3-1. System Requirements

All bank and Government systems used in support of GPC accounts will include the following internal controls:

1) Systems access security,

2) Systems administration integrity,

3) Data exchange security, and

4) Functional responsibility controls.

a. **Systems Access Security**. Appropriate safeguards will be in place to control access to systems. All DoD systems will utilize CAC login for user authentication. Electronic systems used to support the DoD GPC Program must limit access to various functions to only individuals with appropriate authority. DoD GPC personnel are required to use the PIEE SSO capability to log into the card-issuing bank's EAS, unless granted a waiver by DPCAP.

b. **Systems Administration Integrity**. Changes to existing interfaces, or creation of new interfaces, must be approved by DPCAP in advance of planning and implementation. DFARS 204.73 provides information on basic requirements that all DoD system contractors must meet. All DoD systems that support the GPC will be documented in accordance with the requirements of DoDI 5000.75 (for internal DoD systems) and DFARS 204.73 for contractor systems.

c. **Data Exchange Security**. Transmission of all electronic account data will be processed through secure lines of communication. DPCAP requires that any interface used to send files via file transfer must utilize GEX. DPCAP-approved interfaces that leverage an application program interface to make system-to-system calls are exempt from utilizing GEX as an intermediary. "EDI" refers to the automated process for receiving electronic transactions, obligations, invoice, receiving, and other records from a card-issuing bank via GEX to the accounting, ERP, DFAS, or other system. To ensure funding confirmation and reconciliation information integrity, original transactions/invoices will be maintained and cannot be altered. Cardholders will not be able to alter their statements of account once they approve them unless a BO returns a statement to a CH for corrections. Billing officials and Certifying Officers will not be able to alter billing statements (invoices) once they are certified.

d. **Invoice Integrity**. An electronic certification process will be used to ensure that the official (i.e., original, unaltered) electronic invoice is traceable from the card-issuing bank through the certification and entitlement processes and retained in a government record. The BO will ensure any corrections or additions to the original invoice (e.g., reallocations to different funding lines) are proper and the payment totals have not changed. Altering a voucher that is already certified invalidates the original certification. Known or suspected fraudulent transactions not initiated by the authorized CH will be reported as external fraud directly to the card-issuing bank. When external fraud is properly reported to the bank, the current card account must be closed and a new account issued. The BO and A/OPC must be notified immediately, and the CH will comply with the bank's external fraud reporting procedures.

e. **Functional Responsibility Controls**. Systems must be able to segregate role-based capabilities and limit access to these functions to individuals with appropriate authority. The systems must be able to identify who made any data/file content changes in the end-to-end GPC process. Management

oversight reports will be available to report on individual personnel roles and responsibilities.

Parent topic: CHAPTER 3 - GPC ELECTRONIC SYSTEMS