G A O
Accountability * Integrity * Reliability

Comptroller General
of the United States

United States Government Accountability Office
Washington, DC 20548

Decision

Matter of: Technosource Information Systems, LLC; TrueTandem, LLC

File: B-405296; B-405296.2; B-405296.3

Date: October 17, 2011

William A. Shook, Esq., Shook Doran LLP, for the protesters.
Timothy Sullivan, Esq., and Katherine S. Nucci, Esq., Thompson Coburn LLP, for Onix Networking Corporation; E. Charles Rowan, Esq., for Unisys Corporation, the intervenors.
John Cornell, Esq., General Services Administration, Information Technology Service, for the agency.
Eric M. Ransom, Esq., and Edward Goldstein, Esq., Office of the General Counsel, GAO, participated in the preparation of the decision.

DIGEST

1. Protest of agency requirement that any non-U.S.-based cloud computing data centers be located in Trade Agreements Act Designated Countries is sustained where the agency failed to establish a connection to any legitimate government need.

2. Protest of agency requirement for a "government community cloud" limited to United States federal, state, local, or tribal government entities, is denied where the record supports a potentially meaningful security benefit associated with the requirement.

3. Allegation that solicitation's internet routing requirements are ambiguous is sustained where the relevant terms are only apparent by reference to explanations and documents which were not incorporated in, or referenced by, the solicitation.

DECISION

Technosource Information Systems, LLC, of Annapolis, Maryland, and TrueTandem, LLC, of Reston, Virginia, protest the terms of request for quotations (RFQ) No. QTA011GNB0010, issued by the General Services Administration (GSA), Information Technology Service, for cloud computing services.

We sustain the protest in part and deny it in part.

BACKGROUND

GSA issued the RFQ on May 9, 2011, to establish a SmartBUY blanket purchase agreement of GSA Schedule 70 contract holders for cloud computing services including, specifically, e-mail as a service (EaaS). The RFQ contemplates five service offerings divided into five lots: (1) EaaS; (2) Office Automation; (3) Electronic Record Management; (4) Migration Services; and (5) Integration Services. RFQ at 3. Each service lot was further divided into four sub-lots corresponding to various cloud computing deployment models: Government Community Cloud; Provider Furnished Equipment Private Cloud; Secret Enclave; and Public Cloud. Id. Pricing for each sub-lot was further divided into two contract line item numbers (CLIN). The first CLIN was for "U.S. Based Prices" and required all data and data centers to be located in the United States. The second CLIN was for "Non-U.S. Based Prices," which was applicable when any data or data centers would be located "in designated countries defined by Federal Acquisition Regulation (FAR) 25.003."[1] Thus, by its terms, the RFQ did not allow for locating data or data centers in non-U.S. countries other than the designated countries defined by FAR § 25.003.[2]

The RFQ included both common technical requirements applicable to all lots and deployment models, as well as lot-specific and sub-lot-specific technical requirements. Among the common requirements, the RFQ set forth a number of data center facilities requirements. As relevant here, common requirement 17 mandated that:

> 17. The Quoter shall describe their solutions to provide effective separation of network traffic meeting the following objectives:
>
> a. All inbound and outbound data, inclusive of all mail messages, including between the Government and other co-tenants, can be routed through a dedicated network connection.

[1] FAR § 25.003 defines "designated country" to include a World Trade Organization Government Procurement Agreement country, a Free Trade Agreement country, a least developed country, or a Caribbean Basin country.

[2] Among the general requirements, the RFQ further stated that "[t]he quoter shall disclose the locations by (City, State/Country) where data centers are located. For quoters offering data centers outside of the United States, locations shall adhere to FAR § 25.003 and quoters shall provide pricing for these data centers in accordance with section B." RFQ at 35.

> b. The service must exclude co-tenant data, or any other third party data, not intended for the Government from being transmitted through a Government network connection.
>
> c. The service must exclude data intended solely within the Government from being routed through an external (non-government) network connections [sic].

