Part 504 - Administrative Matters

Parent topic: General Services Administration Acquisition Manual

Subpart 504.1 - Contract Execution

504.101 Contracting officer’s signature.

Contract, contract modifications, blanket purchase agreements, and task and/or delivery orders may be executed manually or electronically using a digital signature. In the absence of the original contracting officer, another contracting officer with appropriate warrant authority may sign. Always type or stamp the name and title of the contracting officer signing the contract on the document, unless it is electronically signed. An electronic contract which includes the name of the contracting officer satisfies the typed, stamped or printed requirement found in FAR 4.101. GSA Order CIO 2162.2, GSA Digital Signature Policy, is the guidance for the use of digital signatures as the preferred means of providing signatures for GSA documents, forms, correspondence, and emails.

504.103 [Reserved].

Subpart 504.2 - Contract Distribution

504.201 Procedures.

(a) The contracting officer must send documentation to the paying office on all contracts for which GSA generates a delivery or task order.

(1) For Federal Acquisition Service contracts entered into the FSS-19 system, the contracting officer must send a system generated contract listing.

(2) For all other contracts, the contracting officer must send a “Duplicate Original” of the entire contract or modification.

(b) The contracting officer must certify that the “Duplicate Original” is a true copy of the contract, modification, task and/or delivery order, if not electronically signed, by writing your signature, in ink, on the award or modification form (i.e., SF 26, 33, 1442, etc.). The contracting officer must certify all contracts except:

(1) Leases of real property.

(2) Schedule contracts.

(3) Standard or GSA multipage purchase/delivery/task order carbon forms.

504.203 Taxpayer identification information.

FAR 4.203(a) does not apply to leases of real property (see 504.904) or FAR 38 Federal Supply Schedule Contracting.

Subpart 504.4 - Safeguarding Classified Information Within Industry

504.402 General.

(a) This subpart prescribes procedures for safeguarding classified information required to be disclosed to contractors in connection with the solicitation of offers, and the award, performance, and termination of contracts.

(b) As used in this subpart, the term “Contractor(s)” means prospective contractors, subcontractors, vendors, and suppliers.

504.470 Acquisitions involving classified information.

HCA’s must consider how adequate security will be established, maintained, and monitored before accepting a reimbursable agreement for a requirement involving classified information. Further, HCAs are responsible for ensuring that the contracting officers, other procurement personnel, and contracting officer representatives (CORs) assigned to the acquisition have the appropriate security clearances, prior to accepting a reimbursable agreement involving access to, or generation of, classified information.

504.470-1 [Reserved].

504.470-2 [Reserved].

504.471 Processing security requirements checklist (DD Form 254).

(a) The contracting officer must prepare DD Form 254, Contract Security Classification Specification (illustrated in FAR 53.303-DD-254), for contracts involving contractor access to classified information. This form identifies for contractors the areas of classified information involved. The contracting officer may use written notice of classification for research or service contracts.

(b) Obtain instructions or guidance on completing DD Form 254 from the Security and Emergency Management Division, Office of Mission Assurance (OMA).

504.472 Periodic review.

(a) The contracting officer in coordination with the appropriate program security officer must review DD Form 254 at least once a year, or whenever a change in the phase of performance occurs, to determine if the classified information can be downgraded or declassified.

(b) The contracting officer must inform the contractor of the results of the review by one of the following means:

(1) Issuance of a revised specification.

(2) Written instructions instead of DD Form 254, if authorized.

(3) Written notification if the review results in no change in the classification specifications.

(c) The contracting officer must prepare a final checklist upon termination or completion of the contract in accordance with FAR 4.805-5.

504.473 Recurring procurement.

The contracting officer must prepare a new DD Form 254 only if a change occurs in either of the following:

(a) End item.

(b) Previous security classification.

504.474 Control of classified information.

(a) The contracting officer must record, mark, handle, and transmit classified information in accordance with the requirements of the Security Branch Chief, Security and Emergency Management Division, Office of Mission Assurance (OMA).

(b) The contracting officer must obtain the consent of the originating agency before releasing classified information to a contractor.

504.475 Return of classified information.

(a) Contracting officers must recover classified information, unless it has been destroyed as provided in Section 7 of Chapter 5 of the National Industrial Security Program Operating Manual (NISPOM). Information on NISPOM can be found at https://fas.org/sgp/index.html.

(b) Contracting officers must ensure that classified information provided by the government is returned immediately after any of the following events:

(1) Bid opening or closing date for receipt of proposals by non-responding offerors.

(2) Contract award by unsuccessful offerors.

(3) Termination or completion of the contract.

(4) Notification that authorization to release classified information has been withdrawn.

(5) Notification that a facility:

(i) Does not have adequate means to safeguard classified information; or

(ii) Has had its security clearance revoked or inactivated.

(6) Whenever otherwise instructed by the authority responsible for the security classification.

(c) The Government agency that provided classified information to a GSA contractor is responsible for the return of the information.

504.476 Breaches of security.

GSA employees responsible for the protection of classified information must refer the facts of an unauthorized disclosure promptly to Security Branch Chief, Security and Emergency Management Division, Office of Mission Assurance (OMA).

Subpart 504.5 - Electronic Commerce in Contracting

504.500 [Reserved].

504.502 Policy.

Use of electronic signatures is encouraged and can be used to sign and route documents in GSA's IT systems to contractually obligate funds. The method of authentication used for electronic signatures shall be consistent with the level (1-4) determined from the e-authentication risk assessment in accordance with OMB M-04-04, E-authentication Guidance for Federal Agencies, and the respective technology safeguards applicable to that level or risk from National Institute of Standards and Technology 800-63, Electronic Authentication Guideline.

504.570 [Reserved].

Subpart 504.6 - Contract Reporting

504.604 Responsibilities.

In accordance with FAR 4.604, the Senior Procurement Executive (SPE) has implemented the following policies to monitor and ensure the accurate and timely input of data into FPDS. Additional guidance is available on GSA's Acquisition Portal at https://insite.gsa.gov/acquisitionportal.

(a) *Contract writing systems*.

(1) The responsibility of the contracting officer to report awards in FPDS per FAR 4.604 may be accomplished by a contract writing system that reports the contract action directly to FPDS.

