

**SUMMARY OF MAJOR CHANGES TO
DOD 7000.14-R, VOLUME 10, CHAPTER 23
ELECTRONIC TRANSMISSION OF CONTRACT AND VENDOR PAY
INFORMATION**

**This is a new Department of Defense Financial Management Regulation
("DoDFMR") chapter.**

SEC/PARA	EXPLANATION OF CHANGE/REVISION	PURPOSE
	This chapter replaces Volume 10, Chapter 17, the contents of which were outdated.	

TABLE OF CONTENTS

★ELECTRONIC TRANSMISSION OF CONTRACT AND VENDOR PAY INFORMATION

- ★2301 General
- ★2302 Policy
- ★2303 Procedures

★CHAPTER 23★

**ELECTRONIC TRANSMISSION OF CONTRACT AND VENDOR PAY
INFORMATION**2301 GENERAL

230101. Purpose. This chapter prescribes the policy, standards, and procedures to be followed when using Electronic Business/Electronic Commerce (EB/EC) to process vendor and contract pay transactions. It describes how the Department of Defense (DoD) is using EB/EC to accurately and rapidly process the financing and delivery payments described in this volume, while maintaining proper internal control.

Terms related to EB/EC are defined in Annex 1 of this chapter. Annex 2 provides a broad overview of the electronic transaction sets, and systems that are integral to the DoD electronic data transmission and payment processes. Procedures related to electronic funds transfer (EFT) are in Annex 3 of this chapter.

A. Within the DoD, EB/EC is used to facilitate the exchange of acquisition transaction information with the private sector. The benefits include reduced costs, reduced paper received, processed, and stored, and increased efficiency by speeding up the flow of documents in the order, delivery, billing, and closeout processes. The use of EB/EC virtually eliminates the problem of lost transactions and permits electronic verification of receipt and acceptance and determination to entitlement. Contractors and vendors receive payments faster through electronic submission and processing of payment requests and disbursements by EFT.

B. To ensure secure data transmission and integrity, the DoD is utilizing public key infrastructure certificates (see Annex 1) as a critical element of the Information Assurance Defense-in-Depth technical strategy, which involves layers of defensive functionality to achieve security objectives.

230102 The policy and standards on manually processing transactions are in [Chapter 1](#) of this volume. This includes supporting documentation sent as imaged paper documents (i.e. fax, e-mail, EDM). Manual transactions require the payment technician to ensure that the document contains all the required data elements and that the imaged document is proper for payment support. This method also requires the technician to enter the data into the entitlement system and therefore must comply with the requirements for paper documents. If an electronically submitted data system is in place, to preclude the potential of duplicate payments, the entitlement office should not accept paper documentation.

230103. The policy and procedures related to purchase card payments are in [Chapter 10](#) of this volume.

230104. The policy and procedures related to miscellaneous payments are in [Chapter 12](#) of this volume.

230105. The policy and standards related to Central Contractor Registration (CCR) are in [Chapter 1](#) of this volume.

230106. Documents Outlining the Basic Requirements for the use of EB/EC.

A. The DoD EB/EC Strategic plan, published in May 1999, outlines the direction the department is taking to obtain a seamless flow of electronic business-to-business transactions and increased efficiencies. (See <http://www.defenselink.mil/nii/org/cio/doc/EBECStratPlan.doc>)

B. DoD Directive 8190.2 established the Defense Electronic Business Program office and assigned EB/EC responsibilities to the DoD Components. Under the Directive, each DoD Component shall ensure the insertion of EB/EC capabilities into the development, modernization, expansion, or prototype of systems that interface with DoD business partners or other functional areas. (See https://lad.dtic.mil/whs/directives/corres/pdf/d81902_062300/d81902p.pdf)

2302 POLICY

_____230201. Use of Electronic Transmission.

A. Pursuant to Title 10 United States Code (U.S.C.) Section 2227, (“Electronic Submission and Processing of Claims for Contract Payments”), any claim for payment after October 1, 2002 shall be submitted to the DoD in electronic form. Any DoD transmission of a claim for payment and additional documentation necessary to support the determination to entitlement and payment also must be accomplished electronically if the claim and/or documentation is submitted to another DoD employee. If the Secretary of Defense determines that the requirement for using electronic means for submitting claims is unduly burdensome in any category of cases, the Secretary may exempt the cases in that category from the application of the requirement. Policy and procedures for submitting and processing payment requests in electronic form are in Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 232.70.

