IN THE UNITED STATES COURT OF FEDERAL CLAIMS
Bid Protest

GOOGLE, INC.,	**AGREED-TO PUBLIC VERSION**
and	
ONIX NETWORKING CORPORATION	
Plaintiffs,	
v.	**No. 10-743 C** **Judge Braden**
THE UNITED STATES,	
Defendant,	
and	
SOFTCHOICE CORPORATION,	
Defendant-Intervenor.	

Plaintiffs' Motion For Judgment On The Administrative Record, Reply To Defendant's And Defendant-Intervenor's Oppositions To Plaintiffs' Motion For Preliminary Injunction, And Response To Defendant-Intervenor's Motion To Dismiss

Timothy Sullivan
1909 K Street, N.W., 6th Floor
Washington, D.C. 20006
(202) 585-6930 (tel.)
(202) 508-1028 (fax)

Attorney of Record for Plaintiffs Google, Inc. and Onix Networking Corporation

Of Counsel:

Katherine S. Nucci
Scott F. Lane
Thompson Coburn LLP

Dated: December 3, 2010

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Regulations

IN THE UNITED STATES COURT OF FEDERAL CLAIMS
Bid Protest

GOOGLE, INC.,	**AGREED-TO PUBLIC VERSION**
and	
ONIX NETWORKING CORPORATION	
Plaintiffs,	
v.	**No. 10-743 C** **Judge Braden**
THE UNITED STATES,	
Defendant,	
and	
SOFTCHOICE CORPORATION,	
Defendant-Intervenor.	

Plaintiffs' Motion For Judgment On The Administrative Record, Reply To Defendant's And Defendant-Intervenor's Oppositions To Plaintiffs' Motion For Preliminary Injunction, And Response To Defendant-Intervenor's Motion To Dismiss

Plaintiffs Google, Inc. ("Google") and Onix Networking Corporation ("Onix") hereby submit their Motion for Judgment on the Administrative Record and Reply to Defendant's and Defendant-Intervenor's Oppositions to Plaintiffs' Motion for Preliminary Injunction ("Def. Opp." and "Int. Opp."), as well as Plaintiffs' Response to Defendant-Intervenor's Motion to Dismiss ("Dismissal Motion"). For the reasons described herein, the Court should grant Plaintiffs' Motion on the grounds that the Department of the Interior ("DOI") improperly

selected the Microsoft product on a sole-source basis to satisfy DOI's requirement for a unified, agency-wide messaging system.

The Def. Opp. selectively described the facts to make it appear that, after conducting exhaustive market research into various messaging products and computing cloud models, DOI reasonably determined that only the Microsoft Business Productivity Online Suite-Federal ("BPOS-Federal") could satisfy DOI's minimum needs. In reality, the Administrative Record ("AR") paints a very different picture. The AR shows that DOI chose a Microsoft solution – one that preceded Microsoft's launch of BPOS-Federal by many months – more than a year ago without a sole-source justification pursuant to Federal Acquisition Regulation ("FAR") Subpart 6.3 and solely because DOI had established the Microsoft Office suite as a departmental standard in a standardization memo issued in September 2002. DOI then developed its requirements or "minimum needs" collaboratively with Microsoft in the ensuing months, leading to the June 2010 "proof of concept" project to migrate the Bureau of Indian Affairs ("BIA") to the Microsoft solution and, ultimately, to DOI's Request for Quotations ("RFQ") issued on August 30, 2010 for the purpose of completing the migration to DOI's other offices and bureaus. DOI's so-called extensive market research was tailored after the fact in 2010 to support the 2009 sole-source selection of a Microsoft solution.