(2) Contract writing systems capable of reporting directly into FPDS shall be configured to report as a condition of making an award.

(3) Contract actions reported through contract writing systems shall be routinely examined and compared to data contained in FPDS to ensure that those actions have been reported accurately to FPDS.

(b) *Quarterly Reviews*.

(1) The HCAs are responsible for the following:

(i) Establishing a selection methodology for an appropriate random sample of contract files for review that is representative of their Service's contract actions. The sample does not need to be statistically significant.

(ii) Verifying and validating the accuracy of contract action reports (CARs) entered into FPDS through the reviews.

(iii) Submitting a certification of the accuracy of the CAR data to the Chief Acquisition Officer (CAO). Certifications are due no later than 30 business days after the end of the quarter.

(2) Any data discrepancies identified in the contract file during the verification and validation process shall be corrected.

(3) File selection and review may begin immediately after the end of each quarter using the selection methodology determined by the HCA in paragraph (b)(1)(i) of this section.

(c) *Annual Reviews*.

(1) In accordance with FAR 4.604(c), the CAO shall annually sample the GSA FPDS records and provide a list of transactions to each HCA for verification, validation, and certification.

(2) The verification and validation shall be conducted by an organization or person that did not award the contracts being reviewed. HCAs may institute any appropriate process that complies with this requirement.

(3) The process to verify and validate shall include comparisons of contract file data to FPDS data entries and comparisons of FPDS data to contract writing system data to determine completeness and accuracy, if applicable.

(4) HCAs shall provide certifications of the accuracy and validity of their FPDS data to the CAO based on the list of transactions provided to HCAs under paragraph (c)(1) of this section.

(5) Certifications to the CAO shall include a description of the means used to verify the accuracy and completeness of the data and a statement that all discrepancies found have been corrected.

504.605 Procedures.

(a) *Uniform procurement instrument identification*. This subpart:

(1) Prescribes procedures for identifying contracts, orders, and other procurement instruments regardless of dollar threshold.

(2) Applies to all contracting activities, except real property leasing.

(b) *Transition of procurement instrument identifier (PIID) numbering.*

(c) *Policy.*

(1) Contracting officers shall use the uniform PIID numbering requirements for procurement instruments reported to FPDS.

(2) Complete the contract number block provided on the applicable forms. If a space is not reserved for the prescribed number, place the number in the upper right-hand corner of the form.

(3) Each contracting office must maintain records to ensure continuity and control of PIID numbering.

(d) *Activity Address Codes (AACs).*

(1) AACs are made up of the following:

(i) The first two characters of the AAC must be “47” to identify GSA.

(ii) The third character must be the service/office code identified as follows:

Service/Office Code	Letter Designation
Office of the Administrator	A
Office of the Chief Financial Officer	B
Office of Human Resources Management	C
Office of Mission Assurance	D
Office of Small Business Utilization	E
Office of GSA IT	F
Civilian Board of Contract Appeals	G

Service/Office Code	Letter Designation
Office of Administrative Services	H
Office of Inspector General	J
Office of General Counsel	L
Office of Governmentwide Policy	M
Public Buildings Service	P
Federal Acquisition Service	Q
Congressional & Intergovernmental Affairs	S
Office of Communications and Marketing	Z

(iii) The remaining characters are determined by each service organization, and can be found on GSA's Acquisition Portal at https://insite.gsa.gov/acquisitionportal.

(2) Central Service Point (CSP) individuals are responsible for establishing and updating AAC assignments in the Department of Defense Activity Address Directory (DoDAAD). Additional guidance on AAC assignments and updates can be found on GSA's Acquisition Portal at https://insite.gsa.gov/acquisitionportal.

504.605-70 Federal Procurement Data System Public–Access to Data.

(a) *The FPDS database*. The General Services Administration awarded a contract for creation and operation of the Federal procurement Data System (FPDS) database. That database includes information reported by departments and agencies as required by FAR subpart 4.6. One of the primary purposes of the FPDS database is to provide information on Government procurement to the public.

(b) *Fee for direct hook-up*. To the extent that a member of the public requests establishment of real-time integration of reporting services to run reports from another application, a one-time charge of $2,500 for the original integration must be paid by the requestor. This one-time charge covers the setup and certification required for an integrator to access the FPDS database and for technical assistance to help integrators use the web services. The fee will be paid to the FPDS contractor and credited to invoices submitted to GSA by the FPDS contractor.

504.606 Reporting Data.

(a) *Reporting requirements*. Detailed specification of FPDS data reporting requirements is contained in the FPDS-NG FAQs document available at https://www.fpds.gov/. Reporting offices are encouraged to use automated information systems for FPDS data reporting, provided that the systems contain all required FPDS data elements via the machine-to-machine process and the automated acquisition system has received the proper certification from the FPDS system manager.

(b) The GSA FPDS Sustainability Coding Guidelines found on GSA's Acquisition Portal at https://insite.gsa.gov/acquisitionportal must be followed when selecting codes for the following sustainability data elements:

(1) Recovered Materials/Sustainability.

(2) Use of EPA Designated Products.

(c) FPDS reporting for acquisitions supporting customer agencies.

(1) *GSA-funded acquisitions*. There are instances where GSA conducts an acquisition in support of a customer agency but also provides the predominance of funding for the contract award. In these instances, GSA’s Activity Address Codes (AACs) must be used for the contracting agency codes (e.g. Contracting Office ID) and funding agency codes (*e.g.* Funding Office ID) in FPDS. Examples of GSA funded acquisitions may include those made in support of—

(i) Requisitions. These transactions are transfers of property conducted in accordance with the Federal Property Management Regulation (FPMR) (41 CFR 101-26). Examples of programs that facilitate requisitions from customer agencies include GSA stock supply programs and GSA motor vehicle purchasing. Customer agencies submit requisitions (sometimes referred to as “orders”) to GSA for items under these programs in accordance with the FPMR. GSA then acquires these items from suppliers through contracts or orders in accordance with the FAR and GSAM.