B. Pursuant to the Government Paperwork Elimination Act, Public Law 105-277, the DoD Components shall allow individuals or entities the option to submit information or transact business with the Department electronically, when practicable, by October 13, 2003. The requirement includes the execution of contracts and associated records using electronic signatures of the offeror or contractor and the agency.

230202. Standards for Conducting EB/EC. The DoD and DoD Components shall:

A. Implement EB/EC technologies, standards, and edits across all systems to enhance data integrity. The finance and accounting systems with EB/EC technologies being deployed throughout the DoD shall meet all applicable Joint Financial Management Improvement Program core financial system requirements prior to implementation. (See <http://www.jfmip.gov/jfmip/>).

B. Develop systems using the Joint Technical Architecture (JTA) that mandates the minimum set of information technology standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information. The Combat Support Domain of the JTA has been developed to integrate support elements with a common technical architecture for information exchange. (See <http://www-jta.itsi.disa.mil/>).

C. Develop Information Assurance (IA) policies and implementation guidance in accordance with DoD Chief Information Officer Guidance and Policy Memorandum No. 6-8510, "Department of Defense Global Information Grid Information Assurance" (See <http://www.c3i.osd.mil/org/cio/doc/gigia061600.pdf>).

1. Exchange of unclassified information between the Department and its vendors and contractors requiring IA services using public key techniques will be accomplished through the DoD Interim External Certificate Authorities (IECAs) or GSA Business Access Certificate for Electronic Services (ACES). (See <http://www.c3i.osd.mil/org/sio/ia/pki.html>)

2. Issue DoD PKI certificates (see Annex 1) to all active duty military personnel, members of the Selected Reserve, DoD civilian employees, and eligible contractor personnel, who have access to a DoD Automated Information System (AIS). PKI certificates may be issued to other personnel categories (retirees, dependents, eligible non-U.S. personnel, etc.) as necessary when access to a PKI-enabled DoD AIS is required.

D. Use only Federal Information Processing Standards (FIPS) 161-2 EDI standards and Federal EDI Standards Management Coordination Committee (FESMCC)/DoD EDI Standards Management Committee (EDISMC) approved implementation conventions (ICs) for electronic business transaction exchanges in new and planned logistics business processes. Internal communications among DoD systems shall use FIPS 161-2 and FESMCC/EDISMC approved ICs. External communications between DoD systems and the private sector, other Federal Agencies, or foreign governments will use FIPS 161-2 and FESMCC/EDISMC approved ICs appropriate for the agencies, industries, or governments involved.

E. Use American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12 data exchange standards. This will allow trading partners to only support a single set of EDI standards and take advantage of commercial-off-the-shelf ANSI X12-compliant translation software and the services of Value-Added Networks (VANs) and Value-Added Services (VASs) (see Annex 1). The key transaction sets required for the applications described are in Annex 2 of this chapter. The DoD Components shall:

1. Adopt commercial implementation conventions (ICs) when it is in the best interest of the DoD.

2. Use industry specific implementations of ANSI X12 standards.

For example the:

- a. Uniform Communication Standard shall apply to groceries.
- b. Warehouse Information Network Standards shall apply to warehousing.
- c. Transportation Data Coordinating Committee Standard shall apply to transportation.
- d. Voluntary Interindustry Communication Standard shall apply to retail.

F. Ensure that legal issues regarding the use of electronic records are resolved when considering new or modified EDI processes.

G. Accept Electronic Signature. Federal Acquisition Regulation (FAR) 2.101 defines “signature” or “signed” as the discrete, verifiable symbol of an individual which, when affixed to a writing with the knowledge and consent of the individual, indicates a present intention to authenticate the writing. This includes electronic symbols.