There is no dispute that DOI has had problems with its disjointed e-mail system, or that DOI needs a secure, unified messaging solution to replace the 13 systems currently owned and operated by the various DOI bureaus and offices. These problems and needs, however, do not trump the Competition in Contracting Act's ("CICA") mandate for full and open competition, and DOI's *post hoc* justifications for the selection of Microsoft's solution do not stand up under close scrutiny. Google's messaging solution, Google Apps for Government, was given no

serious consideration by DOI, and DOI did nothing to assess the security of Google's cloud model even though Google Apps is the only computing cloud to have successfully undergone the rigorous certification and accreditation ("C&A") process for Federal Information Security Management Act ("FISMA") authorization.

There is more than one responsible source for a secure, unified messaging solution provided in a cloud computing environment and, thus, DOI has improperly circumvented CICA's requirements for a competitive procurement.

I. STATEMENT OF FACTS ("SOF")

1. Between November 2007 and May 2009, DOI's Chief Technology Officer ("CTO") [redacted]." AR Tab 14, pp. 175-77. DOI has had access to Gartner analysts and materials [redacted]." AR Tab 34. On April 15, 2009, [redacted]. AR Tab 14, p. 176. On April 27, 2009, [redacted]." *Id.* On May 14, 2009, [redacted]." *Id.* Later, on May 28, 2009, [redacted]

[redacted]." *Id.* at p. 177.

2. In June 2009, DOI started [redacted]." *Id.* at p. 180. According to the document in the AR, the [redacted] was last updated on [redacted] and [redacted]. AR Tab 33.[1] The [redacted] states that it is DOI's intention "[redacted]" because DOI had "[redacted]" and "[redacted]." *Id.* at p. 1098. The scope of the [redacted]," (p. 1099) starting with a [redacted]. *Id.* at pp. 1100-01. The [redacted]

[redacted]

[1] Based on discussions with Defendant's counsel, it is unclear whether the [redacted].

[redacted]

* * *

[redacted]

Id. at p. 1106.

3. The [redacted] further stated that [redacted]." This support would include [redacted]." *Id.* at p. 1107. DOI's CTO, Mr. William Corrington, was the [redacted], and Mr. Andrew Jackson, DOI's Deputy Assistant Secretary for Human Capital, Performance and Partnerships, was designated as [redacted]." *Id.* at pp. 1093 and 1100.

4. DOI asked Gartner [redacted]. In a letter dated October 16, 2009, Gartner advised DOI that [redacted]." AR Tab 14, p. 181. Further, Gartner stated "[redacted]

[redacted]

[redacted]." *Id.*

5. As the [redacted], DOI [redacted]. E-mails contained at Tab 32 of the AR evidence [redacted]. *See* Exhibit A attached hereto.[2] DOI and Microsoft [redacted] (AR Tab 32, pp. 1088-89) and [redacted] (Exhibit A, pp. 1-3). Both Mr. Jackson and Mr. Corrington [redacted], described by Mr. Corrington on January 8, 2010 as DOI's "[redacted]." AR Tab 32, pp. 1050-51. Even [redacted]" AR Tab 32, pp. 1046, 1048 and 1050; Exhibit A, p. 2. On February 6, [redacted]

[redacted]

Id. at pp. 1045-46. [redacted] responded by [redacted]

[2] Exhibit A is a chronological summary of events from April 2009 to August 2010 as reflected in e-mail exchanges and other documents contained at various Tabs in the AR. The document is not a supplement to the record but was created to facilitate the Court's review of the record, most particularly the lengthy and repetitive e-mail threads contained at Tab 32.

[redacted]." *Id.* at p. 1045.

6. During this same time frame in mid-to-late 2009, Google representatives were attempting to engage DOI officials in substantive discussions about Google's ability to meet DOI's unified messaging requirements. Mr. Corrington met with Google's Mr. Dave Standish on July 8, 2009 to discuss DOI's goals and Google's interest in meeting those goals, but subsequent Google requests for meetings were either ignored or declined. Exhibit A, pp. 1-2 (referencing AR Tab 6). On September 15, 2009, Google publicly announced its intent to create a Google Apps cloud computing environment dedicated only to government customers, and that Google was near the completion of its FISMA C&A package to be submitted to the Government by the end of the year. *See* http://googleenterprise.blogspot.com/2009/09/google-apps-and-government.html.

