



August 21, 2014

Dennis Harrison
Division Director, IT Schedule 70
U.S. General Services Administration
1800 F St NW
Washington, DC 20006

Re: Proposed Change to Add a Cloud Computing Special Item Number (SIN) on IT Schedule 70

Dear Dennis,

The Coalition for Government Procurement appreciates the opportunity to provide comments on the General Services Administration's Request for Information Proposed Change to Add a Cloud Computing Special Item Number (SIN) on IT Schedule 70. We also appreciate the extension that GSA provided in response to our request.

The Coalition for Government Procurement ("the Coalition") is a non-profit association of firms selling commercial services and products to the Federal Government. Our members collectively account for approximately 70% of the sales generated through the GSA Multiple Award Schedules (MAS) program and about half of the commercial item solutions purchased annually by the Federal Government. Coalition members include small, medium and large business concerns. The Coalition is proud to have worked with Government officials over the past 35 years towards the mutual goal of common sense acquisition.

The following are the Coalition's comments regarding implementation of a new cloud services SIN under IT Schedule 70. The theme of our comments is flexibility. IT Schedule 70 contracts that incorporate the new cloud services SIN must provide flexibility in pricing and solution structure to ensure customer agencies can effectively meet their cloud service requirements.

1. There are two critical acquisition policy reforms that are imperative if the Cloud SIN is to be successful in providing customer agencies with innovative, best value solutions:

A. Waive the Price Reduction Clause (PRC) to the Cloud Services SIN:

- i. Waiving the applicability of the PRC to the Cloud Computing SIN will accelerate best value “cloud computing” solutions and increase access to commercial innovation via IT Schedule 70.
- ii. Given that commercial offerings for cloud service many times involve uniquely structured solutions that may include one or more bundled sub-categories of services identified in the RFI (IaaS, PaaS, SaaS, XaaS), it is impracticable to establish a tracking customer for purposes of PRC compliance. Fundamentally, pricing for cloud services is driven by customer needs—making an objective, apples to apples comparison of pricing under the PRC irrelevant.
- iii. The PRC essentially requires archaic, high risk price certifications that limit a contractor’s ability to offer new technologies, services and solutions. Moreover, the administrative costs and overhead associated with PRC compliance increase costs for government and industry.

B. Allow ODCs under the Cloud Services SIN:

- i. By utilizing the vetted, FAR-based commercial item clauses for acquisition and reimbursement of ODCs, materials and indirect costs, FAS can enhance customer agencies’ ability to efficiently and effectively acquire robust, sound and comprehensive cloud solutions to requirements under IT Schedule 70.

- ii. Inability of customer agencies to include ODCs, materials and indirect costs on Schedule orders effectively blocks companies from providing their latest technologies and comprehensive solutions. Moreover, the lack of ODC capability on IT Schedule hurts small schedule contractors who cannot specifically include and price all potential cloud service elements and/or products under their contracts. ODCs would allow small businesses to fill gaps in service elements/products at the task order competition level. ODCs would also provide greater opportunity for small businesses seeking subcontracts under schedule contracts.
- 2. The contract level terms and conditions should reference a core set of requirements for the cloud services SIN (e.g. NIST, FedRAMP and FISMA) in a flexible manner that allows for robust access to commercial solutions. Some key considerations include:**
- A. The NIST definitions referenced in Table 1 are guidelines and are not intended to be prescriptive. NIST 800-145 notes that cloud technology is rapidly evolving with fluid definitions.
 - B. Specific requirements (e.g. timing of FedRAMP ATO and storage location) should be determined by the acquiring agency at the task order level.
- 3. The Sub-SIN structure is confusing for both contractors and customer agencies. The Sub-SIN could have the unintended consequence of creating stovepipes that limit flexibility, innovation and total cloud solutions.**
- A. Cloud solutions commercially available today often span the proposed Sub-SINs (SaaS, PaaS, IaaS, XaaS). As an example, an IaaS provider may provides PaaS features (managed relational databases). GSA's Cloud Sub-SIN structure should reflect this overlap, especially given that the lines distinguishing current Service Models are likely to become even more blurred in the future. GSA should also include a more general

category for new and emerging cloud services as proposed by the “XaaS” option.

4. Allow for more flexibility under the Cloud Services SIN vs. other Schedule 70 SINS that offer more traditional products and services.

