulations.gov: http://www.regulations.gov. Submit comments via the Federal eRulemaking portal by entering "DFARS Case 2013-D018" under the heading "Enter keyword or ID" and selecting "Search." Select the link "Submit a Comment" that corresponds with "DFARS Case 2013-D018." Follow the instructions provided at the "Submit a Comment" screen. Please include your name, company name (if any), and "DFARS Case 2013-D018" on your attached document.

o E-mail: osd.dfars@mail.mil. Include DFARS Case 2013-D018 in the subject line of the message.

o Fax: 571-372-6094.

o Mail: Defense Acquisition Regulations System, Attn: Mr. Dustin Pitsch, OUSD(AT&L)DPAP/DARS, Room 3B941, 3060 Defense Pentagon, Washington, DC 20301-3060.

Comments received generally will be posted without change to http://www.regulations.gov, including any personal information provided. To confirm receipt of your comment(s), please check www.regulations.gov, approximately two to three days after

submission to verify posting (except allow 30 days for posting of comments submitted by mail).

FOR FURTHER INFORMATION CONTACT: Mr. Dustin Pitsch, OUSD(AT&L)DPAP/DARS, telephone 571-372-6090.

SUPPLEMENTARY INFORMATION:

I. Background

This interim rule requires contractors and subcontractors to report cyber incidents that result in an actual or potentially adverse effect on a covered contractor information system or covered defense information residing therein, or on a contractor's ability to provide operationally critical support. DoD is working to establish a single reporting mechanism for DoD contractor reporting of cyber incidents on unclassified information systems. This rule is intended to streamline the reporting process for DoD contractors and minimize duplicative reporting processes. Cyber incidents involving classified information on classified contractor systems will continue to be reported in accordance with the National Industrial Security Program Operating Manual (see DoD-M 5220.22 available at http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf).

The rule revises the DFARS to implement section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013 (Pub. L.112-239) and section 1632 of the NDAA for FY 2015. Section 941 of the NDAA for FY 2013 requires cleared defense

contractors to report penetrations of networks and information systems and allows DoD personnel access to equipment and information to assess the impact of reported penetrations. Section 1632 of the NDAA for FY 2015 requires that a contractor designated as operationally critical must report each time a cyber incident occurs on that contractor's network or information systems.

In addition, this rule also implements DoD policies and procedures for use when contracting for cloud computing services. The DoD Chief Information Officer (CIO) issued a memo on December 15, 2014, entitled "Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services" to clarify DoD guidance when acquiring commercial cloud services (See memo here: http://iase.disa.mil/cloud security/Pages/docs.aspx). The DoD CIO also released a Cloud Computing Security Requirements Guide (SRG) Version 1, Release 1 on January 13, 2015, for cloud service providers to comply with when providing the DoD with cloud services (See SRG here: http://iase.disa.mil/cloud security/Pages/index.aspx). This rule implements these new policies developed within the DoD CIO memo and the SRG in the DFARS to ensure uniform application when contracting for cloud services across the DoD. The combination of the two statutes as well as the cloud computing policy will

serve to increase the cyber security requirements placed on DoD information in contractor systems and will help the DoD to mitigate the risks related to compromised information as well as gather information for future improvements in cyber security policy.

II. Discussion and Analysis

To implement section 941 of the NDAA for FY 2013 and section 1632 of the NDAA for FY 2015, an existing DFARS subpart and clause have been utilized and expanded upon, and a new provision and clause added. A new subpart, provision, and clause are added for the implementation of cloud contracting policies.

(1) DFARS subpart 204.73 is modified to expand safeguarding and reporting policy to require protection of covered defense information, which includes controlled technical information, export controlled information, critical information, and other information requiring protection by law, regulation, or Government-wide policy.

(2) The clause at 252.204-7012 is renamed "Safeguarding Covered Defense Information and Cyber Incident Reporting" and the scope of the clause is expanded to cover the safeguarding of covered defense information and require contractors to report cyber incidents involving this new class of information as well as any cyber incident that may affect the ability to provide operationally critical support. The table of security controls

based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 is replaced by NIST SP 800-171, entitled "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." NIST SP 800-171 is a publication specifically tailored for use in protecting sensitive information residing in contractor information systems that refines the requirements from Federal Information Processing Standard (FIPS) 200 and controls from NIST SP 800-53 and presents them in an easier to use format. In addition to being easier to use, NIST SP 800-171 greatly increases the protections of Government information in contractor information systems, while simultaneously reducing the burden placed on the contractor by eliminating Federal-centric processes and requirements currently embedded in NIST SP 800-53. For example, a task analysis comparing the requirements of NIST SP 800-171 to the current table of security controls (based on NIST SP 800-53) demonstrates a reduction in required tasks by 30 percent.