RFQ at 39.

Also relevant here are the sub-lot-specific requirements related to the government community cloud deployment model. Specifically, the requirement defining the scope of the government community cloud indicated that, "[t]he Quoter shall provide a cloud specifically limited to Government clients with an appropriate Government issued domain name for a Moderate Impact System." RFQ at 49. The term "Government clients" was not defined by the RFQ.

Finally, the RFQ incorporated "all GSA ordering activity and customer governed IT security standards, policies, reporting requirements, and government-wide laws or regulation applicable to the protection of government-wide information security." RFQ at 68. These policies and regulations include, for example, the Federal Information Security Management Act (FISMA) of 2002; Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Quoters;" and Office of Management and Budget (OMB) Memo M-08-16, "Guidance for Trusted Internet Connection Statement of Capability Form." The policies and regulations section of the RFQ noted that "Quoters are also required to comply with Federal Information Processing Standards (FIPS), the 'Special Publications 800 Series' guidelines published by [the National Institute of Standards and Technology (NIST)], and the requirements of FISMA." Id.

The RFQ was set to close at 11:00 p.m. on July 8, 2011. Technosource filed its protest of the terms of the RFQ on July 7. TrueTandem filed a copy of the Technosource protest as its own protest on July 8, prior to the closing time for the RFQ. The protesters assert that the limitation on the location of vendors' non-U.S. based data centers is unnecessarily restrictive of competition, that the government community cloud sub-lot specifications are unnecessarily restrictive of competition and exceed the government's legitimate needs, and that requirement 17 c. of the common technical requirements is ambiguous and contradictory to the provision of a public cloud solution.[3]

[3] The protesters' primary protest arguments are addressed in this decision. Additional arguments not addressed in the decision were reviewed by our Office and found to be without merit.

ANALYSIS

Data Center Location Requirement

The protesters argue that the solicitation's provision requiring vendors to locate their data services in "designated countries" as defined by FAR § 25.003 is unduly restrictive of competition because the requirement has no basis in law or regulation, and there is no otherwise legitimate need for such a restriction.[4]

As a general matter, a contracting agency has the discretion to determine its needs and the best method to accommodate them. Parcel 47C LLC, B-286324, B-286324.2, Dec. 26, 2000, 2001 CPD ¶ 44 at 7. In preparing a solicitation, a contracting agency is required to specify its needs in a manner designed to achieve full and open competition and may include restrictive requirements only to the extent they are necessary to satisfy the agency's legitimate needs. 10 U.S.C. § 2305(a)(1) (2006); Innovative Refrigeration Concepts, B-272370, Sept. 30, 1996, 96-2 CPD ¶ 127 at 3. To the extent a protester challenges a specification as "unduly restrictive," that is, challenges both the restrictive nature of the requirement as well as the agency's need for the restriction, the procuring agency has the responsibility of establishing that the specification is reasonably necessary to meet its needs. The adequacy of the agency's justification is ascertained through examining whether the agency's explanation is reasonable, that is, whether the explanation can withstand logical scrutiny. Trident World Sys., Inc., B-400901, Feb. 23, 2009, 2009 CPD ¶ 43 at 3. If the agency establishes support for the challenged solicitation term, the burden shifts to the protester to show that it is clearly unreasonable. Outdoor Venture Corp.; Applied Cos., B-299675, B-299676, July 19, 2007, 2007 CPD ¶ 138 at 5.