(ii) Shared Services. Under this model, common administrative services-those activities that are common across all agencies-are conducted by an agency (*e.g.* shared service provider) with expertise in a particular area to reduce duplication and redundancy. In turn, the customer agency reimburses the shared service provider for its costs. Often, shared service providers must conduct acquisitions in order to provide services to other agencies. Accordingly, only the contract/order awarded by the shared service provider to a contractor is reported in FPDS.

(2) *Customer-funded acquisitions*. There are instances where GSA conducts an acquisition in support of a customer agency but the customer agency provides the predominance of funding for the contract action. In these instances, GSA’s AACs must be used for the contracting agency codes (*e.g.* Contracting Office ID) but the customer agency's AACs must be used for funding agency codes (e.g. Funding Office ID) in FPDS. Examples of customer-funded acquisitions may include—

(i) Reimbursable Work Authorizations (RWAs). An RWA is an interagency agreement between GSA and a tenant (*e.g.* federal agency or non-federal source when authorized by statute) whereby GSA recovers its costs for altering, renovating, repairing, or providing services in GSA-managed space over and above the basic operations financed through rent paid by the tenant.

(ii) Assisted acquisitions (see definition at FAR 2.101). GSA regularly acts as the servicing agency in this type of interagency acquisition, where it performs acquisition activities on a customer (requesting) agency's behalf, such as awarding and administering a contract, while the requesting agency provides the required funding.

(d) *Inherently Governmental Functions*. If the procurement is for services, enter the appropriate indicator in the Inherently Governmental Functions field:

(1) “Closely Associated” means functions that are closely associated with inherently governmental functions; those contractor duties that could expand to become inherently governmental functions without sufficient management controls or oversight on the part of the Government. Office of Federal Procurement Policy (OFPP) Policy Letter 11–01, Performance of Inherently Governmental and Critical Functions, provides examples of work that is inherently governmental and therefore must be performed by Federal employees and work that is closely associated with inherently governmental functions that may be performed by either Federal employees or contractors.

(2) “Critical Functions” means functions that are necessary to the agency being able to effectively perform and maintain control of its mission and operations. Typically, critical functions are recurring and long-term in duration.

(3) “Other Functions” means neither “Closely Associated Functions” nor “Critical Functions.”

(4) For services that include performing both “Closely Associated” and “Critical Functions,” select “Closely Associated, Critical Functions.”

Subpart 504.8 - Government Contract Files

504.800 Scope of subpart.

(a) This subpart prescribes a contract file format standard for all contracts that exceed the micro-purchase threshold. This subpart may be applied to purchases at or below the micro-purchase threshold.

(b) The purpose of this standard is to ensure that the documentation in the file complies with FAR 4.801(b)(1) and FAR 4.802(c) requirements.

504.802 Contract files.

(a) Contract files shall be maintained electronically, unless otherwise determined, in writing, by the HCA to be prohibitively burdensome.

(b) The contracting officer must place all information and documentation required by FAR 4.802 and 4.803 in the contract file and organize the file in the format as set out in each individual contracting activity's contract file standard.

(c) Contracting officer responsibilities.

(1) The contracting officer is responsible for the official contract file. Individuals creating documents relating to the contract must provide those documents to the contracting officer for inclusion in the file. Other members of the acquisition team may be responsible for the maintenance and archival of any delegated responsibilities (*e.g.*, contract administration and delegated contract administration function) according to prescribed contracting activity policies and procedures.

(2) The contracting officer shall-

(i) Place all information and documentation required by the FAR (see FAR subpart 4.8), the GSAM, and any other policy and procedure in the contract file.

(ii) Include an index or checklist identifying the location of any documentation contained in the contract file when such identification is not already prescribed by policy. The index or checklist can be electronic.

(iii) Identify in a clear and logical manner, within the contract file, any documentation maintained in another location.

(iv) Comply with applicable file and document naming convention/nomenclature requirements.

(3) When responsibility for a contract transfer from one contracting officer to another contracting officer (*e.g.*, employee departure, transfer of assignments, or redelegation of contract administration authority (intraoffice or interoffice))-

(i) The successor contracting officer shall review the files being transferred. The purpose of the review is to identify any issues with the contract file (*e.g.*, missing or incomplete documentation or information).

(ii) The successor contracting officer shall attempt to resolve any issues identified during their review of the transferred files. The successor contracting officer should write a memo-to-file that documents any issues with the contract file that were not able to be resolved as part of the transfer.

(d) Head of contracting activity responsibilities. Head of contracting activities consistent with their delegated authorities are responsible for-

(1) Developing policies and procedures that discuss, at a minimum, the following:

(i) The different types of files identified in FAR 4.801(c) along with any other files that are to be established (*e.g.*, unsolicited proposals);

(ii) The location where file documentation is to be stored (*e.g.*, an electronic contract filing system, another official system of record, or some type of combination thereof). If file documentation must be stored in different locations, the policy and procedure shall discuss the rationale for the need (*e.g.*, separation of classified and unclassified documentation) and medium (*e.g.*, paper) to be used;

(iii) The approach used to identify the documents to be retained within a contract file (see FAR 4.803) and any other files established per paragraph (d)(1)(ii) of this section (*e.g.*, use of a checklist or index that includes the citation of the authority for retaining a document);

(iv) The organization(s) or individual(s) responsible for maintaining file documentation when such responsibility does not reside with the contracting officer (see 504.802(b));

(v) The filing and document convention/nomenclature to be used;

(vi) The content, access, and other applicable requirements for contracting officer representative (COR) contract files (see FAR 1.604) and any other files (see paragraph (a) of this section); and

(vii) The internal controls (*e.g.* quarterly review by the contracting activity) to be used for ensuring compliance with FAR, GSAM, and other requirements.

(2) Designating a point of contact within its organization for purposes of supporting file audits and reviews by internal and external organizations (*e.g.*, the Procurement Management Review (PMR) office). Support may include, but not be limited to:

(i) Providing copies of applicable policies and procedures;

(ii) Assisting in resolving issues (*e.g.*, locating a contract file) and questions;

(iii) Providing access to files and systems; and

(iv) Notifying the contracting officer of the status of the review or audit.