H. Authentication Techniques in Federal Financial Transactions. The Financial Management Service (FMS), Department of the Treasury, maintains the federal policy outlining the principles and guidelines for the use of electronic authentication techniques for federal payment, collection and collateral transactions. The most current version of the policy may be found on the FMS website at: <http://www.fms.treas.gov/eauth/>. (NOTE: Given the rapidly changing nature of electronic commerce/electronic business, electronic authentication techniques and the related technology infrastructure, the FMS views this policy guidance as a dynamic document which may be revised as necessary, and will accept comments at any time. Changes to this policy will be published as Notices in the Federal Register, as necessary, and posted to the FMS website.)

230203. Records Retention. The EB/EC transactions that are considered to be official records, legally binding, and evidence of government business per the statutory definition of an official record shall be managed pursuant to [Volume 1, Chapter 9](#), of this Regulation.

230204. Management Accountability and Control (Internal Controls).

A. Control Environment and Internal Controls

The transmission of financial information requires strong management controls. The quality of electronically transmitted financial information is to a large extent based on the effectiveness of the control environment and internal controls in place. The control environment (organizational structure, business processes, and management) and internal controls (the systems and procedures used for processing transactions) shall be identified, documented, instituted, and tested for all electronically transmitted information. The payment and disbursing offices shall ensure that local procedures are implemented to ensure that internal controls are in place to preclude improper preparation, certification, and payment of monies, as well as ensure the proper handling of debt collection from contractors or other business entities. Civilian and

military managers who are responsible for internal controls shall be identified at each activity. Once electronic transmissions are established with vendors or individuals, use of paper documentation is no longer appropriate. Civilian and military managers shall:

1. Segregate Duties. Segregation of duties helps ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby have the opportunity to conduct unauthorized actions without detection. Define and document the responsibilities of each individual within the processing chain to ensure the integrity of the system.

2. Information Security. When information is transmitted outside an activity, a memorandum of understanding shall be signed by applicable authorities and include security controls.

3. File Backups. Local procedures shall require that file backups of electronically transmitted financial information are made and properly stored to prevent loss of information, and that an emergency operations plan is in place.

4. Periodic Review. Conduct periodic internal control reviews to test the system and determine that:

a. System access is appropriately limited to current employees based on a demonstrated need.

b. Transactions are properly recorded.

c. Transactions are properly executed.

d. Accounts are reconciled at periodic intervals and adjustments are properly documented.

5. Paper Documentation. Once electronic transmissions are established with vendors or individuals, use of paper documentation is no longer appropriate.

6. Create Local Controls. Individual activities shall develop controls for any unique situations.

B. System Controls. Electronic transmission of financial information requires strong system controls. The DoD finance and accounting systems, systems using EDI, and system interfaces shall be documented, tested, and certified that they provide reasonable assurance that electronically transmitted information is complete, correct, authorized, and secure. In addition, the DoD Components shall validate that each system is capable of ensuring the confidentiality, non-repudiation, and authentication commensurate with the risk and magnitude of the harm from loss, misuse, or unauthorized access to or modification of the information.

1. System controls shall be reviewed and re-tested regularly to ensure that the systems:

a. Incorporate access controls that limit access to the AIS based on one's need to know or detect inappropriate access to computer data, programs, and equipment to protect against unauthorized modification, disclosure, loss, or impairment. Access controls shall also limit access to outputs such as sensitive reports and disbursements.

b. Incorporate internal control and data security measures (e.g., multiple levels of system access, transaction authorization, and approval authority) throughout the system and application software architectures.

c. Incorporate software controls that limit and monitor access to the programs and files associated with the systems.

d. Ensure consistency and compatibility of interfaces among the various accounting, entitlement, disbursing, personnel, supply, travel, finance, transportation, and contract administration systems.

e. Identify and report data errors.

f. Provide the capability to identify and suspend suspected duplicate transactions until proper research is completed and any necessary corrections are made.

g. Provide a full audit trail to maintain accountability and control.

h. Facilitate single source data entry.