- A. Cloud in the commercial market is an on-demand pay-as-you-go type of service. The Cloud Services SIN should allow agency customers to change/purchase any services at any time in order to customize on the fly to meet their mission.
- B. Contracts offered under the Cloud Services SIN should not restrict the customization and flexibility of typical cloud services. The need to issue a modification every time the end user adjusts available features is contrary to the concept of the cloud which is a real time, dynamic model. Allowing cloud service contractors to use their standard commercial price lists will reduce the need to issue modifications for adds/deletes and price increases.
- C. Terms and conditions should map as closely as possible to commercial best practices. Any special terms and conditions should allow for cloud solutions that maximize competition in order to provide best value to the government. GSA should also ensure that any specific terms and conditions minimize administrative process and paperwork burdens that increase costs, result in delays and stifle innovation. It is also critical that intellectual property rights are protected.

5. Clarify GSA’s plans to screen vendors for the Cloud Computing SIN.

- A. The Coalition believes more clarity is needed on this issue. We recommend that the Cloud SIN be structured so that the maximum number of vendors can participate rather than limiting the vendor pool due to restrictive requirements and exerting pricing pressure on vendors that already provide cloud services under Schedule 70.

The Coalition appreciates the opportunity to provide input on the Proposed Change to Add a Cloud Computing Special Item Number (SIN) under IT Schedule 70. We look forward to continuing the dialogue on this important initiative. If there are any questions, please contact me at (202) 315-1051 or rwaldron@thecgp.org.

Sincerely,

A handwritten signature in black ink, appearing to read 'RWaldron', with a long horizontal flourish extending to the right.

Roger Waldron

President

RFI Template

Table 1: Administrative Information

#	Question	Response
a	Company Name	The Coalition for Government Procurement
b	File Name	Coalition_IT70-Cloud-SIN-RFI-Response_final
c	Page Count (including cover)	9

Table 2: B. Questions for Industry - Feedback on Proposed SIN Addition

#	Question	Response
1.a.	Proposed SIN Scope - Does your company have any feedback on the draft scope as stated in Table 1? Please provide a response of any concerns as well as any proposed changes to the scope.	The proposed SIN scope is a reasonable starting point in terms of describing current cloud offerings. However commercial cloud offerings often span the sub-SINs categories proposed. For example, as a company employs an SaaS solution, PaaS may be used as a way to enhance the solution that GSA is offering under the SaaS sub-SIN. The SIN scope should take into account more comprehensive approaches that vendors offer in the commercial market.
1.b.	Proposed SIN Scope - NIST Characteristics - The National Institute for Standards and Technology (NIST) has defined the essential characteristics of Cloud Computing. (NIST Special Publication 800-145). For the purposes of providing commercially available cloud services on a Cloud SIN, should all offerings meet these essential characteristics or are there any that should be specifically excluded from the list? Please provide your rationale.	The NIST definitions are guidelines and should not be prescriptive. The definitions of the essential services in NIST SP800-145 do not encompass all possible cloud services and their characteristics.
1.c.i.	Proposed SIN Scope - Sub-SINs - The current proposed Sub-SINs are IaaS, PaaS, SaaS, and XaaS (See Table 1 in the RFI). i. Do you see value in requiring industry partners to identify this service model distinction at the Sub-SIN level?	The Sub-SIN approach may inadvertently inhibit a vendor's ability to offer comprehensive cloud solutions. As mentioned earlier, comprehensive commercial cloud services often span the proposed Sub-SIN categories. Additionally, there is an assumption through the Sub-SIN structure that cloud services (IaaS, PaaS, SaaS, XaaS) provided by various vendors will function seamlessly together. Utilizing one vendor for IaaS and another vendor for SaaS could be problematic. An agency would not be assured that the software provided by the SaaS vendor

#	Question	Response
		functions correctly on an upgrade implemented by the IaaS vendor. This could leave the agency's systems inoperable as both vendors, not in violation of their contract, are not compelled to fix the problem.
1.c.ii.	<p>Proposed SIN Scope - Sub-SINs - The current proposed Sub-SINs are IaaS, PaaS, SaaS, and XaaS (See Table 1 in the RFI).</p> <p>ii. Do these four categories address the range of expected cloud services, or would you suggest any other relevant Sub-SINs? If so, explain why this would logically fall into the category of Cloud Computing and not any other existing SINs.</p>	
1.c.iii.	<p>Proposed SIN Scope - Sub-SINs - The current proposed Sub-SINs are IaaS, PaaS, SaaS, and XaaS (See Table 1 in the RFI).</p> <p>iii. Do you see value for GSA to vet that the services meet specific qualifications for each Sub-SIN category?</p>	
2.	<p>Vendor Pricing Methodology: What are your commercial pricing methodology structures for a proposed Cloud SIN? (Provide a link to a web page if possible.) A contemplated structure would include firm-fixed price units, for example - components priced by time units such as minutes, hours, months or years (such as per user per month, storage cost per unit (e.g. GB) per hour).</p>	
3.	<p>Industry SIN Management: Given that cloud services are currently offered under SINs 132-32, 132-52 and 132-51 (if not potentially others), identify any challenges you foresee with adding the</p>	To mitigate confusion, the Coalition recommends that GSA update the current SIN definitions (132-32, 132-52 and 132-51) to note that cloud solutions/services are no longer included and that these technologies will be offered under the new cloud SIN.

