11-1. Management Oversight Controls

a. DoD Instruction 5010.40, “Managers’ Internal Control Program Procedures,” 30 May 2013, requires DoD organizations to implement a comprehensive system of internal controls providing reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. Management and program oversight is conducted to achieve the following goals:

1) Validate and promote compliance with existing purchasing and management internal controls.

2) Identify, report, and resolve systemic material program weaknesses.

3) Measure the effectiveness of purchasing and management internal controls.

b. GPC management oversight controls are tools and activities that are used to identify, report, and address fraud, waste, and abuse. The Army GPC Program fully implements guidance and direction addressed in the April 18, 2019, OUSD Memorandum, “DoD SmartPay® 3 Government-wide Commercial Purchase Card policies, Procedures and Tools – SP3 Transition Memorandum #6.”

c. **Data analytics.** Data analytics is the application of electronic tools (software and/or systems) for automated data sorting, filtering and mining techniques using self-learning algorithms to search GPC transaction data in order to identify patterns, trends, risks, opportunities and other information. Data analytics and reporting tools are available as part of the GSA SmartPay® 3 Government-wide charge card program. Agencies have the ability to monitor their account transactions to identify any unusual spending patterns or frequency of transactions. Agency data analytics, in addition to the data analytics techniques already used by the banks to monitor account transactions, provide a multi-layered approach to help identify suspected fraud, misuse and delinquency. Data analytics can also be used to identify opportunities for expanded card use and associated benefits for the Army. A/OPCs should use data analytics tools to assist them in the management and oversight of their GPC program.

d. The Army uses preventive, detective, and directive controls to monitor the GPC program.

1) Preventive controls are designed to discourage errors or irregularities from occurring (e.g., processing a transaction only after it has been properly approved by the appropriate personnel).

2) Detective controls are designed to find errors or irregularities after they have occurred (e.g., IOD data mining, approving statements, and reconciling monthly invoices).

3) Directive controls are designed to encourage a desirable event (e.g., written policies and procedures to assist in compliance and the accomplishment of the goals and objectives of the GPC program).

e. Understanding internal controls assists GPC participants in their stewardship role in achieving GPC program objectives. Internal control is a process designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. This understanding provides an additional reference tool for all GPC participants to identify and assess operating controls, financial reporting, and legal/regulatory compliance processes and to take action to strengthen controls where needed. Over time, controls may be expected to change to reflect changes in the operating environment. In order to achieve a balance between risk and controls, internal controls should address exposure to risk and be proactive, value-added, and cost-

effective.

f. Identifying Fraudulent, Improper and Abusive Purchases. Designing and conducting procedures specifically for the purpose of detecting such transactions (e.g., IOD data mining) serves multiple purposes, including the potential discovery of a previously unrecognized risk in the program. Repeated non-adherence to established internal control policies and procedures, such as inadequate documentation of purchase card transactions or supervisory reviews, if allowed to continue, would contribute to erosion and weakening of the GPC internal control system. Prompt administrative and disciplinary actions can be effective in reducing persistent lack of adherence to policies and procedures by CHs and other program officials.

g. The SCO and A/OPCs are responsible for adhering to the requirements specified in OMB Circular A-123, Management's Responsibility for Internal Control. This circular provides guidance on improving the accountability and effectiveness of GPC programs and operations by establishing, assessing, correcting, and reporting on internal control, as well as prescribing policies and procedures to agencies regarding how to maintain internal controls that reduce the risk of fraud, waste, and error in GPC programs.

h. The SCO and A/OPCs are also responsible for adhering to the requirements specified in 10 USC 4754 (as modified by Public Law 112–194, Government Charge Card Abuse Prevention Act of 2012). These statutory requirements mandate the following actions (list not comprehensive):

1) Using effective systems, techniques, and technologies to prevent or identify improper purchases.

2) Invalidating GPCs from each employee who ceases to be employed by the Government or separates from Military Service.

3) Taking steps to recover the cost of any illegal, improper, or erroneous purchases made with a purchase card or convenience check made by an employee or member of the armed forces, including, as necessary, through salary offsets.

4) Taking appropriate adverse personnel actions or imposing other punishments when employees of the Army violate regulations governing the use and control of purchase cards and convenience checks or who are negligent or engage in misuse, abuse, or fraud with respect to a purchase card, including removal in appropriate cases. Violations of such regulations by a person subject to 10 USC Chapter 47, the Uniform Code of Military Justice (UCMJ), is punishable as a violation of section 892 of article 92 of the UCMJ.

5) Requiring the Army Audit Agency to conduct periodic audits or reviews of GPC programs to identify and analyze risks of illegal, improper, or erroneous purchases and payments and report the result to the Director of the OMB and Congress.

i. A/OPCs must provide monitoring, oversight, training, and administration of all BOs and CHs. Supervisors and BOs are responsible for the monitoring and oversight of BOs and CHs under their purview.

j. To minimize losses to the Army, the program must have an expectation of high integrity and ethical behavior from all participants, and sufficient staff to perform the following functions:

1) Conduct periodic risk assessments to identify fraud, waste, and abuse and establish specific controls to reasonably ensure that losses from these risks are minimized, to include data mining.

2) Conduct proper training and complete reporting and data analysis to ensure personnel have the

skills and information needed to be effective in their positions.

3) Conduct detailed, effective management and oversight.

4) Implement corrective actions when cardholder management is non-compliant with Army policies and procedures.

k. Monitoring and oversight of the GPC is a shared responsibility. All stakeholders in the program, including Resource and Financial Managers, logistics, contracting, and local audit and oversight organizations, are responsible for ensuring that the GPC is used in the proper manner and only authorized and necessary official purchases are made. Organizations should develop and follow a monitoring and oversight plan that establishes frequencies, methods, participation, etc., on how their monitoring/oversight programs will operate.

l. DPC issued several SP3 Transition Memorandums on GPC monitoring and oversight. DPC will rely on the signed Semi-Annual HA data provided by CPMs to accomplish DoD GPC reporting required by OMB. DPC updates visual trending of statistical and violation information to identify trends in GPC use and variances and shares this information with the Army during the GPC CPM Monthly Calls.

m. The GPC Integrated Solutions Team (IST) is DoD’s GPC governance body. IST membership consists of a GPC Governance Board composed of representatives from DPC, Army, Navy, Air Force, other Defense agencies, and supported by the bank team. The bank team consists of U.S. Bank (card-issuing bank), MasterCard (card association), and Oversight Systems (data mining vendor). The IST typically meets semi-annually to achieve the following:

1) Review trends and changes in the GPC industry and the DoD GPC Program.

2) Identify and approve any necessary adjustments to the bank team's electronic capabilities, DoD’s GPC enterprise tools, and/or DoD GPC policies.

3) Identify and approve changes to the DM rules and system parameter settings.

4) Bring efficiencies to the Program by adjusting the business rules/parameters based on transaction risk.

5) Review trends and changes in the GPC industry and the DoD GPC Program.

6) Identify any necessary adjustments to the bank team's electronic capabilities, DoD’s GPC enterprise tools, and/or DoD GPC policies.

7) Identify and approving changes to the Data Mining rules.

8) Review relevant data mining case information and recommendations provided by the bank team (e.g., percentage of data mining cases created for review; frequency with which each rule is triggered and associated DM case disposition, and information about the findings, determinations, and corrective actions identified) and results of the Semi-Annual HA process to inform its decision making.

Parent topic: Chapter 11 - Management Controls and Program Oversight