504.803 Contents of contract files.

In addition to the examples of contract file documents described in FAR 4.802 and listed in FAR 4.803, the contract file shall include, if applicable, the following:

(a) GSA Form 2689 (see 519.502-70 for applicability), and

(b) Checklist documenting review of the small business subcontracting plan (see 519.705-4 for applicability).

(c) Documents required by individual contracting activity in accordance with such activity's internal policies and procedures.

504.804 Closeout of contract files.

504.804-5 Procedures for closing out contract files.

(a) *Contracting Officer Responsibilities Upon Evidence of Physical Completion.* Upon receipt of evidence of physical completion of a contract, the contracting officer must, within 14 calendar days, ensure input of the status of “physically complete” (or similar) into any contract administration and/or financial systems applicable to the contract.

(b) *Contracting Officer Responsibilities To Reconcile Financial Balances of Physically Completed Contracts.*

(1) Upon receipt of evidence of physical completion of a contract (including those contracts using simplified acquisition procedures), the contracting officer must, within 14 calendar days, determine if any outstanding financial balance exists. The contracting officer may request, as needed, information from the Office of the Chief Financial Officer (OCFO).

(2) The contracting officer must reconcile any outstanding balances (*e.g.*, through discussing final billings with contractors, descoping, deobligating funds, cancelling the contract in whole or in part, or terminating the contract in whole or in part, as applicable). The contracting officer must then take the necessary corrective actions to resolve such financial balances, in coordination with OCFO as needed.

(3) Contracting officers must notify OCFO within 30 days of receipt of evidence of physical

completion, of all known or anticipated excess financial balances remaining that meet or exceed $100,000, that have not previously been communicated to OCFO through other means such as regular OCFO data calls. Excess financial balances are any known or anticipated financial balances after receipt and payment of the final invoice or billing from the contractor (*e.g.*, the amount expected remaining to be deobligated or descoped by the contracting officer).

504.805 Storage, handling, and disposal of contract files.

The contracting officer’s accountability for contract files ends when the following three conditions exist:

(a) The files’ retention period expires.

(b) The contracting officer receives the notice of disposal from the National Archives and Records Administration.

(c) The records liaison officer whose organization has functional responsibility for the files approves disposal.

Subpart 504.9 - Taxpayer Identification Number Information

504.902 General.

(a) *Debt collection*. The Debt Collection Improvement Act of 1996 requires each contractor doing business with GSA to furnish its Tax Identification Number (TIN). The Government is required to include with each certified voucher prepared and submitted to a disbursing official, the TIN of the contractor receiving payment under the voucher. The TIN may be used by the Office of Financial Policy and Operations to collect and report on any delinquent amounts arising out of the contractor's relationship with the Government.

(b) *Information reporting to the IRS*. The TIN is also required for Office of Financial Policy and Operations reporting of certain contract information (see FAR 4.903) and payment information (see GSAM 504.904) to the IRS.

504.904 Reporting contract information to the IRS.

(a) The Office of Financial Policy and Operations reports to IRS on payments made to certain contractors for services performed and to lessors for providing space in buildings. This is required by 26 U.S.C. 6041 and 6041A and implemented in 26 CFR. To assist the Office of Financial Policy and Operations in reporting to the IRS, contracting officers must indicate on obligating documents sent to Finance (*e.g.*, purchase, delivery, or task orders; contracts; or certified invoices) the contractor's organizational structure (*e.g.*, corporation, or partnership) and taxpayer identification number (TIN).

Subpart 504.11 - System for Award Management

504.1103 Procedures.

In addition to the requirements found in FAR 4.1103, prior to awarding a contractual instrument the contracting officer must-

(a) Verify that the prospective contractor's legal business name, Doing-Business-As (DBA) name (if any), physical street address, and unique entity identifier, as found in the System for Award Management (SAM), match the information that will be included in the contract, order, or agreement resulting from the vendor's quote or proposal. Correct any mismatches by having the vendor amend the information in the SAM and/or the quote or proposal.

(b) Ensure that the contractor's address code exists in Pegasys and that it is SAM enabled with the contractor's unique entity identifier. This can be done by searching Pegasys records using the contractor's Taxpayer Identification Number (TIN). If no code exists, request that a new address code be established by the Finance Center for SAM compliance.

(c) Ensure that the contractor's identifying information is correctly placed on the contractual instrument, using special care to ensure that the legal name and "remit to" name match exactly. (Note: Lockbox names or numbers should not be used to replace the contractor's name in the remittance block on the contractual instrument.)

(d) Unless one of the exceptions to registration in SAM applies (see FAR 4.1102(a)), the contracting officer must not award a contract to a prospective contractor who is not registered in SAM. If no exceptions are applicable, and the needs of the requiring activity allows for a delay in award, see FAR 4.1103(b)(1).

Subpart 504.13 - Personal Identity Verification of Contractor Personnel

504.1301 Policy.

Contracting officers must follow the procedures contained in CIO P2181.1 - GSA HSPD-12 Personal Identity Verification and Credentialing Handbook, which may be obtained from the CIO Office of Enterprise Solutions, to ensure compliance with Homeland Security Presidential Directive-12 (HSPD-12) "Policy for a Common Identification Standard for Federal Employees and Contractors," Office of Management and Budget Memorandum M-05-24, and Department of Commerce FIPS PUB 201.

504.1303 Contract clause.

Insert the clause at 552.204-9, Personal Identity Verification Requirements, in solicitations and contracts when it is determined that contractor employees will require access to federally controlled facilities or information systems to perform contract requirements.

504.1370 GSA Credentials and Access Management Procedures.

(a) General.

The CIO P 2181.1 - GSA HSPD-12 Personal Identity Verification (PIV) and Credentialing Handbook includes guidance for–

(1)Managing contract employee credentials;

(2) Ensuring contract employee credentials are returned to the GSA Office of Mission Assurance (OMA) when a contractor employee receives an unfavorable suitability determination, leaves the contract or when a contract ends; and

(3) Disabling access to information technology when a contractor employee leaves the contract or when a contract ends.

(b)Delegating Responsibilities.

(1) Contracting officers must manage PIV cards, also referred to as “GSA Access Cards”, provided to contractor employees. Contracting officers may delegate this authority to a contracting officer’s representative.