(3) A new provision at 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, is added to ensure that offerors are aware of the requirements of clause 252.204-7012 and allow for a process to explain; (i) how alternative, but equally effective, security measures can compensate for the inability to satisfy a particular

requirement; or (ii) why a particular requirement is not applicable.

(4) A new clause at 252.204-7009, Limitations on the Use and Disclosure of Third-Party Contractor Reported Cyber Incident Information, is added to protect information submitted to DoD in response to a cyber incident.

(5) DFARS subpart 239.76 is added to implement policy for the acquisition of cloud computing services.

(6) A new provision at 252.239-7009, Representation of Use of Cloud Computing, is added to allow the offeror to represent their intention to utilize cloud computing services in performance of the contract or not.

(7) A new clause at 252.239-7010, Cloud Computing Services, is added to provide standard contract language for the acquisition of cloud computing services; including access, security and reporting requirements.

(8) The term “cyber incident,” is removed from the definitions section of subpart 204.73 and is now defined at 202.1. The terms “compromise” and “media” are also added to 202.1, because the terms are used in parts 204 and 239.

(9) The new clauses and provisions added by this rule are added to the list of solicitation provisions and contract clauses for the acquisition of commercial items at 212.301(f).

This rule is part of DoD's retrospective plan, completed in August 2011, under Executive Order 13563, "Improving Regulation and Regulatory Review." DoD's full plan and updates can be accessed at: http://www.regulations.gov/#!docketDetail;D=DOD-2011-OS-0036.

III. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is a significant regulatory action and, therefore, was subject to review under section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993. This rule is not a major rule under 5 U.S.C. 804.

IV. Regulatory Flexibility Act

DoD expects that this interim rule may have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act 5 U.S.C. 601, et seq. Therefore, an initial regulatory flexibility analysis has been prepared and is summarized as follows:

This rule expands on the existing information safeguarding policies in the DFARS and requires contractors to report cyber incidents to the Government in a broader scope of circumstances.

The objectives of this rule are to improve information security for DoD information stored on or transiting contractor systems as well as in a cloud environment. The rule implements section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013 (Pub. L. 112-239), section 1632 of the NDAA for FY 2015, and DoD CIO policy for the acquisition of cloud computing services. The benefits of the increased security requirements implemented through this rule are that more information will be protected from release, inadvertently or through malicious intent. Additional protection for DoD information will assist with a greater overall level of national security across the board.

This rule will apply to all contractors with covered defense information transiting their information systems. DoD estimates that this rule may apply to 10,000 contractors and that less than half of those are small businesses.

This rule requires that contractors report cyber incidents to the DoD. Of the required reporting fields several of them will likely require an information technology expert to provide information describing the cyber incident or at least to

determine what information was affected, to be noted in the report.

The rule does not duplicate, overlap, or conflict with any other Federal rules.

No significant alternatives, that would minimize the economic impact of the rule on small entities, were identified.

DoD invites comments from small business concerns and other interested parties on the expected impact of this rule on small entities.

DoD will also consider comments from small entities concerning the existing regulations in subparts affected by this rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C. 610 (DFARS Case 2013-D018), in correspondence.

V. Paperwork Reduction Act

This rule affects the information collection requirements in the provisions at DFARS 252.204-7012, currently approved under OMB Control Number 0704-0478, titled "Enhanced Safeguarding and Cyber Incident Reporting of Unclassified DoD Information Within Industry," in accordance with the Paperwork Reduction Act (44 U.S.C. chapter 35). The rule revises the collection reporting requirements based on—

- Changes to DFARS clause 252.204-7012, which is now titled "Safeguarding Covered Defense Information and Cyber Incident Reporting";
- A new DFARS provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls;
- A new DFARS provision at 252.239-7009, Representation of Use of Cloud Computing; and
- A new DFARS clause 252.239-7010, Cloud Computing Services.

The revisions to the information collection requirements contained in this rule require the approval of the Office of Management and Budget under the Paperwork Reduction Act (44 U.S.C. chapter 35). OMB has provided emergency clearance for the revision of 0704-0478. This collection is being revised to reflect the expanded contractually mandated cyber incident reporting requirements as well as contracting for cloud services, which are covered by the DFARS clause and provision collection requirements as discussed in the beginning of this section.