GSA has offered various justifications for the data center location requirements set forth in the RFQ. In its agency report, GSA acknowledged that the specification represented a compromise between the security needs of federal agencies (which desired all data to be stored and processed in the United States) and the United States Trade Representative's (USTR) office (which according to the agency, advised that a U.S. data center limitation impermissibly restricted free trade). Agency Report (AR), Legal Memo, at 7. Nonetheless, GSA has argued that the government has a need to know where its data resides and transits, because when U.S. government data crosses national borders, the governing legal, privacy, and regulatory regimes

[4] The protesters' also argue that the restriction violates FAR § 25.408(3), which specifies that a contracting officer must "not include technical requirements in solicitations solely to preclude the acquisition of eligible products." Because we conclude that the restrictions do not otherwise meet a legitimate government need and sustain the protest on that basis, we need not address the protester's argument in this regard.

become ambiguous and raise a variety of concerns including the potential of foreign jurisdictions to assert access rights to U.S. Government data.

Later, in response to specific questions from our Office, GSA argued that the data center location requirements were not unduly restrictive or unreasonable because GSA was attempting to achieve a "balance between security and free trade," and that "[t]o state that data centers can be located anywhere in the world would be irresponsible, given the many factors that must be addressed when considering risk inherent in any IT system." GSA Response at 6.

Finally, our Office also held a hearing in this protest. During the hearing, we again requested that GSA explain the basis for its data center location requirements. In response, GSA repeated that the solicitation had originally limited data center locations to the continental United States, but that the Office of Management and Budget (OMB) and the USTR considered the limitation restrictive of trade, and advised GSA to permit data centers located in foreign countries. Transcript at 13-14. During the hearing, the contracting officer testified that GSA expressed its view that allowing data centers located in foreign countries was unnecessary under applicable trade agreements, specifically the Trade Agreements Act (TAA), 19 U.S.C. § 2512, et seq., but that OMB and the USTR nonetheless wanted to expand the requirements to data centers located outside the U.S. Id. at 25-26.

The contracting officer further explained that after GSA determined to expand the requirements to include CLINs for cloud solutions utilizing data centers outside the United States, it found that it had no list of countries that it considered acceptable, or any basis to exclude one country versus another. Id. at 18-19. In the absence of making country-by-country determinations, the contracting officer explained that limiting data centers to "designated countries" under the TAA allowed for the exclusion of countries of particular concern such as Cuba, Iran, North Korea, and China, id. at 21, and would ensure at least some trade framework was in place between the U.S. and the government of any foreign country in which a data center was located, since "designated countries" are covered by trade agreements with the United States. Id. at 22-23. Ultimately, GSA acknowledged that the addition of CLINs for non-U.S. data centers reflected a compromise given the concerns raised by OMB and the USTR, Id. at 31, and acknowledged that it expects the non-U.S. CLINs to see very limited, if any, use. Id. at 23, 27.

As an initial matter, we concur with the agency's stated position to OMB and the USTR, that the requirements at issue are not mandated by the TAA. As a general matter, the TAA requires the acquisition of only U.S.-made or designated country end

products or U.S. or "designated country" services, unless certain exceptions apply.[5] FAR § 25.403(c)(1).

According to FAR § 25.402(a)(2), when analyzing the origin of services--to determine whether the services are of a "designated country"--the determination is made based on "the country in which the firm providing the services is established." Since compliance with the TAA in this context turns on where a cloud provider's business is established--and not on where the data centers that process and store subscriber data are located--the location of a provider's data centers would not be determinative of TAA compliance.[6]

We do not, however, conclude that GSA's explanations for the non-U.S. data center location requirements are otherwise reasonable, or withstand logical scrutiny. First, with regard to GSA's argument that the government has a need to know where U.S. government data resides and transits, this objective is accomplished by the requirement for vendors to identify the locations of their data centers. Second, while we appreciate the security concerns and legal ambiguities associated with subjecting

---

[5] The agency and the protesters both acknowledge that all GSA Schedule 70 contract holders are subject to the TAA.

