

9-8. E-Commerce Platforms

a. An e-marketplace platform is an online platform where CHs can evaluate and order products via a portal operated by a vendor: the portal provider. The e-marketplace platforms can offer portal provider products and/or third-party vendor products. Portal providers and third-party vendors are generally responsible for fulfilling orders for their respective products.

b. GSA's Commercial Platforms program (also known as GSA's e-commerce platforms) provides a managed channel for open-market purchases through select commercial online platforms (this currently includes AmazonBusiness.com, FisherSci.com, and OverstockGovernment.com). As this program is a relatively new initiative, DPC approval is required in advance of Component participation. Components making or seeking to make purchases using all other non-DoD e-commerce platforms are required to notify the Agency Program Management Office in writing and provide implementation information as requested.

c. Third-party payment processor policy does not apply to e-commerce platforms or brick-and-mortar merchants that do not accept payment using third-party payment processors. In the e-commerce space, this includes, at a minimum, those in GSA's Commercial Platforms program, and AmazonBusiness.com (separate and distinct from AmazonBusiness.com participating in GSA's Commercial Platforms program). However, as such platforms could change their payment practices and begin allowing use of third-party payment processors, CPMs are responsible for issuing Component-level policy that:

1) Establishes and implements procedures for validating that each applicable e-commerce platform continues to disallow use of third-party payment processors. Procedures shall include a certain periodicity for re-validating following initial validation, for each applicable e-commerce platform. This re-validation shall occur at least semi-annually.

2) Ensures that following completion of each validation and re-validation, GPC oversight personnel and CHs are notified regarding whether or not the applicable e-commerce platform does not/continues not to accept payment using third party payment processors to meet this criterion for non-applicability of third-party payment policy.

3) Mandates that upon notification that an e-commerce platform has begun accepting payment using third party payment processors, CHs begin complying with DoD and Component third-party payment policy, for the applicable platform.

d. **E-Marketplace Platform Method of Payment.** The GPC is the only authorized method of payment for purchases placed on the e-marketplace platforms. CHs are not allowed to use any other forms of payment, including third-party payment processors (e.g., PayPal, Venmo, Google Wallet, WePay, etc) or payments using any form of cryptocurrency. The GPC will be the only allowable method of payment, and all GPCs must be used by an authorized CH. The e-marketplace model encourages robust competition not only at the platform level by offering millions of products across thousands of suppliers, but also at the product level, with multiple suppliers competing to sell a given product.

e. **Compliance with AbilityOne.** Mandatory sources such as AbilityOne are effectively represented and promoted in this program. Rather than simply state that e-marketplaces are required to "block and sub" the commercial item for the AbilityOne item, GSA requires platform providers to prevent the sale of a commercial item which is "essentially the same" as an item on the AbilityOne

Procurement List. In addition, GSA requires platform providers to ensure the vendors selling AbilityOne products are, in fact, authorized distributors.

f. **Data Visibility.** Identifying leakage through the commercial platforms will allow the Army the ability to identify purchases that could be going to AbilityOne distributors, small business suppliers, excluded entities, or spend outside of strategic or mandatory-use agency contracts. This data then allows the Army to take the necessary action in an effort to appropriately manage this spend. Spend data will be available to the Army through on-demand reports and dashboards, allowing the Army to see line-level spend from all e-marketplace platforms. CHs will also have real-time, account level access to their purchasing data through the e-marketplace platforms for purchase card reconciliation and spend analysis.

g. **Supply Chain Security.** To address vulnerabilities within the global supply chain, GSA is implementing several solutions to create additional visibility and reduce concerns related to supply chain security. The approach is two-fold and addresses removal of both prohibited vendors and prohibited products. GSA's approach includes the following:

- 1) Section 1634, which limits or prohibits the purchase of certain items, based on statutory requirements that apply to all Federal purchases, including purchases from Kaspersky Lab.
- 2) Curating or filtering what Federal buyers can purchase, by allowing agencies to prohibit categories of items from purchase, where necessary.
- 3) Recommending best practices for e-commerce platforms and third-party marketplaces, as described in the DHS report, *Combating Trafficking in Counterfeit and Pirated Goods*, from January 24, 2020.
- 4) Leveraging the commercial Supply Chain Risk Management practices that e-marketplace platforms already possess around counterfeit and supply chain concerns, to include data associated with country of origin and detailed product descriptions, as well as quality control practices and supplier performance.
- 5) Reviewing spend data post-purchase to identify any suspect purchases that might have slipped through the cracks and warrant further review.
- 6) Section 889 on the prohibition on procurement of certain telecommunication and video surveillance equipment applies to the commercial e-commerce program as it does to every other Federal contract.
- 7) CHs may consider a product's Country of Origin when made available on the e-marketplace platforms as a part of their buying criteria.

Parent topic: [Chapter 9 - Required Sources of Supplies and Services](#)