Public reporting burden for this collection is estimated to average approximately 4 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. The annual reporting burden is estimated as follows:

Respondents: 10,954.

Responses per respondent: 5.5 approximately

Total annual responses: 60,494.

Preparation hours per response: 4.15 hours approximately

Total response Burden Hours: 250,840.

Request for Comments Regarding Paperwork Burden. Public comments are particularly invited on: whether this collection of information is necessary for the proper performance of functions of the DFARS, and will have practical utility; whether our estimate of the public burden of this collection of information is accurate, and based on valid assumptions and methodology; ways to enhance the quality, utility, and clarity of the information to be collected; and ways in which we can minimize the burden of the collection of information on those who are to respond, through the use of appropriate technological collection techniques or other forms of information technology.

Written comments and recommendations including suggestions for reducing this burden, should be sent to Ms. Jasmeet Seehra at the Office of Management and Budget, Desk Officer for DoD, Room 10236, New Executive Office Building, Washington, DC 20503, or e-mail Jasmeet K. Seehra@omb.eop.gov, with a copy to the Defense Acquisition Regulations System, Attn: Mr. Dustin Pitsch, OUSD(AT&L)DPAP/DARS, Room 3B941, 3060 Defense Pentagon, Washington, DC 20301-3060, or email osd.dfars@mail.mil.

Comments should be received not later than 60 days after the date of publication in the Federal Register. You may also submit comments, identified by docket number and title, by the following method: Federal Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments. All submissions received must include the agency name, docket number and title for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at http://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

There are two other OMB Control Numbers currently in place for information collection requirements associated with the overall cyber reporting program. They are discussed below and are not being changed as a result of this rule.

OMB Control Number 0704-0489, Defense Industrial Base Voluntary Cyber Security/Information Assurance (DIB CS/IA) Cyber Incident Reporting, (regulations codified under Title 32 of the CFR) supports "voluntary" reporting and covers the online collection medium, a Defense Industrial Base/Information Assurance Incident Collection database, which is an online repository used for both voluntary reporting and reporting that

is contractually mandated under the DFARS clauses and provisions.

OMB Control Number 0704-0490, Defense Industrial Base Voluntary Cyber Security/Information Assurance (DIB CS/IA) Points of Contact (POC) Information, (regulations codified under Title 32 of the CFR) addresses the application process for participating companies. OMB Control Number 0704-0490 involves collection of personally identifiable information and is supported by a System of Records Notices for the cyber incident reporting program. The Privacy Act Statement of Records Notice (SORN) system identifier, DCIO 01, Defense Industrial Base (DIB) Cybersecurity Records, includes stipulations related to the release and disclosure of information collected. An update was published in the Federal Register on May 21, 2015, at 80 FR 29315 (see http://www.gpo.gov/fdsys/pkg/FR-2015-05-21/pdf/2015-12324.pdf).

VI. Determination to Issue an Interim Rule

A determination has been made under the authority of the Secretary of Defense that urgent and compelling reasons exist to promulgate this interim rule without prior opportunity for public comment. This action is necessary because of the urgent need to protect covered defense information and gain awareness of the full scope of cyber incidents being committed against defense contractors. The proliferation of information

technology and increased information access allowed by cloud computing environments has also increased the vulnerability of DoD information via attacks on its systems and networks and those of DoD contractors. The combination of the two statutes as well as implementation of the DoD cloud computing policy will serve to increase the cyber security requirements placed on DoD information on contractor systems and will help the DoD to mitigate the risks related to compromised information as well as gather information, through the reporting requirements, for future improvements in cyber security policy.

This rule expands upon the existing coverage in the DFARS, which previously only covered the protection of and reporting of incidents affecting the controlled technical information, but not other incidents within the contractor system. This interim rule expands the protection and reporting to entire contractor systems (i.e., "covered contractor information system") as well as a new type of information "covered defense information" which includes controlled technical information as a subset. This interim rule increases the number of circumstances where contractors must implement security controls as well as when they must report incidents.

Recent high-profile breaches of Federal information show the need to ensure that information security protections are clearly, effectively, and consistently addressed in contracts.

Failure to implement this rule may cause harm to the Government through the compromise of covered defense information or other Government data, or the loss of operationally critical support capabilities, which could directly impact national security. However, pursuant to 41 U.S.C. 1707 and FAR 1.501-3(b), DoD will consider public comments received in response to this interim rule in the formation of the final rule.

List of Subjects in 48 CFR Parts 202, 204, 212, 239, and 252

Government procurement.

Jennifer L. Hawes,

Editor, Defense Acquisition Regulations System.

