September 11, 2015

Daniel Kim
General Services Administration
1800 F St NW
Washington, DC 20405

Re: Request for Information (RFI) - GSA Proposal to Add a CyberIA Special Item Number (SIN) on IT Schedule 70

Mr. Kim:

The Coalition for Government Procurement ("the Coalition") appreciates the opportunity to provide comments on the proposed change to add a Cybersecurity/Information Assurance (CyberIA) Special Item Number (SIN) on IT Schedule 70.

The Coalition is a non-profit association of firms selling commercial services and products to the Federal Government. Our members collectively account for a significant percentage of the sales generated through General Services Administration (GSA) contracts including the Multiple Award Schedules program. Coalition members are also responsible for many of the commercial item solutions purchased annually by the Federal Government. Members include small, medium and large business concerns. The Coalition is proud to have worked with Government officials for more than 35 years towards the mutual goal of common sense acquisition.

As stated in the RFI, GSA's overall objective in adding a CyberIA SIN is to improve the way that GSA offers CyberIA products and services through IT Schedule 70, increase visibility, improve access to CyberIA offerings, and to provide industry partners the opportunity to differentiate their CyberIA products and services from other IT related products and services.

The RFI specifically refers to the Cyber Security Act of 2012 which suggests that "The administrator of GSA is to develop a Multiple Award Schedule special item number under Schedule 70 for information security products and services and consolidate those products and services under that special item number to promote acquisition." However given that the Cyber Security Act of 2012 was not passed into law, there is no statutory requirement that GSA create a unique SIN under Schedule 70 specifically for CyberIA products and services. In fact, Congress considered this proposal and it was rejected. Therefore, rather than adding a CyberIA SIN we recommend that GSA pursue more efficient and cost effective alternatives to improving ease of access to CyberIA products and services for customer agencies.

Unnecessary Inefficiencies & Added Costs

While the Coalition supports GSA's efforts to explore new ways to enhance its acquisition offerings for customer agencies, the addition of a CyberIA SIN would complicate and duplicate current IT offerings under Schedule70, add costs to both government and industry, and fragment Schedule 70 as a total solution. IT products and services that would be added to the new CyberIA SIN are already available under the current structure of Schedule 70. Some of the sub-categories under the proposed SIN overlap with existing services provided on Schedule 70 or potentially overlap with the recently created Cloud Computing SIN (e.g., Secure Web Hosting).

It would be highly inefficient for both GSA and Schedule 70 vendors to have to add the same products and services that are already available under the IT Schedule to a cyber-specific SIN. The associated administrative costs are not insignificant. Investments that contractors will have to make include changes to accounting systems, additional reporting and new training. From a contract administrative perspective, there are also additional complications involving the Industrial Funding Fee (IFF) and compliance with the Price Reductions Clause. Given that cybersecurity is entrenched through various different solutions, industry would have the additional financial and administrative burden of determining where to categorize sales for IFF reporting. Additionally, separate Basis of Award customers may need to be identified, tracked, and reported. This would leave industry with more internal expenses and no clear value from increased sales on a new SIN. These added costs to the taxpayer would not provide additional value to GSA's customers because the services and products can already be obtained using the existing IT Schedule.

The existing SIN structure facilitates the ability to acquire total solutions. In the services arena, members note that there are not many "pure" CyberIA services contracts in existence. CyberIA requirements are often intertwined in the larger overall general IT requirement. Today, those efforts are scoped and priced with labor services that may include this capability amongst the entire team. In this regard, it is unclear how a new Cyber SIN would be beneficial. For example, recent government agency efforts can be primarily built on CyberIA but include some system administration functions as well. Moreover, there are many task orders for primarily IT services, but have a small CyberIA component within the RFI that would not fall within the proposed SIN.

Like the proposed Health IT SIN, a CyberIA SIN would fragment the current IT Schedule 70 based on a specific type of customer need. Tailoring SINs to specific markets is a major change to the structure of the MAS program. There is no real limit to the potential unique markets that additional SINs could be created for within the Schedules program. For Schedule 70 alone, some more examples are Financial IT or Modeling and Simulation IT. The creation of SINs specific to unique customer needs would proliferate duplication of effort and inefficiencies throughout the program for GSA and its contractors with, again, no real advantage to customer agencies or the taxpayer.