7. Consistent with [redacted], DOI awarded a task order to [redacted]." AR Tab 36. [redacted]." *Id.* at p. 1176. The task order had a six-month period of performance. *Id.* at p. 1179.

8. On February 18, 2010, DOI finally agreed to a Google request for a meeting. Mr. Corrington, Mr. Jackson and another DOI official, Mr. Bernard Mazer, met with three Google

representatives, including Google's Vice-President of North America. Exhibit A, p. 2 (referencing AR Tab 6); *see also* AR Tab 9, p. 150.[3] The meeting agenda included executive introductions, an update of the FISMA certification status of Google's cloud messaging solution, and Google's expressed desire for further, more detailed discussions regarding Google's ability to meet DOI's requirements. Complaint, ¶ 7.

9. On February 24, 2010, Microsoft publicly announced its plans to launch BPOS-Federal. AR Tab 32, p. 1044. Microsoft's press release stated that BPOS-Federal "is launching today for U.S. federal government agencies, related government contractors and others that require the highest levels of security features and protocols." Complaint, ¶ 40.

10. In April 2010, Google's Mr. Standish made further requests to meet with DOI officials. Exhibit A, p. 3 (referencing AR Tab 6 and Tab 32 e-mails). On April 28, 2010, Mr. Corrington and Mr. Mazer attended a public Google presentation on cloud computing for government IT leaders. AR Tab 9, p. 150. After the presentation, Mr. Corrington informed Google's representatives that "a path forward had already been chosen" for DOI's messaging solution and there would be no opportunity for Google to compete because its solution did not meet DOI's security requirements. Complaint, ¶ 8.

11. Google addressed its reaction to Mr. Corrington's statements, and its concerns about DOI's strategy, in a letter dated May 17, 2010 sent to Ms. Debra Glass, DOI's Chief of Acquisition Management. AR Tab 2. Google's letter described how its Google Apps solution was a competitive alternative for DOI and why a solicitation restriction for a Microsoft solution

---

[3] Tab 9 purports to be a summary of meetings and other interactions between DOI and Google prepared by Mr. Corrington based on his meeting notes. This summary presents a one-sided, self-serving description of the discussions at the referenced meetings and, as such, has little probative value as to the actual discussions (particularly what was said by Google's representatives) that took place at the referenced meetings.

was contrary to CICA's competition requirements. Google requested that Ms. Glass investigate Google's concerns and that the anticipated solicitation be revised to allow for the offer of Google Apps as a potential solution. Ms. Glass forwarded the letter to Mr. Corrington, stating "[redacted]." AR Tab 6, p. 101.

12. Around this same time, DOI was [redacted]. AR Tab 32, p. 1036 ([redacted]"); *see also* AR Tab 31, p. 859 (Corrington June 4 memo regarding [redacted]). The record does not explain why or how DOI [redacted].

13. On May 27, 2010, Ms. Glass sent an invitation to Google to make a presentation of the Google Apps solution. AR Tab 4. The letter made no reference to Google's May 17 letter; instead, it referenced the "market research discussions" at the February 18 meeting. DOI asked Google to address how its solution meets each of 11 stated requirements at a meeting to be held at DOI headquarters. Referencing market research conducted from October 2009 through March 2010 by a third-party vendor (*i.e.*, [redacted]), the letter stated that "[t]he information obtained from the market research will be used to improve the Government's knowledge of private industry's commercial and government practices and capabilities" and that "[m]arket research sessions are the preliminary steps taken to enhance a procurement strategy." *Id.* at p. 48.

14. Google made its presentation at a meeting held on June 9, 2010 that was attended by six DOI officials, including Mr. Jackson and Mr. Corrington. AR Tab 9, p. 151; AR Tab 14,

p. 184-85. According to Mr. Corrington's summary of his meeting notes, Google's representatives informed DOI that Google was incapable of providing service on a dedicated infrastructure and that Google's "community cloud" for government customers (federal, state and local) would satisfy DOI's needs.