i. Post budgetary and proprietary accounts simultaneously.

j. Validate funds availability prior to scheduling payment and communicate the need for additional funds.

k. Permit prepayment examinations from diverse locations and include standard edits for shared data.

l. Provide transaction details to support account balances.

m. Provide periodic review of user access privileges.

n. Ensure service continuity of critical operations without interruption and the protection of critical and sensitive data.

o. Identify and report suspected processing errors and exception conditions.

p. Identify and report overrides and noncompliance with control procedures.

q. Determine that the payment data has not been altered since being transmitted from its point of origin, and after transmission to the Federal Reserve Bank, following message authentication specifications in the American National Standard Financial Institution (ANSI) X9.9 Message Authentication.

2. Civilian and military managers shall conduct periodic system tests and review testing by others for compliance with the original design documentation and later changes. System reviews shall comply with policies set forth in the Federal Manager's Financial Integrity Act and The Office of Management and Budget Circulars No. A-123, "Management Accountability and Control," A-127, "Financial Management Systems," and A-130, "Management of Federal Information Resources". The tests shall confirm that key systems accurately process transactions, are reliable, and that system documentation is properly maintained and updated. Testing methods should include management control reviews, system manager/user reviews, or ad hoc studies. Testing by others may take the form of consolidated system evaluations, inspections, audits, or management studies. System managers shall ensure that changes or enhancements made have not negated or downgraded the system's overall level of internal control.

2303 PROCEDURES

230301. General. The use of EB/EC does not alter the documentation required to support vendor and contract pay transactions or the need to properly determine entitlement to requested financing or delivery payments. Invoices and information from contracts, purchase orders, and receiving/acceptance reports must support payments. Original documentation, however, may be captured, stored, and made available for review, matching, and payment processing in electronic form. The following paragraphs describe the electronic transmission of contract and vendor pay related information within the DoD.

A. Procurement. The DoD Components currently use several contract writing systems with electronic capabilities. The Standard Procurement System (SPS) is the standard automated contract writing/contract administration system for DoD procurement. The SPS is a standard automated processing system, that is data based and data managed, and includes EB/EC capabilities. SPS provides a seamless flow of contracting data to and from the finance, logistics, and payment systems. The Defense Finance and Accounting Service (DFAS) uses SPS electronic contract, contract administration, and delivery information as the basis for making financing payments and payments for goods and services received.

B. Acceptance and Receipt. Acknowledgement that supplies or services conform to applicable quality and quantity requirements may be documented electronically through the use of an electronic signature. The DFAS uses electronic acceptance and receipt data to match the contract and any modifications and the invoice as the basis for making payments for goods or services. An electronic receiving report shall be treated the same as a hard copy receiving report and shall contain data elements specified for a proper receiving report.

C. Invoicing. The repetitive nature of processing most transactions and the uniform examination procedures applied to invoice processing usually permit extensive automation. The DoD processes large volumes of transactions in highly automated systems with automated controls, electronic data interchange, the World Wide Web, and computer assisted examination techniques. The Web Invoicing System (WinS) and Wide Area Work Flow-Receipt and Acceptance (WAWF-RA) are two of these web-based systems that allow vendors to submit invoices electronically at little or no cost to the vendor or government users (see Annex 2 of this chapter for additional details). WinS functionality will be migrated into WAWF-RA. Until complete migration occurs, use of WinS or WAWF-RA for invoicing needs depends upon the type of contract issued to the vendor. The implementation of technology does not change the need to maintain audit trails of authorizations, transactions processing, and adjustments. When an approved EDI system or other method of electronic transmission is implemented, the payment office is authorized to make use of the following electronically transmitted data when processing contractor payments.