[6] In both its agency report and supplemental agency report, GSA argued that the data center location requirements did not put "companies from designated countries at any disadvantage against domestic [companies]," and agreed that "[w]here a company is established (the FAR measure for origin) and data center location are two entirely different things." Agency Report, Legal Memo, at 7. In its supplemental agency report, GSA reiterated that "[d]ata center location has nothing to do with where the quoter's company is established." Supplemental Agency Report, at 7. In post-hearing comments, GSA, without any explanation, reversed its position on whether data center location was relevant to the TAA origin of services analysis. For the first time, GSA argued that it is necessary to restrict data center location to assure compliance with the country of origin requirements of the TAA. In this connection, GSA argued that FAR § 25.402(a)(2), requiring the contracting officer to "determine the origin of services by the country in which the firm providing the services is established," should not be interpreted to mean that the origin of services is the country in which the firm is, for example, incorporated; rather, the agency suggests that the contracting officer should be able to consider the location of the servers as solely determinative of the origin of services. We disagree. A plain reading of FAR § 25.402(a)(2) dictates that the origin of services is determined based on the country in which the firm providing the service is legally established, not on the location from which the service is ultimately provided. Moreover, applying GSA's interpretation, cloud services could be provided by firms incorporated or headquartered in non-designated countries, e.g., China, simply because they will be using data servers located in a designated country. It is not apparent that such a result would be consistent with the TAA.

U.S. government data to the jurisdictions of foreign countries,[7] to the extent the solicitation allows for locating U.S. government data outside the United States, it is apparent that the limits drawn by GSA in this regard have been established in an arbitrary manner.

In this connection, the legal ambiguities and hazards associated with locating data outside the jurisdiction of the United States exist without regard to whether a country is a "designated country" under the TAA. GSA has provided no explanation for why its security concerns would be less acute in relation to data stored or processed in designated countries, which include, for example, Yemen, Somalia, and Afghanistan, versus data stored or processed in non-designated countries, such as Brazil, India or South Africa. Further, GSA has acknowledged that it has no basis to differentiate between countries with acceptable data rights regulations and those with unacceptable data rights regulations. In fact, examples articulated by the agency regarding concerns about foreign governments asserting jurisdiction over U.S. government data involve countries that would be considered designated countries under the solicitation.[8] Accordingly, we conclude that GSA has failed to proffer an adequate explanation for limiting non-U.S. based data centers to those countries listed as designated countries in accordance with the TAA, and we sustain the protest on this basis.

Government Community Cloud Requirement

The protesters generally argue that the government only cloud deployment model which is contemplated by the RFQ is unduly restrictive because it is essentially redundant with the less restrictive public cloud model, which is also contemplated by the RFQ.[9] In this regard, the protesters assert that, after accounting for the technical and security requirements set forth by the RFQ, there is no meaningful distinction between the public cloud deployment model and the government cloud deployment model.

---

[7] Given GSA's explanation of the benefits of regulatory consistency, and the avoidance of cross-border data transit, it is apparent why agencies may be justified in requiring the maintenance of data and data servers within the United States.

[8] During the hearing at our Office, GSA cited problems with data maintained in Europe; however, many of the countries in Europe are defined as "designated countries" under FAR § 25.003 since many of the countries in Europe are parties to the World Trade Organization Government Procurement Agreement. Tr. at 22 and 38

[9] The protesters also assert that they are aware of only one entity currently offering cloud infrastructure that purports to meet the RFQ's definition of a government community cloud: Google, Inc.

Prior to addressing the protesters' challenge in this regard, we first review relevant definitions provided by the NIST "Special Publications 800 Series" guidelines, with which the vendors were advised to comply. For example, NIST Special Publication 800-145 is titled "The NIST Definition of Cloud Computing (Draft)," and provides general background on cloud computing deployment models. As relevant, according to NIST 800-145, in a public cloud, "the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services." In contrast, in a community cloud, "the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy and compliance considerations)." In addition, community clouds may also be managed by the users or a third party, either on premise or off premise. NIST 800-145, at 3.