(2) If delegated, the contracting officer must ensure any contracting officer's representative delegation letter includes language for credentials and access management responsibilities.

(3) The Government contracting official who requests PIV cards on behalf of a contractor employee is also referred to as a “requesting official” pursuant to CIO P 2181.1.

(4) Standard delegation language can be found on GSA's Acquisition Portal at https://insite.gsa.gov/acquisitionportal.

(c) Required Verifications. There are multiple types of verifications to ensure only contractor employees who require PIV cards have them.

(1) Automated verification.

(i) Contractors and authorized Government contracting officials are automatically notified prior to the end date of the contract period of performance listed in the Office of Mission Assurance (OMA) system GSA Credentialing and Identity Management System (GCIMS). PIV cards will be automatically inactivated 30 days after the period of performance.

(ii) If the contractor requires a PIV card beyond 30 days after the contract period of performance, the authorized Government contracting official must submit a contractor information worksheet (CIW) (GSA Form 850) to update GCIMS, including appropriate justification.

(iii) When a contractor is made inactive in GCIMS, GCIMS will send an email to contractors and authorized Government contracting officials notifying everyone that the contractor PIV card needs to be returned. If the contractor does not comply with the terms of the automated notification, the authorized Government contracting official shall take the actions listed in paragraph (d).

(iv) The contracting officer shall include documentation in the contract file, as necessary.

(2) Manual verification.

(i) Authorized Government contracting officials are required to conduct a PIV card review annually or prior to exercising an option (see 517.207(c)), whichever comes first, to verify the contract information in GCIMS is correct (e.g. contract number, contract period of performance, contractor point of contact).

(ii) Authorized Government contracting officials shall send a letter to contractors to determine the need for continued access of individual employees and for return of PIV cards, requesting a response within no more than 15 business days.

(iii) Authorized Government contracting officials are required to submit a contractor information worksheet (CIW) (GSA Form 850) to update GCIMS, as necessary.

(iv) The contracting officer shall include documentation in the contract file, as necessary.

(d) The authorized Government contracting official shall take the following actions when a contractor fails to return PIV cards.

(1) Withhold Final Payment. COs may delay final payment under a contract if the contractor fails to comply with the PIV card requirements in accordance with paragraph (c) of FAR 52.204-9.

(2) Contractor Performance Assessment Rating System (CPARS). The Contracting Officer shall include within CPARS evaluations instances where a contractor fails to return a PIV card or other Government Furnished Equipment (GFE). This information shall be noted within the narrative of the CPARS "Regulatory Compliance" contractor performance evaluation factor (see subpart 542.15).

(3) Suspension/Debarment Referral Considerations. For willful non-compliance, the CO shall refer the contractor to the Suspension and Debarment Official (SDO). The SDO will review the complaint and decide whether or not action should be taken against the contractor.

(4) Termination Considerations. If the contractor shows a pattern of willful non-compliance regarding PIV card requirements during the performance of the contract (*e.g.*, annual review of PIV cards), the CO may terminate the contract.

(e) The CIO P 2181.1 - GSA HSPD-12 Personal Identity Verification and Credentialing Handbook, as well as additional resources for implementing the credentials and access management requirements, can be found on the Acquisition Portal at: https://insite.gsa.gov/hspd12inprocurement.

Subpart 504.16 - Unique Procurement Instrument Identifiers

504.1603 Procedures.

(a) *Elements of a PIID*. The PIID consists of 13 alphanumeric characters as follows:

Character(s)	Content	Content Description Location	Example

Character(s)	Content	Content Description Location	Example
1-6	Activity Address Code	See 504.605	47PA01
7-8	Last Two Digits of Fiscal Year of Number Assignment		15
9	Instrument Code	See 504.1603(b)	F
10-13	Serial Number	See 504.1603(c)	0001

(b) *Procurement Instrument Type Codes*. Indicate the type of instrument consistent with the letter designation provided in FAR 4.1603(a)(3). The letter designations for the identified type of instruments unique to agency policy are identified as follows:

Instrument	Letter Designation
Purchase orders (open market simplified acquisition) - manual	M
Request for information	N
Standing price quote (SPQ)	T

(c) *Serial Number Codes*.

(1) A separate series of numbers may be used for each basic instrument type (see 504.1603(b)).

(2) For delivery or task orders, each order issued by contracting office must receive a consecutive serial number. That is, orders are numbered in sequence as issued by the contracting office, but they are not in sequence under any individual contract.

(3) At the beginning of each fiscal year, the first number assigned is 0001.

(4) Alphanumeric characters are serially assigned after the numeric series is exhausted.

(5) The allowable numeric and alphanumeric sequences, excluding alpha I and O are–

(i) 0001 through 9999;

(ii) A001 through A999, B001 through B999;

(iii) and so on to Z001 through Z999.

(6) Each issuing office is responsible for controlling serial number assignments.

504.1670 Unique identifier for procurements supporting a leasehold interest.

(a) *General*. Procurements supporting a leasehold interest include: architectural and engineering (A&E) design and other related activities, project management, construction, space alterations (irrespective of size or scope), security-related tenant buildout, building-specific security countermeasures, personal (moveable) property, and overtime utilities.

(b) *Procurement Actions*. Any procurement supporting a leasehold interest (including those at or below the micro-purchase threshold), including stand-alone contracts or lease amendments, must reference the associated lease number (8-character number such as LMA00001) in the system of record (e.g., EASi, G-REX, RETA, REXUS, Pegasys) in which that action is being processed or recorded, and on the procurement document. Data must be recorded in a standardized data field, as appropriate. For systems that do not have the capability to capture the associated lease number, the lease number may be placed on the procurement document itself alone.

(c) *Reimbursable Work Authorizations (RWAs)*.

(1) *RWAs prior to lease award*. For any RWA submissions (including at or below the micro-purchase threshold) where the lease is not yet awarded, the associated lease number (8-character number such as LMA00001) shall be input into the system of record for the RWA and on the procurement document, within 3 business days of the lease award date or the creation of a lease number, whichever is later. Data must be recorded in a standardized data field, as appropriate. For systems that do not have the capability to capture the associated lease number, the lease number may be placed on the procurement document itself alone.