1. Electronic Invoice. An electronically transmitted invoice shall be treated the same as a hard copy invoice and shall contain the data elements specified for a proper, hard copy invoice (see [Chapter 1](#) of this volume for the minimum data elements that are required, [Chapter 7](#) of this volume for Prompt Payment policy and standards, and [Volume 1, Chapter 9](#), of this Regulation for DoD Records Management). For audit purposes, the payment office shall retain a copy of the electronically transmitted invoice. The DFAS shall maintain a duplicate copy of each electronic invoice for the full FAR administrative post-contract retention time period in accordance with General Records Schedule 3 (Procurement, Supply, and Grant Records) and General Records Schedule 6 (Accountable Officers' Accounts Records). Copies of the General Records Schedule may be obtained from the National Archives and Records Administration, Washington, DC 20408. (See <http://www.archives.gov/>.)

a. The following additional information must be contained on all electronically transmitted invoices from the receiving/acceptance office, which is the office that accepts the contractual goods or services, to the payment office:

- (1) Date the goods or services were accepted.
- (2) Date the goods or services were received.
- (3) Date the Contractor's invoice was received.
- (4) Date the Contractor's invoice was sent to the designated payment office.
- (5) Contract Line Item Number (CLIN) (if applicable).
- (6) Contract Sub-Line Item Number (SLIN) (if applicable).
- (7) Shipment number (if applicable).

(8) Destination of shipment (if applicable).

(9) Name of acceptance activity.

b. The bill paying activity will ensure an electronic equivalent of every invoice transmitted is available for hard copy print out.

c. Electronically transmitted invoices that need to be returned to the vendor also may be returned electronically. The transmitted invoice must be accompanied by an electronic message reporting the reason for return.

2. Direct Billing. The DoD allows for the direct electronic submission of vouchers (requests for payment on cost-type contracts) directly to the DFAS. The DFAS uses WinS to process and route direct bill invoices to the appropriate payment system. WAWF-RA will support direct billing once the migration of WinS into WAWF-RA is complete. Direct billing results in faster payment, improved contractor cash flow, and eligibility to submit interim vouchers via EDI and/or Web invoicing. Contractors will continue to submit the final voucher on each cost-type contract to the DCAA to assist in the closing of contracts. See [Volume 10, Chapter 1](#) of this Regulation for more details on direct billing.

D. Payment. The date of an EFT payment is considered the invoice payment date and payment should be made so as to be received by the due date.

1. Electronic Payment Certification. The certifying officer shall verify the validity of expected payments to the payment office through the use of an electronic signature.

a. Documentation, whether electronic or hard copy, required to support payments shall be based on evidence of a valid contract, obligation document, receipt and acceptance, and the invoice when required.

b. When electronic payment certification is used, it generally is not necessary to physically transfer the hard copy documentation to the payment office for examination. However, in certain situations, the contractor may be asked to provide hard copy documentation.

c. The payment office shall maintain a certified electronic invoice file to permit post payment audit and review. Receiving and acceptance activities shall maintain corresponding electronic files.

d. Disbursing officers shall periodically test the suitability of internal controls and insure that such internal controls remain in place and are operating as designed.

e. Proposed disbursements shall be finalized and released for payment by electronic signature capability only after it is determined that:

(1) A valid contract has been established and an obligation recorded in the accounting systems.

(2) Goods or services have been received.

(3) Invoices have been received and matched to the obligating documents and receiving reports.

2. Electronic Signature for Payment. The electronic signature shall indicate the certifying official's approval and include his/her name, and title. It may be used in instances where an authorized signature must be present on a hardcopy document. Electronic signature is the recommended method of approving vouchers processed through an automated system.

a. If final certification of vouchers is accomplished electronically, the electronic signal or symbol adopted as the certifying officer's electronic signature must be:

(1) Unique to the certifying officer.

(2) Capable of verification.

(3) Under the sole control of the certifying officer.

b. In addition, the signature should be linked to the data such that if the data were changed, the signature is invalidated.

c. Electronic certification of the final voucher also requires that control procedures be in place to ensure the authenticity of transmitted data, including the electronic signature. Such controls shall provide reasonable assurance that deliberate or inadvertent manipulation, modification, or loss of data during transmission is detected.

3. Electronic Funds Transfer (EFT). The DFARS section 204.7302 requires a vendor to be registered in the CCR database, and mandates use of EFT data provided in the registration for payment purposes. See Annex 3 of this chapter for more details.