15. On that very same day, Mr. Corrington [redacted] ("[redacted]"). AR Tab 31A. According to [redacted]" *Id.* at p. 1003.1. Section 8 of the [redacted]." *Id.* at p. 1003.3. This section further states that, [redacted]." *Id.*

16. Based on the [redacted], Section 5 of the [redacted]. *Id.* at p. 1003.2. [redacted]

[redacted]. *Id.* at p. 1003.4. [redacted]. Finally, the [redacted]. *Id.* at pp. 1003.7-1003.10.

17. On June 10, 2010, DOI issued Modification No. 0003 to [redacted]. AR Tab 31, p. 855. The prices are for "[redacted], p. 901. Exhibit J to the [redacted]. *Id.* at p. 902.

18. On June 17, 2010, Google sent DOI's Mr. Jackson a letter thanking DOI for the opportunity to make the presentation on June 9, stating that Google Apps could meet or exceed DOI's requirements, and explaining Google's view that a private cloud was neither necessary nor reflective of industry "best practices." Google's letter stated that DOI's security concerns could be addressed in the same manner as a recent GSA solicitation for enterprise e-mail and collaboration services from a commercial provider of cloud computing services and software, wherein GSA's Statement of Objectives required the contractor to "provide security controls that are confirmed to meet the security standards for Moderate Impact systems as described in NIST SP 800-53 with an accepted Certification and Accreditation (C&A)." By stating its needs in

such a manner, Google stated that DOI and the taxpayers would benefit from a much more robust competition.[4] AR Tab 5.

19. Mr. Jackson sent Google's Mr. Standish an e-mail the following day to thank Google for the presentation and the June 17 letter. Mr. Jackson asked Google questions about when the complete government-only community cloud, and elements of the cloud, would be available. Mr. Jackson further stated:

> Also, I feel I need to clarify a misconception noted in your letter. As I stated last week, DOI has not finalized its procurement strategy for the planned cloud messaging solution. We continue to evaluate all options in light of our business requirements.

AR Tab 32, p. 1034 (emphasis added). DOI's Competition Advocate, who had received a copy of Google's June 17 letter, also wrote to Mr. Standish stating that her office was "confident that Google, and all interested parties, will be treated fairly during the process." *Id.* at p. 1033.

20. On June 23, 2010, Mr. Standish responded to Mr. Jackson's questions regarding the current availability of Google Apps and the messaging functionality. Regarding Mr. Jackson's assurances that DOI's procurement strategy was not yet finalized, Mr. Standish wrote:

> Finally, we are encouraged by your clarification that the DOI has not finalized its procurement strategy for the planned cloud messaging solution and is continuing to evaluate all options in light of DOI's business requirements. However, we believe you should know that we continue to hear very disconcerting rumors that project deployment activities are already underway to migrate the DOI to a pre-determined messaging solution notwithstanding the lack of any legitimate market research or a "full and open" competition for the DOI's messaging solution. We would

[4] On December 1, 2010, GSA announced its award of a five-year task order pursuant to the referenced solicitation, stating that "GSA is the first federal agency to move e-mail to a cloud-based system agencywide." The $6.7 million award was made to Unisys Corp, which partnered with Google and two other companies. *See* www.gsa.gov (Latest News – "GSA Becomes First Federal Agency to Move E-mail to the Cloud Agencywide"). Under this Unisys task order, GSA's entire e-mail system will move to Google's government community cloud.

> therefore appreciate your confirmation that product selection remains part of DOI's procurement strategy that is currently being defined.

AR Tab 32, p. 1029-30.