Therefore, 48 CFR parts 202, 204, 212, 239, and 252 are amended as follows:

1. The authority citation for 48 CFR 202, 204, 212, and 252 continues to read as follows:

Authority: 41 U.S.C. 1303 and 48 CFR chapter 1.

PART 202—DEFINITIONS OF WORDS AND TERMS

2. Amend section 202.101 by adding, in alphabetical order, the definitions for "compromise," "cyber incident," and "media" to read as follows:

202.101 Definitions.

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.

* * * * *

Media, as used in parts 204 and 239, 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.

* * * * *

PART 204 ADMINISTRATIVE MATTERS

3. Revise subpart 204.73 heading to read as follows:

Subpart 204.73—Safeguarding Covered Defense Information and Cyber Incident Reporting

4. Revise section 204.7300 to read as follows:

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 controls. 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.

5. Amend section 204.7301 by—

a. Removing the definition of "cyber incident";

b. Adding, in alphabetical order, the definitions for "contractor attributional/proprietary information," "covered contractor information system," "covered defense information," "information system," "operationally critical support," and "rapid(ly) report(ing)"; and

c. Revising the definition for "controlled technical information".

The additions and revision read as follows:

204.7301 Definitions.

* * * * *

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 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 information that—

(1) Is—

(i) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

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

(2) Falls in any of the following categories:

(i) Controlled technical information.

(ii) Critical information (operations security). Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(iii) Export control. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations, and munitions list; license applications; and sensitive nuclear technology information.

(iv) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).

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

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(ly) report(ing) means within 72 hours of discovery of any cyber incident.

* * * * *

6. Revise section 204.7302 to read as follows:

204.7302 Policy.

(a) DoD and its contractors and subcontractors will provide adequate security to safeguard covered defense information on their unclassified information systems from unauthorized access and disclosure.

(1) Contractors and subcontractors are required to 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(a)(1)(ii) for instructions on contractor submissions of media and malicious software.

(b) Subcontractors are required to rapidly report cyber incidents directly to DoD at http://dibnet.dod.mil and to the prime contractor. Subcontractors shall provide the incident report

number from DoD to the prime contractor. Lower-tier subcontractors are required to likewise report the same information to their higher-tier subcontractor, until the prime contractor is reached.

(c) The Government acknowledges that information shared by the contractor under these procedures 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 information safeguards for covered defense information on their unclassified information systems, or has otherwise failed to meet the requirements of the clause at 252.204-7012. When a cyber incident is reported, the contracting officer shall consult with the DoD component CIO/cyber security office prior to assessing contractor compliance (see PGI 204.7303-3(a)(2)). 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., providing forensic analysis services, damages assessment services, or other services that require access to data from another contractor) are subject to restrictions on use and disclosure.

204.7303 [Amended]

7. Amend section 204.7303 by removing "unclassified controlled technical information" and adding "covered defense information" in its place.

8. Revise section 204.7304 to read as follows:

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 and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial 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 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.

PART 212—ACQUISITION OF COMMERCIAL ITEM

9. Amend section 212.301 by—

a. Redesignating paragraphs (f)(ii)(A) through (E) as paragraphs (f)(ii)(C) through (G);

b. Adding new paragraphs (f)(ii)(A) and (B);

c. Revising the newly redesignated (f)(ii)(D);d. Redesignating paragraphs (f)(xv)(A) and (B) as paragraphs (f)(xv)(C) and (D);

e. Adding new paragraphs (f)(xv)(A) and (B).

The additions and revision read as follows:

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

(f) * * *

(ii) * * *

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

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

* * * * *

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

* * * * *

(xv) * * *

(A) Use the provision 252.239-7009, Representation of Use of Cloud Computing, as prescribed in 239.7603(a).

(B) Use the clause 252.239-7010, Cloud Computing Services, as prescribed in 239.7603(b).

* * * * *

PART 239—ACQUISITION OF INFORMATION TECHNOLOGY

10. The authority citation for 48 CFR part 239 is revised to read as follows:

Authority: 41 U.S.C. 1303 and 48 CFR chapter 1.

11. Add subpart 239.76 to read as follows:

Subpart 239.76—Cloud Computing

Sec.

Subpart 239.76—Cloud Computing

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.

Spillage means a 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.

239.7602 Policy and responsibilities.

239.7602-1 General.

(a) Generally, the 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) The contracting officer shall only award a contract to acquire cloud computing services from any 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. Provisional authorization processes are also available at the SRG website. Cloud service providers with existing provisional authorization are listed at http://www.disa.mil/Computing/Cloud-Services/Cloud-Support.

