
2.0 BUSINESS ISSUES

Businesses contemplating doing business with the Federal government under the EC program need to be aware of several items. Unlike the traditional means of establishing trading partner relationships on a bilateral, trading partner by trading partner basis, this program establishes a new means. There are implications of which you should be aware.

2.1 IMPLEMENTATION CONSIDERATIONS

The way to become a Federal trading partner is to submit an 838 profile. In doing so, you are acknowledging that you have accessed the standard Federal Trading Partner Agreement (TPA) and that you agree to be bound by the terms and conditions contained therein directly and by reference. (See Appendix E, *Streamlining Procurement through Electronic Commerce*.) As to electronic funds transfer (EFT), the Department of the Treasury has a vendor payment program called Vendor Express. Agencies are required to use this program. Private sector business should assure themselves that their financial institutions are capable of handling both EFT and remittance advices.

2.2 TIMING OF TRANSACTIONS

The Federal EC architecture calls for the date-time stamping of transaction sets from the private sector as they are received by the government's network entry point(s) (NEPs). On transaction sets received from the government, date-time stamping occurs at the site of origination and again at the NEP.

2.3 MODES OF OPERATION

The initial mode of operation is store-and-forward. As networking interoperability on a national level matures (expected in the latter half of this decade), other modes of operation will be considered.

2.4 SECURITY

Agencies are responsible for adherence to Federal Information Processing Standards (FIPS) and other statutes relating to computer security and privacy. The private sector may be interested in reviewing the documents that are identified in the following guidance to agencies:

- Obtain, study, implement, and enforce the NIST FIPS (112) on passwords. Make the practice of safe computing a condition of continued employment and let your staff know it.
- Conduct a risk assessment as described in Appendix M of *Streamlining Procurement Through Electronic Commerce*.

- Apply the recommendations from NIST Special Publication 800-9, *Good Security Practices for Electronic Commerce, Including Electronic Data Interchange* as appropriate.