(2) *RWAs after lease award*. For any RWA submissions (including at or below the micro-purchase threshold) where the lease is already awarded, the associated lease number (8-character number such as LMA00001) shall be input into the system of record for the RWA and on the procurement document. Data must be recorded in a standardized data field, as appropriate. For systems that do not have the capability to capture the associated lease number, the lease number may be placed on the procurement document itself alone.

Subpart 504.70 - Cyber-Supply Chain Risk Management

504.7000 Scope of subpart.

This subpart prescribes acquisition policies and procedures for mitigating cyber-supply chain risks of procurements funded by GSA. Procedures in this subpart apply to all GSA-funded contracts and orders, regardless of the estimated value of the solicitation, contract or order, including purchases under the micro-purchase threshold and purchases using a Government Purchase Card.

504.7001 Definitions.

“Cyber-Supply Chain Event” means any situation or occurrence in or to a network, information system, or within the supply chain, not purchased on behalf of another agency, that has the potential to cause undesirable consequences or impacts. Cyber-Supply Chain Events, as they relate to this subpart, can include:

(a) Occurrence of an IT security incident;

(b) Discovery of a prohibited article or source; and

(c) Identification of supply chain risk information.

“Cyber-Supply Chain Risk Management”, or “C-SCRM”, means management of cyber-related (or, more generally, technology-related) risks in all phases of the acquisition lifecycle and at all levels of the supply chain, regardless of the product(s) or service(s) procured.

“Cyber-Supply Chain Risk Management Policy Advisor” means the identified lead of the Service-level acquisition management (e.g., the Federal Acquisition Service’s Office of Policy and Compliance (OPC), the Public Building Service’s Office of Acquisition Management (OAM), the Office of Administrative Services).

“IT security incident” means an occurrence that:

(a) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system;

(b) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies;

(c) Results in lost, stolen, or inappropriately accessed Controlled Unclassified Information (CUI) (including Personally Identifiable Information (PII)), lost or stolen GSA-owned devices (mobile phones, laptops, Personal Identity Verification (PIV) cards), and any other incident included in CIO-IT-Security-01-02); or

(d) Results in a situation that severely impairs, manipulates, or shuts down the operation of a system or group of systems (e.g., Building Automation Systems, Heating, Ventilation, Air Conditioning (HVAC) systems, Physical Access Control Systems (PACS), Advanced Metering Systems, Lighting Control Systems).

“Prohibited article” means any prohibited product, system, or service that the contractor offers or provides to the Government that conflicts with the supply chain terms or conditions of the solicitation or contract (e.g., Federal Acquisition Security Council (FASC) exclusion order, GSA CIO Order, counterfeit items, or FAR provision or clause, including, without limitation, FAR Clause at 52.204-23, Prohibition on Contracting for Hardware, Software, Products and Services Developed or Provided by Kaspersky Lab and Other Covered Entities, FAR Provision at 52.204-24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment, and FAR Clause at 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment).

“Prohibited source” means any entity with which the Government may not enter into or renew a contract or from which the Government may not purchase products or services due to conflicts with the supply chain terms or conditions of the solicitation or contract (e.g., FASC exclusion order, GSA CIO Order, FAR provision or clause, contract-specific provision or clause).

“Supply chain risk information” is defined at 41 C.F.R. 201-1.101. Failure of an offeror to meet a solicitation’s requirements, including security requirements, will not by itself constitute supply chain risk information.

“Substantial supply chain risk information” means supply chain risk information that leads to any of

the following:

(a) Removal of a presumptive awardee from pre-award consideration or competition;

(b) Rejection of a proposed subcontractor;

(c) Removal of a subcontractor from a contract; or

(d) Termination of a contract.

504.7002 Policy.

(a)The Federal Information Security Modernization Act of 2014 (Public Law 113-283) and associated National Institute of Standards and Technology (NIST) guidance requires Federal agencies to manage supply chain risks for Federal information systems and to ensure the effectiveness of information security controls and risks.

(b)The SECURE Technology Act (Public Law 115-390), which includes the Federal Acquisition Supply Chain Security Act of 2018, established the Federal Acquisition Security Council (FASC) to improve executive branch coordination, supply chain information sharing, and actions to address supply chain risks and requires GSA to have a lead representative for the agency.

(c) OMB Circular A-130, “Managing Information as a Strategic Resource,” directs agencies to implement supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, and poor manufacturing and development practices throughout the system development life cycle.

(d) GSA Information Technology (IT) Security Procedural Guide CIO-IT Security-01-02, “Incident Response (IR)” (including successor policies), provides additional processes and procedures for incident response, as outlined by GSA’s Office of the Chief Information Security Officer (OCISO).

(e) GSA Information Technology (IT) Security Procedural Guide CIO-IT Security-21-117, “Office of the Chief Information Security Officer (OCISO) Cyber Supply Chain Risk Management (C-SCRM) Program” (including successor policies), establishes a C-SCRM program within GSA’s OCISO and serves as the Tier 2 plan for GSA.

(f) GSA CIO Order 2100.1, “GSA Information Technology (IT) Security Policy” (including successor policies), sets forth GSA’s IT security policy and establishes controls required to comply with Federal laws and regulations.

504.7003 General procedures.

(a) GSA contracting activities may discuss supply chain concerns with the relevant Cyber-Supply Chain Risk Management Policy Advisor(s) listed on the GSA Acquisition Portal (http://insite.gsa.gov/cscrm) at any time, including during acquisition planning, requirements development, and post award. Changes to this list shall be reported to spe.request@gsa.gov.

(b)In addition to the Cyber-Supply Chain Events listed in 504.7005, additional risks may require notification to GSA’s Office of Mission Assurance (OMA):

(1) Any law enforcement or criminal activity, suspicious packages, or damage to GSA infrastructure should be reported to the GSA Emergency Operations Center (as specified under GSA Order 2400.2) at EOC@gsa.gov or 202-219-0338.