One of the greatest benefits of the Schedules program is that it streamlines and simplifies the procurement process for its customers. We recommend that GSA continue this feature by maintaining the current structure and not tailoring SINs to specific markets.

Cybersecurity Standards

The establishment of a CyberIA SIN also involves the difficult task of determining which cybersecurity standards should apply to the scope of products/services eligible for the new SIN. For example, the Common Criteria standard that governs the purchase of IA equipment for use in classified environments already categorizes IA equipment and mandates that the equipment be certified against the standard prior to acquisition of such equipment by government agencies. However, this standard may not be applicable to Federal agencies using IA equipment in unclassified environments.

The risk of developing a CyberIA SIN and defining the scope based on a particular set of cybersecurity standards is that it may unnecessarily limit available products and services under the new SIN. Therefore, it is preferable to maintain the current system of having cyber products and services available under multiple SINs and allowing customer agencies to determine the applicable standards at the task order level per FAR 8.404(b)(1). GSA could then provide information and resources for customer agencies to identify CyberIA products/services and the associated cybersecurity standards through eTools like GSA Advantage or the IT Hallway of the Acquisition Gateway.

Alternatives to a CyberIA SIN

In order to achieve its goal of improving the way that GSA offers CyberIA products and services through IT Schedule 70, the Coalition recommends that GSA take the following steps:

1. Update its Terms & Conditions to include CyberIA for SINs 132-8, 132-12, 132-32, 132-33, 132-34, 132-51 as well as 132-35 and 132-50. The Coalition suggests that 132-50 Training Courses include CyberIA terms and conditions as well given the current demand for these types of services.

    a. The new terms and conditions should reflect those that have already been developed and put in place by the Department of Defense (DoD) and the Intelligence Community for CyberIA products and services.

    b. Further, per FAR 8.404(b)(1), any additional cyber-specific terms and conditions can be added at the task order level by customer agencies.

2. Update language in the labor category descriptions that assures customer agencies that contractors can provide CyberIA services.

3. Allow for greater flexibility for CyberIA products and services under Schedule 70 in order to meet urgent customer demand.

    a. Develop a streamlined process so that CyberIA products and services may be added to IT Schedule 70 quickly. To meet the CyberIA needs of customer agencies, there is simply not enough time to take a newly developed product to market, have sufficient sales to satisfy the Commercial Sales Practices

requirements, and conduct negotiations. Otherwise, it is often too late in the product life-cycle to meet the critical mission that the new CyberIA product or service was created to support.

b. Address potential restrictions of the Price Reductions Clause (PRC) that limit access to CyberIA technology and services that are currently being utilized in the commercial market, such as subscription-based and fixed unit pricing models.

4. Utilize GSA's already well developed eTools to consolidate CyberIA products and services for ease of customer discovery and access, to support market research and acquisition planning.

    a. Establish a service catalog for CyberIA firms, which can be maintained without adding a SIN. The list could be created within GSA's e-Library -- or as part of some future functionality within the planned common acquisition platform.

    b. Consider offering CyberIA services under SIN 132-51 in GSA Advantage with distinct subcategories.

5. Maximize value for customer agencies through Category Management by using GSA's new Common Acquisition Platform to market CyberIA products and services.

    a. Implement a targeted marketing/communication plan to help customer agencies identify cyber-specific products and services along with best practices, information about applicable cybersecurity and IA standards, and capable vendors within the new IT Hallway.

Upon review of the RFI for the CyberIA SIN proposal, it is not clear that the proposal would provide any increased value for GSA or its agency customers. The proposal will, however, increase costs and complexity for contractors and government.

Again, the Coalition appreciates the opportunity to share our comments in response to the RFI. We also welcome any opportunities to work with GSA on the suggested alternatives to enhance the availability of CyberIA products and services under IT Schedule 70.

If you have any questions concerning our comments, please contact me anytime at (202) 331-0975 or rwaldron@thecgp.org.

Sincerely,

Roger Waldron
President