June 21, 2016

Shon Lyublanovits
Supervisory IT Specialist
General Services Administration
1800 F St NW
Washington, DC 20405-0001

Subject: GSA Highly Adaptive Cybersecurity Services (HACS) SIN RFI

Dear Ms. Lyublanovits,

Thank you for the opportunity to provide comments in response to the Request for Information (RFI) regarding the Special Item Number (SIN) for Highly Adaptive Cybersecurity Services (HACS) under IT Schedule 70. The RFI reflects the direction provided by the Office of Management and Budget's (OMB's) *Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* dated October 30, 2015. One of the key management goals set forth in the memorandum directs GSA, in coordination with OMB and the Department of Homeland Security (DHS), to research and identify contract vehicle options for incident response services.

GSA's current proposal to add an HACS SIN to IT Schedule 70 rather than create a new standalone contract vehicle supports efficient, effective and continuous access to the commercial marketplace for cybersecurity services. As you know, continuous open seasons are a key feature of IT Schedule 70 providing for the submission of proposals/modifications for new technologies and services, including new cyber capabilities, every working day of the year. The Coalition for Government Procurement ("the Coalition") strongly agrees that highlighting vital cybersecurity services offerings to customers via the HACS SIN is preferable to the creation of a new contract vehicle.

Reducing Barriers to IT Schedule 70

The Coalition makes the following recommendations to further reduce contracting barriers on IT Schedule 70 to ensure access to innovative cybersecurity service providers and to increase the rapid deployment of highly adaptive cybersecurity services. In addition to the steps GSA has already taken through the *Making It Easier* initiative, these changes would further reduce barriers

to entry and risk for contractors, increase the flexibility of Schedule 70, and increase value for GSA's customer agencies.

1. *Eliminate the Price Reduction Clause (PRC)*

Coalition members consistently report that they are unable to add new services and solutions to IT Schedule 70 due to the compliance risk associated with the PRC. Dating back to the early 1980s, the PRC is an anti-competitive, outdated compliance mechanism that requires that a contractor reduce its MAS contract price, whenever it reduces its price to the commercial customer that was the basis of award[1]. The PRC reflects a time when the MAS program was a mandatory source for all federal agencies and competition at the order level was limited. It also reflects a time when robust task and delivery order competitions were not mandated by law or regulation.

The PRC increases contract administration costs for government and industry at a time when pricing is driven by competition at the task order level. The government and contractors spend tens of millions of dollars a year negotiating, overseeing, reviewing and complying with the PRC. Contractors implement compliance infrastructures, including personnel and systems, to address compliance risk associated with the PRC. These compliance costs create barriers to entry for new technologies and when they are added to the contracts later, the increased costs of PRC compliance are ultimately passed on in the form of higher prices. In turn, the government maintains a costly infrastructure to oversee and review compliance with the PRC. The Coalition conducted a survey and submitted comments to GSA regarding the costs and burdens associated with the PRC[2].

The PRC is not necessary to ensure fair and reasonable pricing for cybersecurity services. Due to changes in federal regulations within the past 20 years, providing increasingly greater competition at the task order level, the PRC is no longer needed to assure reasonable task order pricing. Schedule vendors must watch their pricing at all times to stay competitive. Task order competition for specific requirements is mandated by statute and regulation and drives lower pricing for agency customers.

Eliminating the PRC will save government and industry time and money while fostering increased access to emerging cyber technologies. With the right reforms, the MAS Program

---

[1] GSA Multiple Award Schedule Pricing: *Recommendations to Embrace Regulatory and Commercial Market Changes*, September 9, 2013, http://thecgp.org/images/MAS-Pricing-White-Paper-Attach-Included-FINAL-9.9.13.pdf

[2] Re: Information Collection 3090-0235, Price Reductions Clause, February 27, 2012, https://netforum.avectra.com/public/temp/ClientImages/CGP/b134922c-52d9-4fdb-a3cf-cff83cb83bc2.pdf & Re: Information Collection 3090-0235, Price Reductions Clause, April 16, 2012 https://netforum.avectra.com/public/temp/ClientImages/CGP/a41c0eb3-35e3-44ea-bc6b-8d35d75c5fe0.pdf

can serve as a virtual innovation portal connecting government customers to companies providing leading edge commercial technologies[3].

2. *Incorporate Other Direct Costs (ODCs)*

Today, agencies often need to acquire comprehensive cyber solutions rather than isolated products or services. To provide a solution, MAS vendors may need to rely on materials that have not been listed on an MAS Schedule to fulfill a particular agency's specific need. Incorporating ODCs into IT Schedule 70 will enhance access to commercial cyber solutions, allowing customer agencies and contractors to compete for and perform comprehensive cyber solutions.