(2)Insider threats, including acts of commission or omission by an insider who intentionally or unintentionally compromises an agency's ability to accomplish its mission (e.g., espionage, unauthorized disclosure of information, any activity resulting in the loss or degradation of departmental resources or capabilities) should be reported to the OMA Insider Threat Program at insider-threat-program@gsa.gov

504.7004 Acquisition Considerations.

(a) *Acquisition Planning*. For cyber-supply chain risk management acquisition planning considerations, see 507.105.html#GSAM_507_105 (f).

(b) *Market Research*. For cyber-supply chain risk management market research considerations, see 510.002 (c) and (d)

(c) *Evaluation*. As part of evaluating past performance, review the Contractor Performance Assessment Reporting System (CPARS) for any reported noncompliance with supply chain requirements and/or otherwise evaluate similar past performance information in accordance with the policies and procedures contained in the applicable subpart.

(d) *Pre-award*. Apparent successful offeror. If the apparent successful offeror responds that it “will” provide or “does” use covered telecommunications equipment or services in response to the representation provision at FAR 52.204-24 then, regardless of the offeror’s response to the SAM representation provision(s) (e.g., FAR 52.204-26, FAR 52.212-3(v)), clarify with the apparent successful offeror to ensure that it accurately completed the representation(s). After clarifying the apparent successful offeror accurately completed the representation(s), follow the procedures at 504.7005 (c) and consider the following:

(1) If the contracting officer determines that awarding to the apparent successful offeror will result in a violation of the prohibition at FAR 52.204-24(b), the contracting officer should determine that the offeror is not eligible for award and should move to the next offeror in line for award.

(2) If the contracting officer does not identify an eligible offeror, the acquisition team should explore other acquisition strategies, making a partial award, cancelling the solicitation, changing the requirement, or finding another approach that does not involve the use of covered telecommunications equipment or services.

(3) As a last resort, the acquisition team may consider pursuing a waiver for an offeror. The acquisition team should contact the appropriate Cyber-Supply Chain Risk Management Policy Advisor (see 504.7003 (a)) for assistance and coordination. Instructions for requesting a waiver are available on the GSA Acquisition Portal (http://insite.gsa.gov/cscrm).

504.7005 Notification procedures for cyber-supply chain events.

(a) *General*.

(1) For any potential cyber-supply chain event, including occurrence of an IT security incident,

discovery of a prohibited article or source, or identification of supply chain risk information, the contracting officer or another acquisition team member must contact the GSA IT Service Desk by phone at 866-450-5250 or by email at ITServiceDesk@gsa.gov.

(i) Do not include source selection sensitive information in the notification to the GSA IT Service Desk.

(ii) Do not include other sensitive information (e.g., IP address, access information such as an account login and password) in the notification to the GSA IT Service Desk. The notification should state that additional information is sensitive and will be provided in person or via a secured method.

(iii) Determining whether the identified issue or potential issue is applicable under the procedures for each event type should not delay the acquisition team member from submitting a notification. When unsure, it is better to notify quickly rather than delay the event notification. The GSA IT Service Desk can assist in defining the event type once submitted.

(b) *Occurrence of an IT security incident*.

(1) If an IT security incident occurs, concerning any GSA information system or data (owned or operated by GSA or by a contractor or other organization on behalf of GSA), regardless of the estimated value of the contract or order, including purchases under the micro-purchase threshold and purchases using a Government Purchase Card, the contracting officer or another acquisition team member must immediately contact the GSA IT Service Desk.

(2) The notification to the GSA IT Service Desk - whether via phone or email - should document as much information as possible, including:

(i) Description, date and time of the incident;

(ii) Whether any PII or contractor-attributional information is affected; and

(iii) Contract information (contract number, contractor name, name of GSA contracting office), as applicable.

(3) Do not delay notifying the GSA IT Service Desk even if all the information requested or considered to be relevant is not available.

(4) Additional guidance is available from the GSA IT Security Procedural Guide CIO-IT Security-01-02, “Incident Response (IR)”, and GSA IT Security Procedural Guide CIO-IT Security-21-117, “OCISO Cyber Supply Chain Risk Management (C-SCRM) Program”.

(5) After initial notification, GSA IT may request additional information and will work with the notifier to resolve the issue.

(c) *Discovery of a prohibited article or source* .

(1)If a prohibited article or source is discovered within the supply chain of a procurement, regardless of the estimated value of the solicitation, contract, or order, including purchases under the micro-purchase threshold and purchases using a Government Purchase Card, the contracting officer or another acquisition team member must immediately contact the GSA IT Service Desk.

(2)The notification to the GSA IT Service Desk - whether via phone or email - should document as much information as possible, including:

(i)Contract or solicitation information, including contract or solicitation number, contractor or offeror name, and name of GSA contracting office;

(ii)Prohibited article or source name; and

(iii)Reason why prohibited article or source is banned on contract.

(iv) A “critical date,” no less than three (3) business days in the future, for when a response from GSA’s Supply Chain Review Board is requested.

(3) Do not delay notifying the GSA IT Service Desk even if all the information requested or considered to be relevant is not available.

(4) After initial notification, GSA’s Supply Chain Review Board may request additional information and will work with the notifier to resolve the issue.

(i) If the SCRM Review Board has not responded by the “critical date” required by 504.7005(c)(2)(iv), the contracting officer may make a determination without the SCRM Review Board’s input, but should seek input and guidance from the appropriate Cyber-Supply Chain Risk Management Policy Advisor (see GSAM 504.7003(a)) and review additional guidance available on the GSA Acquisition Portal (http://insite.gsa.gov/cscrm) prior to making the determination.

(d) *Identification of supply chain risk information*.

(1)If substantial supply chain risk information is identified, or the contracting officer or another acquisition team member including the GSA Information Technology Office (GSA IT) (e.g., Chief Information Officer, Chief Information Security Officer) thinks supply chain risk information should be voluntarily shared with the FASC, the contracting officer or another acquisition team member must contact the GSA IT Service Desk. The GSA IT Service Desk will gather relevant information and share it with the appropriate Cyber-Supply Chain Risk Management Policy Advisor.

(i) Service-level policy may adopt additional procedures to provide acquisition team members with guidance prior to notifying the GSA IT Service Desk.

(2) After initial notification, the appropriate Cyber-Supply Chain Risk Management Policy Advisor may request additional information and will work with the notifier to resolve the issue.