#	Question	Response
	proposed SIN, and identify any proposed mitigating actions.	
4.	Potential Service Offerings: Please provide a brief indication of service offerings your company would like to offer in a proposed SIN including sub SIN categories.	
5.	Terms and Conditions: As with other IT Schedule 70 SINs, a future Cloud Computing Services SIN would have special Terms and Conditions. ¹ These Terms and Conditions would address both industry partner requirements as well as information useful to Ordering Activities. Please identify any feedback on the proposed topic areas and suggest any additional terms and conditions topic areas that GSA should consider for this SIN.	As mentioned in the Coalition’s outline above, our members recommend that any special terms and conditions for cloud services allow the government and contractors the flexibility to solicit and offer cloud solutions that enhance competition in order to provide the best value to the government. These terms and conditions should include sufficient protection of the intellectual property rights of prospective contractors, the use of commercial products and services and the reduction of administrative processes and paperwork burdens that increase costs and hamper innovation.
5.a.i.	Security/Information Assurance: FedRAMP: It is contemplated that FedRAMP will be referenced in the Terms and Conditions. The scope does not currently propose that industry partners hold a FedRAMP JAB provisional ATO or an agency-granted FedRAMP compliant ATO because FedRAMP compliance is already the de facto standard and issuing an ATO is the ultimate responsibility of the ordering agency. Does your company see any value in requiring a FedRAMP-compliant ATO or any other specific FedRAMP compliance language?	The Coalition recommends that the requirement of a FedRAMP–compliant ATO be issued at the Task Order level.
5.a.ii.	FISMA: It is contemplated that	

¹ Refer to the “13 - Critical Information Specific to Schedule 70” package attachment on the IT Schedule 70 Solicitation published on FedBizOpps at the following URL:
https://www.fbo.gov/index?s=opportunity&mode=form&id=d24cd9e270944b554632f37b34866aa6&tab=core&_cview=1

#	Question	Response
	the Federal Information Security Management Act (FISMA) of 2002 will be referenced in the Terms and Conditions	
5.a.iii.	Data Requirements: It is contemplated that a set of high level data requirements may be included in the Terms and Conditions. Identify any data requirements you believe should be included as Terms and Conditions (for example, requirements related to data privacy, HIPAA, interoperability, etc.)	<p>The inclusion of any data requirements should consider the costs involved and the associated return to the taxpayer.</p> <p>For HIPAA compliance GSA may want to consider reference to the HIPAA Business Associates Agreement. The recently published ISO 27018 standard may be helpful in prohibiting the use of customer data for advertising or marketing purposes.</p>
5.a.iv.	Information Assurance: Identify any information additional assurance requirements you believe should be included in the Terms and Conditions.	
5.b.	Legislative Requirements: Identify any legislative requirements you believe should be referenced.	
5.c.	Service Model and Delivery Model: It is expected that industry partners should provide at minimum the service model (e.g. IaaS, PaaS, SaaS) and deployment model (public, private, community, hybrid, etc.) of cloud services provided.	
5.d.	NIST Characteristics: As described in question 1b, it is anticipated that in some capacity the NIST characteristics will form the basis of determining whether the service provided is truly a cloud service, and therefore reflected in the Terms and Conditions.	

#	Question	Response
5.e.	<p>Pricing: Specific pricing requirements may be included in the Terms and Conditions; for example pricing and/or billing requirements to ensure that government agencies can take advantage of the scalable and metered nature of cloud services.</p>	
5.f.	<p>Data Center Location: Location of the data centers can be a high priority concern for many government customers. It is contemplated that the data center locations will not be restricted at the SIN level, but must be identified at the Task Order level. Based on a wide variety of customer requirements it is expected that it will be the responsibility of the Ordering Activity to make a determination of acceptable data center locations and set any location-specific requirements.</p>	<p>The Coalition maintains that data center location should be identified by the ordering agency. Only a high level set of requirements for data center locations should be required by the Cloud SIN.</p>
6.	<p>General Feedback: Does your company have any other general feedback about the proposed SIN?</p>	