# PGI Part 239 - ACQUISITION OF INFORMATION TECHNOLOGY

PGI 239.71 -SECURITY AND PRIVACY FOR COMPUTER SYSTEMS

PGI 239.7102 Policy and responsibilities.

PGI 239.7102-3 Information assurance contractor training and certification.

PGI 239.74 -TELECOMMUNICATIONS SERVICES

PGI 239.7402 Policy.

PGI 239.7405 Delegated authority for telecommunications resources.

PGI 239.7406 Certified cost or pricing data and data other than certified cost or pricing data.

PGI 239.7407 Type of contract.

PGI 239.76 -CLOUD COMPUTING

PGI 239.7602 Policy and responsibilities.

PGI 239.7602-1 General.

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

PGI 239.7603 Procedures.

PGI 239.7603-1 General.

PGI 239.7603-2 Notification of third party access requests.

PGI 239.7603-3 Cyber incident and compromise reporting.

PGI 239.7603-4 DoD damage assessment activities.

**Parent topic:** PGI Defense Federal Acquisition Regulation

## PGI 239.71 -SECURITY AND PRIVACY FOR COMPUTER SYSTEMS

### PGI 239.7102 Policy and responsibilities.

#### PGI 239.7102-3 Information assurance contractor training and certification.

(1) The designated contracting officer’s representative will document the current information assurance certification status of contractor personnel by category and level, in the Defense

Eligibility Enrollment Reporting System, as required by DoD Manual 8570.01-M, Information Assurance Workforce Improvement Program.

(2) DoD 8570.01-M, paragraphs C3.2.4.8.1 and C4.2.3.7.1, requires modification of existing contracts to specify contractor training and certification requirements, in accordance with the phased implementation plan in Chapter 9 of DoD 8570.01-M. As with all modifications, any change to contract requirements shall be with appropriate consideration.

# PGI 239.74 -TELECOMMUNICATIONS SERVICES

## PGI 239.7402 Policy.

(c) *Foreign carriers*.

(i) Frequently, foreign carriers are owned by the government of the country in which they operate. The foreign governments often prescribe the methods of doing business.

(ii) In contracts for telecommunications services in foreign countries, describe the rates and practices in as much detail as possible. It is DoD policy not to pay discriminatory rates. DoD will pay a reasonable rate for telecommunications services or the rate charged the military of that country, whichever is less.

(iii) Refer special problems with telecommunications acquisition in foreign countries to higher headquarters for resolution with appropriate State Department representatives.

(d) *Long-haul telecommunications services.*DISA will acquire all long-haul telecommunications services for DoD. See DoD Directive 5105.19, Defense Information Systems Agency (DISA).

## PGI 239.7405 Delegated authority for telecommunications resources.

Related Documents:

Documents related to DoD’s delegated authority to enter into telecommunications service contracts are available here.

## PGI 239.7406 Certified cost or pricing data and data other than certified cost or pricing data.

Examples of instances where certified cost or pricing data, if required in accordance with FAR 15.403-4, or data other than certified cost or pricing data, if required in accordance with FAR 15.403-3, may be necessary to support price reasonableness include—

(1) Nontariffed services;

(2) Special rates and charges not included in a tariff, whether filed or to be filed;

(3) Special assembly rates and charges;

(4) Special construction and equipment charges;

(5) Contingent liabilities that are fixed at the outset of the service;

(6) Proposed cancellation and termination charges under the clause at 252.239-7007, Cancellation or Termination of Orders, and reuse arrangements under the clause at 252.239-7008, Reuse Arrangements;

(7) Rates contained in voluntary tariffs filed by nondominant common carriers; or

(8) A tariff, whether filed or to be filed, for new services installed or developed primarily for Government use.

### PGI 239.7407 Type of contract.

When using a basic agreement in conjunction with a communication service authorization—

(1) Use DD Form 428, Communication Service Authorization (CSA), or an electronic data processing substitute to award, modify, cancel, or terminate telecommunications services. The CSA shall—

(i) Refer to the basic agreement;

(ii) Specify the types and quantities and equipment to be provided as well as the tariff (or other price if a tariff is not available) of those services and equipment;

(iii) Specify the premises involved;

(iv) Cite the address for billing;

(v) Identify the disbursing office;

(vi) Provide funding information; and

(vii) Include an expiration date.

(2) Before awarding a CSA, comply with the requirements in FAR and DFARS, e.g., for competition, reviews, approvals, and determinations and findings.

## PGI 239.76 -CLOUD COMPUTING

### PGI 239.7602 Policy and responsibilities.

#### PGI 239.7602-1 General.

(c)(6) When the clause at DFARS 252.239-7010 applies, the contracting officer shall provide the contractor with the name of the responsible Government official to contact in response to any spillage occurring in connection with the cloud computing services being provided. The requiring activity will provide the contracting officer with the name of the responsible official in accordance

with agency procedures, as required by Enclosure 7 of DoDM 5200.01-V3, DoD Information Security Program: Protection of Classified Information.