21. Later that same day, Mr. Jackson sent Mr. Standish an e-mail seeking clarification of when Google's complete government-only messaging solution would be available because Mr. Standish's explanation appeared to conflict with statements made during the June 9 presentation. As to Mr. Standish's concerns about the rumors Google was hearing, Mr. Jackson again sought to allay those concerns:

> As for the "disconcerting rumors" you allude to below, I would encourage you to treat rumor and innuendo as just that. As I am sure you are aware, moving from 13 separate messaging platforms to 1 messaging instance is necessarily a traumatic process for many of our bureaus. It is one of the challenges of bringing transformative change to a very decentralized department. We have of course required our bureaus to commence preparations for a migration to our new messaging system, and we believe these preparation activities will be useful for a successful migration, no matter which messaging provider is ultimately selected. If you are being told otherwise, I would request that you recommend that your source contact me directly, so that I can help correct any misconceptions.

AR Tab 32, pp. 1026-27 (emphasis added).

22. The next day, June 24, Mr. Standish answered Mr. Jackson's questions by stating that Google's engineering team had delivered the government-only cloud ahead of schedule, and reiterating that Google would contractually commit to meeting any DOI-specified implementation timelines "given the importance of the DOI as a Google customer." Further, Mr. Standish stated:

> Finally, I want to thank you for again confirming that the procurement strategy and product selection are still being evaluated by the DOI. As you can see, Google is sincerely interested in the opportunity to compete for the DOI's business.

> Please let us know if you need any additional details on our products or our FISMA certification and accreditation package.

AR Tab 32, p. 1023.

23. Mr. Jackson forwarded Mr. Standish's e-mail to many colleagues with the following message: "[redacted]." AR Tab 6, p. 114. Mr. Jackson did not respond to subsequent e-mails from Mr. Standish, except to tell Mr. Standish to address all correspondence to Ms. Glass. Exhibit A, p. 5 (referencing e-mails at AR Tabs 6 and 32).

24. DOI issued its "Risk Assessment of Cloud Deployment Models for Department of the Interior Unified Messaging" ("Risk Assessment") on June 29, 2010. AR Tab 11. DOI used a framework developed by the Cloud Security Alliance ("CSA")[5] [redacted]. As defined by the National Institute of Standards and Technology ("NIST"), a cloud "solely dedicated to DOI" is a private cloud whereas a cloud dedicated "to DOI and other Federal government customers only" is a community cloud. *Id.*, p. 162. The Risk Assessment discussed [redacted]

[5] The Cloud Security Alliance is a not-for-profit organization formed as a "grassroots effort to facilitate the mission to create and apply best practices to secure cloud computing." AR Tab 14S, p. 305.

[redacted]." *Id.*, p. 166. The Risk Assessment contradicts itself by [redacted]. Moreover, the Risk Assessment does not mention [redacted].

25. Also on June 29, 2010, [redacted] issued a report summarizing its market research.[6] AR Tab 12. The [redacted] report states that its research included "[redacted]. *Id.*, pp. 170 and 172. The abbreviated report [redacted]." After [redacted]. The report concludes that only BPOS-Federal "[redacted]." *Id.*, p. 171.

26. DOI issued [redacted] on July 15, 2010. The first [redacted]. AR Tab 16. The decision states that no

[6] It is not clear why [redacted].

[redacted]. *Id.*, p. 761. The second [redacted]. AR Tab 15. The decision addresses the [redacted]. The decision concludes that, among other things, DOI requires "[redacted]." *Id.*, p. 756.

27. On July 26, 2010, Google publicly announced that its Google Apps had received FISMA certification and that Google Apps for Government had been launched. Google's Mr. Standish notified Mr. Corrington of the FISMA certification on August 2, 2010. AR Tab 6, p. 108. Mr. Standish asked Mr. Corrington to "confirm what next steps DOI has planned for a competition and selection of a messaging solution for the Department." *Id.* Mr. Standish sent another e-mail the same day inquiring about DOI's next steps and what Google could do to show DOI that Google Apps for Government "can help advance successful mission outcome by the Department." *Id.*, pp. 109-10. Mr. Corrington responded that Mr. Standish should direct all correspondence to Ms. Glass, the Bureau Procurement Chief. *Id,* p. 110.