(c) When contracting for cloud computing services, the contracting officer shall ensure the following information is provided in the purchase request—

(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., CDRL, SOW 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 limitations and requirements regarding contractor and third-party access to, and use and disclosure of, Government data and Government-related data;

(4) 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;

(5) Appropriate requirements to support and cooperate with applicable system-wide search and access capabilities for inspections, audits, investigations, litigation, eDiscovery, records management associated with the agency's retention schedules, and similar authorized activities; and

(6) A requirement for the contractor to coordinate with the responsible Government official designated by the contracting officer, in accordance with agency procedures, to respond to any spillage occurring in connection with the cloud computing services being provided.

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, Risk Management Framework (RMF) for DoD Information Technology (IT), 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 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.

(b) 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.

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

12. Add section 252.204-7008 to read as follows:

252.204-7008 Compliance with Safeguarding Covered Defense Information Controls.

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

COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (AUG 2015)

(a) Definitions. As used in this provision—

Controlled technical information, covered contractor information system, and covered defense 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, Covered Defense Information and Cyber Incident Reporting, shall be implemented for all covered defense information on all covered contractor information systems that support the performance of this contract.

(c) If the Offeror proposes to deviate from any of 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, http://dx.doi.org/10.6028/NIST.SP.800-171 that is 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 CIO, a written explanation of—

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

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

(d) An authorized representative of the DoD CIO will approve or disapprove offeror requests to deviate from NIST SP 800-171 requirements in writing prior to contract award. Any approved deviation from NIST SP 800-171 shall be incorporated into the resulting contract.

(End of provision)

13. Add section 252.204-7009 to read as follows:

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:

LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (AUG 2015)

(a) Definitions. As used in this clause—

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 information that—

(1) Is—

(i) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

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

(2) Falls in any of the following categories:

(i) Controlled technical information.

(ii) Critical information (operations security). Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(iii) Export control. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and

nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

(iv) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).

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.

(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 the substance of this clause, including this paragraph (c), in all subcontracts 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.

(End of clause)

14. Revise section 252.204-7012 to read as follows:

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

As prescribed in 204.7304c, use the following clause:

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (AUG 2015)

(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.

Contractor information system means an information system belonging to, or operated by or for, the Contractor.

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 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 information that—

(i) Is—

(A) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

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

(ii) Falls in any of the following categories:

(A) Controlled technical information.

(B) Critical information (operations security). Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(C) Export control. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

(D) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).

Cyber incident means actions taken through the use of computer networks that result in 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.

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 information is recorded, stored, or printed within an 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.

Rapid(ly) report(ing) 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.

(b) Adequate security. The Contractor shall provide adequate security for all covered defense information on all covered contractor information systems that support the performance of work under this contract. To provide adequate security, the Contractor shall—

(1) Implement information systems security protections on all covered contractor information systems including, at a minimum—

(i) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government—

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

(B) 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; or

(ii) For covered contractor information systems that are not part of an IT service of system operated on behalf of the

Government and therefore are not subject to the security requirement specified at paragraph (b)(1)(i) of this clause—

(A) 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, http://dx.doi.org/10.6028/NIST.SP.800-171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer; or

(B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection approved in writing by an authorized representative of the DoD CIO prior to contract award; and

(2) Apply other security measures when the Contractor reasonably determines that such measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

(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, 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/certificate.html.

(d) 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.

(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 32CFR 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 the substance of this clause, including this paragraph (m), in all subcontracts, including subcontracts for commercial items; and

(2) Require subcontractors to rapidly report cyber incidents directly to DoD at http://dibnet.dod.mil and the prime Contractor. This includes providing the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable.

(End of clause)

15. Add section 252.239-7009 to read as follows:

252.239-7009 Representation of Use of Cloud Computing.

As prescribed in 239.7603(a), use the following provision:

REPRESENTATION OF USE OF CLOUD COMPUTING (AUG 2015)

(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 (b) 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)

16. Add section 252.239-7010 to read as follows:

252.239-7010 Cloud Computing Services.

As prescribed in 239.7603(b), use the following clause:

CLOUD COMPUTING SERVICES (AUG 2015)

(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.

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.

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.

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;

(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 the Department of Defense 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 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 the substance of this clause, including this paragraph (l), in all subcontracts that involve or may involve cloud services, including subcontracts for commercial items.

(End of clause)

[FR Doc. 2015-20870 Filed: 8/25/2015 08:45 am; Publication Date: 8/26/2015]