Under this RFQ, the requirements for the public cloud sub-lot state that "[t]he Quoter shall provide a public cloud with an appropriate Government issued domain name for a Moderate Impact System." RFQ at 53. In comparison, the requirements for the government community cloud sub-lot state that "[t]he Quoter shall provide a cloud specifically limited to "Government clients" with an appropriate Government issued domain name for a Moderate Impact System." RFQ at 49. Thus, as the parties recognize, the only operational distinction between the public cloud and the government community cloud stems from what entities can have their data co-located in these two cloud deployment models. In the public cloud, an agency may be a co-tenant with any entity, government or non-government, while in the government community cloud, co-tenancy is restricted to "Government clients."[10] The protest therefore turns on whether the government community cloud's restriction on possible co-tenants provides a legitimate benefit to the government. We conclude that it does.

In response to the protesters' allegations, GSA argues that there are seven points of distinction between the two deployment models, based on a general discussion of the topic presented in NIST special publication NIST 800-146. We agree with the protesters' criticism of the agency's argument in nearly every regard,[11] but one. In the security area, we conclude that the evidence presented in the NIST Special Publication 800 Series of guidance demonstrates the existence of security

---

[10] Although we ultimately deny the protesters challenge to the government community cloud requirement, since we sustain this protest on other grounds we encourage GSA to consider whether the government community cloud requirement could be better defined, and more substantially justified in an amended RFQ.

[11] The protester generally asserts, correctly, that the distinctions between a "public cloud" and "community cloud" as defined by NIST, do not translate to the public cloud and government community cloud under the RFQ, because under the RFQ, both deployment models are subject to identical common technical requirements.

vulnerabilities unique to co-tenants in a multi-tenant cloud environment. On the basis of these unique risks, we conclude that the identity of the co-tenants in a given cloud deployment model can present a meaningful security distinction. As it concerns the RFQ, we conclude that the risk mitigation afforded in this regard by a cloud deployment model limited to U.S. government entity co-tenants is sufficient to constitute a reasonable basis for the requirement.

Specifically, NIST 800-144, "Guidelines on Security and Privacy in Public Cloud Computing," identifies risks inherent in multi-tenancy and co-location of data, and establishes that limitations on multi-tenancy can contribute a level of security beyond that offered by the minimum security standards applicable to both the public cloud and government community cloud under the RFQ. NIST 800-144 explains that a cloud system is constructed from multiple layers. NIST 800-144, at 4. The lowest layer consists of the provider's physical plant, such as power, air conditioning, and communications connectivity. Id. On top of that layer is the hardware layer, which contains the physical processors, data storage components, and network routers that constitute the cloud's resources. Id. The remaining layers denote the "logical elements" of the cloud environment. Id. Through software--commonly software programs known as "virtual machine monitors" or "hypervisors"--the provider's physical hardware is divided into a far greater number of "virtual machines."[12] Id. at 19. The hypervisor software can then be programmed to task the virtual machines to process the subscribers' data, and to maintain logical separation between virtual machines to prevent subscribers from viewing other subscribers' data. Id. at 19, 22.

However, NIST 800-144 also explains that the hypervisors do not provide unassailable software and data isolation. The special report specifically states that:

> Multi-tenancy in virtual machine-based cloud infrastructures, together with the subtleties in the way physical resources are shared between guest virtual machines, can give rise to new sources of threat. The most serious threat is that malicious code can escape the confines of its virtual machine and interfere with the hypervisor or other guest virtual machines.

NIST 800-144, at 23. The report provides several examples of "attack vectors" possible in a co-tenant environment, beginning with mapping the cloud provider's infrastructure, which researchers have shown to be possible in a cloud providers' service. Id. By mapping the cloud, an attacker can identify the location of a target virtual machine, and create new virtual machines directly co-tenant with the target virtual machine. Id. The attacker can then attempt to bypass or overcome the hypervisor's containment system, which has proven possible. Id. For example, NIST

[12] The NIST guidance also states that, while virtual machine technology is commonly used at this layer, other means of providing the necessary software abstractions are not precluded. NIST 800-144 at 4.