28. On August 11, 2010, Google's Mr. Standish sent another e-mail to Mr. Jackson and Ms. Glass because Google had just learned of the POC project. Mr. Standish stated:

> As you surely recognize, it is very troubling to learn that this project was being developed behind-the-scenes while we were being provided with repeated assurances of a full and open competition. Google is making the following requests of DOI:

> 1. We request that the DOI provide an explanation of how the pilot meets the Competition in Contracting Act's requirements for full and open competition and how it comports with your statements that the DOI has not finalized its procurement strategy.
>
> 2. We request that DOI immediately award and undertake a similar pilot for Google Apps to fully evaluate and compare the technologies. Such action would be consistent with your statement that DOI is continuing to explore all options regarding the best means for satisfying its messaging system requirements.
>
> As we have repeatedly stated, Google seeks only a fair and equal opportunity to compete for the DOI's messaging system as we firmly believe that Google's solution offers the best value to the Government. I look forward to your prompt response to this communication.

AR Tab 32, pp. 1004-05. Mr. Standish also sent an e-mail to Mr. Corrington seeking his feedback on the Google Apps for Government announcement. AR Tab 6, p. 111. No one at DOI responded to either of Mr. Standish's e-mails.

29. Google's announcements of its Google Apps for Government product offering and its FISMA certification prompted an internal reaction at DOI. In a memorandum to Mr. Jackson and Ms. Glass, dated August 20, 2010, Mr. Corrington addressed [redacted]. AR Tab 21. Mr. Corrington expressed his opinion that the [redacted]." *Id.*, p. 784. The memo then referenced and quoted from a news article in the online publication Washington Technology [redacted]. Assuming the accuracy and truth of this article, but without

any attempt at verification, Mr. Corrington concluded that the [redacted]." *Id.* Regarding Google's FISMA certification, Mr. Corrington [redacted]. *Id.*, pp. 784-85. The memo omitted the obvious fact that, regardless of the newness of cloud computing technology, [redacted]. *See* AR Tab 14KK, [redacted]," pp. 702-05 (describing federal laws and guidance that specify requirements for protecting federal systems and data). Mr. Corrington's memo also failed to note that BPOS-Federal is not FISMA-certified.

30. DOI published a Limited Source Justification pursuant to FAR 8.405-6 and in support of the RFQ that was issued on August 30, 2010. AR Tab 27. The Limited Source Justification, executed by various DOI officials between August 19 and August 30, addresses the same concerns and rationale contained in the prior justifications, concluding that BPOS-Federal is the only commercial product that satisfies DOI's requirements. *Id.*, pp. 847-48.

31. DOI issued the RFQ on August 30, 2010 via GSA e-Buy. Consistent with DOI's Project Plan developed more than a year earlier, the RFQ represents the continuation of the POC project and completion of the migration of all DOI users to the BPOS-Federal messaging solution. AR Tabs 22-30.

II. THE COURT HAS JURISDICTION TO DECIDE, AND PLAINTIFFS HAVE STANDING TO BRING, THIS CASE

The facts show that Google continuously demonstrated its desire and commitment to provide a messaging solution to meet DOI's needs throughout the period of DOI's alleged market research, and there is no doubt that, but for the restrictions articulated in the Limited Source Justification, Plaintiffs would have submitted a proposal in response to the anticipated solicitation. Contrary to the Defendant-Intervenor's position, urged upon the Court in its Dismissal Motion, the Court clearly possesses jurisdiction to decide Plaintiffs' protest against DOI's violations of law in connection with a procurement. Moreover, under applicable precedent, Plaintiffs have standing to bring this action.[7]