However, under current practice for most Schedules, ODCs must be listed at the contract level to be included in an order[4]. The challenge of this approach is that a contractor often cannot know in advance what the ODCs will be required for the work. As a result, such materials have to be acquired as open market items. This constrains the flexibility and efficiency of IT Schedule 70 and limits the government's access to cutting edge cybersecurity services.

The Federal Acquisition Regulation ("FAR") already provides flexibility to accommodate a solution to this problem. This approach has been employed for multiple award IDIQ contracts that are priced on a time and materials ("T&M") or labor hour basis. Comparable flexibility may be employed for the benefit of the MAS Program. Pursuant to FAR 52.212-4 Alternate 1, GSA may authorize agencies to identify ODCs at the order level when placing orders under the MAS Program. FAR Part 12 and the corresponding commercial item clauses clearly authorize ODCs.

As the largest commercial item IT contract in government, GSA has an opportunity to move the entire market forward in providing the latest commercial solutions for highly adaptive cybersecurity services. GSA should act on this long proposed recommendation and incorporate ODCs into IT Schedule 70 as soon as possible.

3. *Return to the standard commercial item order of precedence language*

As a result of the *Class Deviation Addressing Commercial Supplier Agreement (CSA)*

[3] MAS Reform: Towards an Innovation Portal, January 28, 2014, http://thecgp.org/images/MAS-Innovation-Letter-Final-with-Attachments-No-Cover-Letter.pdf

[4] Other Direct Costs Working Group White Paper, September 30, 2011, http://thecgp.org/images/CGP-ODC-White-Paper1.pdf

Terms dated July 31, 2016, the current language in IT Schedule 70 increases risk and barriers to entry for contractors. It essentially provides that all government unique terms and conditions take precedence over commercial terms[5]. This approach is inconsistent with the *Federal Acquisition Streamlining Act of 1994 (FASA)* and its implementing regulations. FASA is implemented at Part 12 of the FAR. FAR 12.301(a) provides, in part, that "contracts for the acquisition of commercial items shall, to the maximum extent practicable, include only those clauses required by law or "[d]etermined to be consistent with customary commercial practice." The plain language of the statute and regulations mandates a preference for commercial item contract terms and conditions. Unfortunately, the deviation, itself counter to the law and regulation, creates a preference for government terms and conditions.

The IT Schedule 70 current order of precedence increases barriers to entry for commercial technologies and stifles innovation.

Given GSA's objective of attracting best in class HACS offerors to the new SIN, the Coalition recommends that GSA return to the previous order of precedence language which would significantly reduce barriers to entry and risk for commercial companies.

Flexible SIN Structure & Scope

The structure of the HACS SIN should be designed to reduce burdens for Schedule contractors and the government. The Coalition recommends that the HACS SIN be structured to provide flexibility at the task order level to meet customer agency mission requirements across the best value continuum. An inflexible SIN structure will restrict competition and limit the government's access to "best in class" commercial cybersecurity providers. To the maximum extent practicable, minimizing vendor capability, evaluation, security requirements and Terms & Conditions at the SIN level will increase competition, best value and sound performance outcomes to meet customer agency missions. In our members' experience, allowing more requirements to be determined at the task order level will provide ordering contracting officers the greatest flexibility when ordering Highly Adaptive Cybersecurity solutions under Schedule 70. Additionally, requirements at the contract level should be limited to cybersecurity capabilities that reflect a broad set of customer agency needs and innovative commercial companies.

The scope of the proposed HACS SIN should seek to minimize duplication and added costs. In order to do so, the SIN should only include "Highly Adaptive Cybersecurity Services" as

[5] RE: Request to Rescind Class Deviation Addressing Commercial Supplier Agreement Terms that Conflict or Are Incompatible with Federal Law (Acquisition Letter MV-15-03), September 30, 2015, http://thecgp.org/images/Commercial-Supplier-Agreement-Deviation-Letter-to-GSA.pdf

proposed in the RFI and not expand to services available under other Schedule 70 SINs. Additionally, the three proposed categories (Proactive, Reactive and Remediation) may not reflect how HACS are offered in the commercial market. Agencies often acquire cybersecurity services as a part of total solution, not as a standalone service. For example, a contractor may offer a bundled package of IT services to meet an agency's need to include HACS, at times providing both reactive and remediation services as a part of routine operations and maintenance of an IT system. The new SIN should be flexible enough to accommodate HACS as part of a comprehensive solution consistent with contractors' commercial practices.

Conclusion

The Coalition appreciates the opportunity to provide feedback on the development of a HACS SIN under Schedule 70. If you have any questions concerning the above recommendations or need more information, please contact me at rwaldron@thecgp.org or 202-331-0975.

Regards,

Roger Waldron
President