800-144 states that "a serious flaw . . . was discovered in the power management code of [one] hypervisor," and that "a denial of service vulnerability, which could allow a guest virtual machine to crash the host computer along with other virtual machines being hosted, was also uncovered in . . . [another] popular virtualization software product." Id. at 23-24. The NIST report also explains several other, more indirect, attacks that can be staged from within a cloud system.[13]

While FISMA, HSPD-12, and OMB M-05-16, among other security related standards, apply to all cloud deployment models established under the RFQ, GSA explained that these standards provide only the framework, or baseline, for conducting an IT security inquiry. More specifically, GSA stated that:

> dating back to 2002 [NIST and FISMA's guidance] . . . has developed a set of controls that are geared toward agency implemented solutions. And although even since 2002 we have had, you know, contractor-owned, contractor-operated or COCO, if you will, environments that provide these services, they're still generally viewed within the context of single tenancy. And that's why, especially as you look at FISMA, if you were to search FISMA for any controls regarding virtualization as a case in point, you know, specific technology that's generally employed within cloud environments--not all but some cloud environments--the only control that exists within NIST's interpretation for FISMA is one that says it's probably a good idea to virtualize.

Transcript, at 62-63.

Accordingly, in conducting the required FISMA certification and accreditation of multi-tenant outsourced cloud IT systems, heads of agencies must look beyond the bounds of the existing guidance in their examination of risk. Such an examination may lead to the consideration of the risks presented by co-tenancy of agency data with the data of, for example, potentially hostile foreign entities. Such a risk would simply not be present in a cloud limited to U.S. government entities.[14] Given NIST's

---

[13]GSA also stated, with regard to a multi-tenant environment that, "[i]t's all zeros and ones. Someone has a higher possibility of [hacking] into that than they would if I was completely segmented in a private community cloud, and even less if I had all my controls and my environment was completely hardware-specific to me. So, I have less possibility of someone coming into my system and cracking the code and hacking in to my system." Transcript, at 50-51.

[14] While limiting a cloud to U.S. government entities may not mitigate the risks associated with threats posed by persons operating within those government entities, such risks will always exist. The limitation does, however, insulate government entities from being unnecessarily exposed to threats posed by co-

(continued...)

substantiation of unique risks present in multi-tenant cloud environments, the additional layer of security provided by a cloud limited to U.S. government entities--the ability to operate in an environment exclusive of foreign, business, and other potentially hostile entities--presents, in our view, a meaningful benefit inherent to the government community cloud set forth in the RFQ, that could properly be considered as a part of an ordering agency's risk analysis. On this basis, we conclude that there is a meaningful security advantage to the government community cloud deployment model set forth in the RFQ, which justifies the inclusion of the requirement.

Ambiguous Technical Requirements

The protesters next allege that the common data center facilities requirements are ambiguous and potentially inconsistent with the provision of a public cloud. Generally, a contracting agency must provide offerors with sufficient detail in a solicitation to enable them to compete intelligently and on a relatively equal basis. AirTrak Travel et al., B-292101 et al., June 30, 2003, 2003 CPD ¶ 117 at 12-13. A solicitation ambiguity exists where two or more reasonable interpretations of the terms of the solicitation are possible. Ashe Facility Servs., Inc., B-292218.3, B-292218.4, Mar. 31, 2004, 2004 CPD ¶ 80 at 10.

The protesters' arguments center on requirement 17 c. of table 8 of the RFQ, and are informed by the entirety of requirement 17 of that table, which states:

> 17. The Quoter shall describe their solutions to provide effective separation of network traffic meeting the following objectives:
>
> a. All inbound and outbound data, inclusive of all mail messages, including between the Government and other co-tenants, can be routed through a dedicated network connection.
>
> b. The service must exclude co-tenant data, or any other third party data, not intended for the Government from being transmitted through a Government network connection.
>
> c. The service must exclude data intended solely within the Government from being routed through an external (non-government) network connections [sic].

