



May 22, 2020

Laura Stanton
Acting Assistant Commissioner for Category Management, IT Category
General Services Administration (GSA)
1800 F Street, NW
Washington, DC

Subject: E-Marketplace Response to E-Commerce Developments

Dear Laura,

In response to concerns expressed by members of the Coalition for Government Procurement, I am writing to ask about the status of the e-Marketplace procurement in light of recent developments surrounding e-commerce and how the solicitation for that initiative will be changed. You may recall that, earlier this year, the Coalition opined on this subject in connection with the President's January 31st issuance of Executive Order 13904, "Ensuring Safe and Lawful E-Commerce for United States Consumers, Businesses, Government Supply Chains, and Intellectual Property Rights Holders" (the E.O.). This E.O. sought to address the integrity of the nation's supply chain and e-commerce by establishing a framework for combating trafficking in counterfeit products, including addressing the role and responsibilities of e-commerce platforms.

Just before the release of the E.O., on January 24th, the Department of Homeland Security (DHS) issued a report to the President entitled, "[Combating Trafficking in Counterfeit and Pirated Goods](#)," (Report). That report outlined the risks and harms to consumers, producers, and the economy overall associated with the prevalence of counterfeit products on e-commerce platforms and third-party marketplaces. It also provided actions to be taken by the government, along with best practices for e-commerce platforms and third-party marketplaces, to address these risks and harms. Included among them are the following:

Immediate Actions by DHS and Recommendations for the U.S. Government

- Suspend and Debar Repeat Offenders; Act Against Non-Compliant International Posts
- Apply Civil Fines, Penalties and Injunctive Actions for Violative Imported Products
- Analyze Enforcement Resources
- Create Modernized E-Commerce Enforcement Framework
- Assess Contributory Trademark Infringement Liability for Platforms

Best Practices for E-Commerce Platforms and Third-Party Marketplaces

- Comprehensive "Terms of Service" Agreements
- Significantly Enhanced Vetting of Third-Party Sellers
- Limitations on High Risk Products
- Rapid Notice and Takedown Procedures

- Enhanced Post-Discovery Actions
- Indemnity Requirements for Foreign Sellers
- Pre-Sale Identification of Third-Party Sellers
- Establish Marketplace Seller ID
- Clearly Identifiable Country of Origin Disclosures

The DHS report noted that,

Strong government action is necessary to fundamentally realign incentive structures and thereby encourage the private sector to increase self-policing efforts and focus more innovation and expertise on this vital problem. (Report, at 5).

Further,

Government action alone is not enough to bring about the needed paradigm shift and ultimately stem the tide of counterfeit and pirated goods. All relevant private-sector stakeholders have critical roles to play and must adopt identified best practices, while redoubling efforts to police their own businesses and supply chains. (Report, at 6).

The Coalition has responded to GSA's requests for comments on what ultimately has become the e-Marketplace solicitation. Coalition member concerns included the inappropriate access to, and use of, platform supplier transactional and other proprietary data and the risk giving inordinate market power of platform providers by placing them in the position of gate keepers to the federal marketplace. Further, the Coalition expressed concerns that the absence of a requirement for platform providers to identify accurately the country of origin of products offered for sale on their platforms, coupled with the failure to hold platform providers accountable for compliance with the Trade Agreements Act (TAA), risked subjecting the government market and government systems to products of unknown integrity.

These concerns represent only a subset of a number of concerns. Our recent [blog](#) identified a series of issues associated with the government's establishment and use of a duplicative acquisition platform for commercial products. For instance, multiple [studies](#) have [demonstrated](#) that, product-for-product, GSA's existing online Schedules prices are lower than the commercial e-commerce platform prices being sought via the program. In addition, with purchases limited to those below the Micro Purchase Threshold, the e-Marketplace program, by design, is grounded in the avoidance of law, which, in addition to the aforementioned risk, does not provide a solid platform for the facilitation of government policy.

As you can see, the DHS report only heightens our previously expressed concerns. Focusing on the best practices identified in the Report, it is clear that there are several contradictions between the e-Marketplace acquisition and DHS recommendations. Specifically:

- Comprehensive "Terms of Service" agreements derived to address the concerns identified herein are not required.
- The solicitation does not provide for significantly enhanced vetting of third-party sellers beyond certain existing, specified government requirements, such as AbilityOne, Section 889, and a ban on Kaspersky.
- Regarding limitations on high risk products, although specialty marketplaces for healthcare or IT products are prohibited due to what GSA describes in the SOW as "heightened supply chain

concerns,” the e-marketplaces may provide IT and healthcare products despite real risks to cybersecurity and patient safety.

- Regarding rapid notice and takedown procedures, GSA only identified as an objective (not a requirement) the ability to remove from the platform those vendors who are suspended or debarred, as well as products that are essentially the same as AbilityOne.
- Enhanced post-discovery actions are not a requirement.
- Indemnity requirements for foreign sellers are not a requirement.
- Regarding pre-sale identification of third-party sellers, GSA only requires this information to be provided to the government as a monthly transactional data extract after the purchase.
- Establishment of marketplace seller ID is not a requirement.
- Regarding clearly identifiable country of origin disclosures, the government requires such disclosures if available from the vendor and normally provided to buyers in alignment with the e-marketplace’s commercial practices.

In light of the foregoing, we ask whether and how the e-Marketplace solicitation will be amended to include specific requirements that address each of the best practices identified in the Report. While the latest version of the solicitation asks that e-Marketplace platform providers describe their commercial practices in many of these areas, we do not find that this approach is sufficient to protect Federal buyers from purchasing counterfeit and gray market products. As shown above, to a great extent, these best practices have not been addressed in the current solicitation, and thus, in the interest of maintaining the integrity of the contracting process, the Coalition believes that the changes should be released for public comment, and the solicitation timeframe amended accordingly.

We recognize that the concerns expressed herein come at a very difficult time. As our nation responds to the pandemic, we are coming to [see the serious impact of counterfeit products on our frontline workers](#), as well as the danger of relaxing critical government requirements. It is for this reason that the Coalition has supported making platform providers ultimately accountable for TAA and other compliance associated with the products on their platforms.

The Coalition appreciates your expeditious review and response to the issues we have raised and commend you and your team for all the work GSA is doing to support the Federal response to COVID-19. If you have any questions, I may be reached at (202) 751-2035 or tsisti@thecgp.org.

Sincerely,



Thomas R. Sisti
Executive Vice President & General Counsel