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

(b) Prior to authorizing storage of data outside the United States and outlying areas, the contracting officer must receive written authorization from the authorizing official.

## PGI 239.7603 Procedures.

**PGI 239.7603-1 General.**

(a) When the apparently successful offeror indicates in the provision at DFARS 252.239-7009 that cloud computing services will be used in the performance of the contract, the contracting officer shall review the DoD Cloud Service Catalog at http://www.disa.mil/Computing/Cloud-Services/Cloud-Support (look under the "Additional Information" tab for "Service Catalog") to verify that the cloud service provider's offering to be used in the performance of the contract has a provisional authorization prior to award (see DFARS 239.7602-1(b)).

(b) When the contractor indicated in the provision at DFARS 252.239-7009 that it did not anticipate the use of cloud computing services in the performance of the contract and requests, after award, in accordance with the clause at DFARS 252.239-7010(b)(1), that the contracting officer approve the use of cloud computing services in the performance of the contract, the contracting officer shall—

(1) Request approval from the requiring activity for the contractor to use cloud computing services; and

(2) If the requiring activity provides approval, review the DoD Cloud Service Catalog at http://www.disa.mil/Computing/Cloud-Services/Cloud-Support (look under the "Additional Information" tab for "Service Catalog") to verify that the cloud service provider's offering to be used in the performance of the contract has a provisional authorization (see DFARS 239.7602-1(b)).

**PGI 239.7603-2 Notification of third party access requests.**

When a contractor provides notification of a request from a third party for access to Government data or Government-related data, in accordance with DFARS 252.239-7010(j), the contracting officer shall convey the request to the requiring activity. The requiring activity will coordinate a response with the mission or data owner.

**PGI 239.7603-3 Cyber incident and compromise reporting.**

(a) When a cyber incident is reported by a contractor, the DoD Cyber Crime Center (DC3) will send an unclassified encrypted email containing the cyber incident report to the contracting officer(s) identified on the Incident Collection Format (ICF). The DC3 may request the contracting officer to

send a digitally signed email to DC3.

(1) The procuring contracting officer (PCO) shall notify the requiring activities that have contracts identified in the ICF. In cases where an administrative contracting officer (ACO) receives the cyber incident report, in lieu of the PCO, the ACO shall notify the PCO for each affected contract, who will then notify the requiring activity.

(2) In cases of cyber incidents involving multiple contracts, the DoD components will work together to designate a single contracting officer to coordinate the effort. The requiring activity will notify the contracting officer once a lead is designated.

(b) When requested by the contractor, the contracting officer shall provide the contractor with the "Instructions for Malware Submission" document available at http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions_for_Submitting_M... . The contracting officer should never receive malicious software directly from the contractor.

(c) If the requiring activity requests access to contractor information or equipment, in accordance with DFARS 252.239-7010(g), the contracting officer shall provide a written request to the contractor.

(d) For additional information on cyber incident reporting, see the frequently asked question document at http://www.acq.osd.mil/dpap/pdi/network_penetration_reporting_and_contr... .

**PGI 239.7603-4 DoD damage assessment activities.**

(a) Prior to initiating damage assessment activities, the contracting officer shall verify that a contract(s) identified in the cyber incident report include(s) the clause at DFARS 252.239-7010. If the contracting officer determines that a contract identified in the report does not contain the clause, the contracting officer shall notify the requiring activity that damage assessment activities, if required, may be determined to constitute a change to the contract.

(b) In cases of cyber incidents involving multiple contracts, a single contracting officer will be designated to coordinate with the contractor regarding media submission.

(c) If the requiring activity requests the contracting officer obtain media, as defined at DFARS 252.239-7010, from the contractor, the contracting officer shall—

(1) Provide a written request for the media;

(2) Provide the contractor with the "Instructions for Media Submission" document available at http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions_for_Submitting_M...; and

(3) Provide a copy of the request to DC3, electronically via email at dcise@dc3.mil, and the requiring activity.

(d) If the contracting officer is notified by the requiring activity that media are not required, the contracting officer shall notify the contractor and simultaneously provide a copy of the notice to DC3 and the requiring activity.

(e) The contracting officer shall document the action taken as required by paragraph (c) or (d) of this section, in the contract file.

(f) Upon receipt of the contractor media, DC3 will confirm receipt in writing to the contractor and the requesting contracting officer.

(g) When the requiring activity determines that the damage assessment activities are complete, the requiring activity will provide the contracting officer with a report documenting the findings from the damage assessment activities affecting covered defense information.

(h) The contracting officer shall include the report documenting the findings in the contract file(s) and provide a copy to the contractor.