(...continued)
tenancy with actors which may join a public cloud specifically to exploit their co-tenancy status in order to obtain or corrupt government data.

RFQ at 39. While the protesters represent that they understand the requirements associated with 17 a. and b., they have alleged that they do not understand the meaning of the term "external (non-government) network connections" in requirement 17 c. In this regard, they assert that the meaning of the term is not apparent from the requirements associated with 17 a. and b., and is not expressly defined within the RFQ. The protesters argue that given the lack of definition within the RFQ, the language of requirement 17 c. is impermissibly vague.

Prior to the closing date of the RFQ, GSA solicited questions from potential vendors concerning the RFQ's requirements. One such question specifically asked GSA to clarify, with respect to requirement 17 c., "what 'external network connection' refers to." Question and Answer No. 178. GSA did not provide a meaningful response to this question; rather, GSA generally advised that 17 c., "specifies the requirements that are applicable to cloud-based technology and services" and noted that the "requirements for this section are divided into the following areas: service-management requirements and data center facilities requirements." Id.

During the hearing convened for this protest, our Office requested that the parties further explain their interpretation and understanding of the above requirements. Concerning requirement 17 c., GSA explained as follows:

> So this . . . really becomes a requirement of [the Department of Homeland Security's] Trusted Internet Connection referenced architecture. FISMA and the NIST controls only cover Trusted Internet Connection . . . And it really just implies that the agency should use, take, and follow the referenced architecture guidance that exists there. But it's through these OMB memorandums that agencies are instructed to use Trusted Internet Connection. And then the underlying requirements are spelled out in the referenced architecture, which is mentioned.

Transcript at 112-113.

Acknowledging that the 17 c. requirement stems from Department of Homeland Security (DHS) Trusted Internet Connection referenced architecture, GSA points us to the DHS' "Federal Network Security, Trusted Internet Connection (TIC) Update, July 29, 2009," (TIC Update) document to define the meaning of "external connection" in the context of requirement 17 c. It is not apparent however, that potential vendors would have understood the 17 c. requirement in the context of the TIC Update definition, where the RFQ did not otherwise incorporate or reference the TIC Update document. Moreover, while the DHS' TIC Update document does

provide a meaningful definition of "external connection,"[15] it also identifies "external connection" as one of several "ambiguous terms" that the document hopes to clarify. TIC Update, July 29, 2009, at 5. Again, absent any reference to this document in the solicitation, or in response to the specific question seeking clarification of the 17 c. "external network connection" requirement, it is not apparent how vendors could have had a common understanding of the acknowledged "ambiguous" term. We therefore sustain this aspect of the protest as well.

RECOMMENDATION

We sustain the protesters' challenge to the data center facilities location requirement of the RFQ as well as their challenge regarding the ambiguity of requirement 17 c. in this solicitation. We recommend that GSA amend the RFQ to reflect its actual needs concerning non-U.S. data center locations, clarify its 17 c. requirements, reopen the competition, and allow offerors to submit new or revised proposals. We also recommend that the protesters be reimbursed the costs of filing and pursuing their protests, including reasonable attorneys' fees. Bid Protest Regulations, 4 C.F.R. § 21.8(d)(1). Technosource and TrueTandem should submit their certified claims for these costs, detailing the time spent and the costs incurred, directly to the agency within 60 days of receiving our decision. 4 C.F.R. § 21.8(f)(1).

The protest is sustained.

Lynn H. Gibson
General Counsel

[15] Specifically, the document states, in relevant part, that an "external connection" is a "physical or logical connection between information systems, networks, or components of information systems and networks that are, respectively, inside and outside of specific Department or Agency's (D/A) Certification and Accreditation (C&A) boundaries established by the D/A." TIC Update, July 29, 2009, at 10.