(3) The Cyber-Supply Chain Risk Management Policy Advisors will share information with the Office of Acquisition Policy within OGP.

(4)OGP will share supply chain risk information with relevant GSA offices and personnel, as appropriate, and with the FASC when:

(i)The FASC requests information associated with a particular source, a covered article, or a covered procurement (as defined at 41 U.S.C. 4713(k));

(ii) GSA determines that a substantial supply chain risk associated with a source, a covered article, or a covered procurement exists as described in 41 C.F.R. 201-1.101; or

(iii) GSA identifies supply chain risk management information (including both C-SCRM and non-C-SCRM risks) associated with a source, a covered article, or a covered procurement action and deems such information relevant to share with the FASC.

(e) *Cyber-Supply Chain Event Risk Mitigation*. The contract administration procedures under FAR part 49 (*e.g.,* cure notice, termination for cause, past performance review) can be used as needed to address immediate or future supply chain event concerns. Additional guidance on contract administration procedures is available on the GSA Acquisition Portal (http://insite.gsa.gov/cscrm).

(f) *Past Performance Evaluation*. The contracting officer must report any contractor non-compliance with supply chain requirements within the "Other Areas" portion of any applicable past performance evaluation form.

Subpart 504.71 - Acquisition Reviews

504.7100 Scope of subpart.

This subpart prescribes policies and procedures concerning acquisition reviews. FAR part 18 acquisitions are exempt from this subpart.

504.7101 Purpose.

The purpose of this subpart is to–

(a) Support FAR parts 7, 10, and 11 to ensure requirements meet the needs of the customer, align and support the mission, are acquired efficiently and effectively, and comply with Federal and agency policies and procedures;

(b) Establish a requirement for acquisition reviews for various types of acquisitions and contract actions; and

(c) Promote early and frequent engagement by the SPE.

504.7102 General.

(a) An acquisition review is a type of internal control as well as a best practice that provides an opportunity for collaboration and meaningful conversation amongst members of the acquisition team and stakeholders. Acquisition reviews enable information to be shared early and often during the acquisition life cycle.

(b) The need for an acquisition review should be commensurate with the risk, complexity, and criticality of the acquisition or contract action. Criteria supporting the need for an acquisition review may include the criteria described in 507.103.html#GSAM_507_103 (b)(2).

(c) An acquisition may require more than one acquisition review. An acquisition review may occur at any time during the various phases of the acquisition life cycle:

(1) Market research phase;

(2) Acquisition planning phase;

(3) Pre-solicitation phase;

(4) Pre-award phase; and

(5) Post-award phase.

(d) The following are examples of topics that may be a part of an acquisition review:

(1) Requirement details (e.g., description of requirement, period of performance, estimated value);

(2) Market research (e.g., techniques to be used, historical data, commerciality, industry capabilities and practices, potential sources, existing contract vehicles, expected usage by other agencies);

(3) Acquisition strategy (e.g., degree of competition, small business consideration, contract type, category management, proposed evaluation factors);

(4) Business and procurement risks (e.g., project scope, funding, life cycle, compliance, alignment to agency mission, political interest, other external factors or circumstances);

(5) Important policies, procedures, and processes (e.g., IT requirements, customer agency requirements, class deviations, consolidation and bundling analyses, category management requirements);

(6) Pre-award milestones (e.g., existing contract expiration date, planned solicitation date, anticipated date of award);

(7) Debriefings, brief explanations, and other post-award communications;

(8) Contract administration requirements and key activities (e.g., post-award orientation, contractor performance, government property, option renewal or award term review, disposal requirements); and

(9) Post-award milestones, deliverables, and other important information.

504.7103 Head of the contracting activity responsibilities.

The head of the contracting activity consistent with their delegated authority shall establish acquisition policies, procedures and guidance concerning acquisition reviews for their respective organization(s) in support of this subpart.

(a) These acquisition policies, procedures and guidance shall include, but be not limited to:

(1) Commensurate with the risk, complexity, and criticality of the acquisition or contract action–

(i) Pre-award acquisition reviews (e.g., contract review board, peer reviews); and

(ii) Post-award acquisition reviews.

(2) A process for capturing best practices and innovative approaches to share with the acquisition workforce.

504.7104 Acquisitions and contract actions requiring SPE review and approval.

Acquisitions and contract actions requiring SPE review or approval must conduct an acquisition review, consistent with HCA policy established under 504.7103.

(a) *General*. The FAR, GSAM, Acquisition Letters, and other policies and procedures identify acquisitions and contracting actions that require SPE review or approval. The SPE may request review of any acquisition or contract action, in addition to those where SPE review or approval is required.

(1)An HCA may notify the SPE according to paragraph (b) of this section of acquisitions or contract actions that otherwise do not require SPE review or approval. A reason may be to seek assistance, advice, or guidance from the SPE about a potential or planned acquisition, a contract action, or an award.

(b) *Notification*. The SPE shall be notified of acquisitions and contract actions requiring SPE review or approval as early in the acquisition life cycle as possible. Notification shall be sent to spe.request@gsa.gov and include the following information:

(1)Description of the need for SPE involvement (*e.g.,* SPE approval of a consolidation determination);

(2)Description of the requirement, including key dates (*e.g.*, anticipated solicitation date, anticipated award date);

(3)Date(s) of acquisition review(s); and

(4)Any other important information.

(c) *Approval*. Acquisitions and contract actions requiring SPE review or approval shall be sent to spe.request@gsa.gov and include the following information;

(1)Description of the requirement, action required, and due date;

(2)The document(s) requiring SPE review or approval;

(3)Evidence of Service-level concurrences;

(4)Evidence of legal concurrence;

(5)Evidence of other applicable concurrences where applicable (*e.g.*, category manager and OSDBU);

(6)Supporting attachments, if applicable; and

(7)Any other important information.

(d) *Participants*. Acquisition reviews involving the SPE are to include key members of the acquisition team as well as the following participants:

(1)SPE or authorized designee;

(2)Head of the contracting activity or authorized designee;

(3)Office of Small and Disadvantaged Business Utilization; and

(4)Other key stakeholders (*e.g.*, Office of GSA IT for GSA-funded technology acquisitions).