A. The Court's Relevant Bid Protest Jurisdiction

When deciding a motion to dismiss for lack of subject matter jurisdiction, the Court is "obligated to assume all factual allegations to be true and to draw all reasonable inferences in plaintiff's favor." *Kenney Orthopedic, LLC v. United States*, 88 Fed.Cl. 688, 697 (2009), quoting *Henke v. United States*, 60 F.3d 795, 797 (Fed.Cir. 1995). Nonetheless, a plaintiff bears the burden of establishing jurisdiction by a preponderance of the evidence. *See Reynolds v. Army & Air Force Exch. Serv.*, 846 F.2d 746, 748 (Fed.Cir. 1988). In doing so, a plaintiff need only set

---

[7] Plaintiffs acknowledge that Onix, unlike Google, did not file a protest at the GAO before proposals were due in response to the RFQ. Defendant-Intervenor cited the decision in *Blue & Gold Fleet L.P. v. United States,* 492 F.3d 1308 (Fed.Cir. 2007), in support of its argument that Onix lacks standing. Dismissal Motion at pp. 10-12. The underlying rationale for the Federal Circuit's holding in *Blue & Gold* was Section 1491(b)'s mandate that "the courts shall give due regard to the interests of national defense and national security and *the need for expeditious resolution of the action.*" *Id. at* 1313 (emphasis in original). Since Google filed its GAO protest before proposals were due, DOI was precluded from making a contract award during the pendency of the protest. 31 U.S.C. § 3553(c)(1). Thus, as a practical matter, Onix's joining Google as a plaintiff in this bid protest does not impede or otherwise affect the Court's adherence to this statutory mandate underlying the holding in *Blue & Gold.*

forth a *prima facie* showing of jurisdictional facts to survive a motion to dismiss. *Raymark Indus., Inc. v. United States*, 15 Cl.Ct. 334, 338 (1988).

The U.S. Court of Federal Claims has recognized three categories of bid protest jurisdiction under the Tucker Act: (1) a pre-award solicitation protest, which is an objection to "a solicitation by a Federal agency for bids or proposals for a proposed contract or to a proposed award...of a contract," 28 U.S.C. § 1491(b)(1); (2) a post-award contract protest, which objects to "the award of a contract," *id.*; or (3) a protest objecting to "any alleged violation of statute or regulation in connection with a procurement or a proposed procurement." *Id.*; *see also Magnum Opus Technologies, Inc. v. United States*, 94 Fed.Cl. 512, 527 (2010). This protest fits squarely within the third category because Plaintiffs object to DOI's violations of the Competition in Contracting Act ("CICA") and FAR Subpart 6.3 in connection with DOI's acquisition of a messaging solution based on the Limited Source Justification. *See* Complaint ¶¶ 49, 50, 52.

The U.S. Court of Appeals for the Federal Circuit recently provided additional insight into the analysis of protests under this third category and observed that "the phrase, 'in connection with a procurement or proposed procurement,' by definition involves a connection with any stage of the federal contracting acquisition process, including the process for determining a need for property or services." *Distributed Solutions, Inc. v. United States*, 539 F.3d 1340, 1346 (Fed. Cir. 2008) (quotations omitted). In *Distributed Solutions, Inc.*, the Federal Circuit was deciding an appeal from this Court's dismissal of two software vendors' protest for lack of subject matter jurisdiction. The underlying facts were that the U.S. Agency for International Development and the Department of State jointly initiated market research through a Request for Information ("RFI") for commercial off-the-shelf software. *Id.* at 1342. After completing their review of the RFI responses, however, the agencies announced that they would

use a specific prime integrator, SRA, to select the vendors that would provide the software. *Id.* The award was added to SRA's pre-existing Millennia Government Wide Acquisition Contract ("GWAC") with the General Services Administration ("GSA"), and SRA coordinated with the agencies to select subcontractors for the necessary software. *Id.* SRA did not select the software of Distributed Solutions, Inc. and another vendor, and the two then filed a protest action with this Court.

The Federal Circuit reversed this Court's dismissal of the action, holding that the Court possessed jurisdiction under the third category of protests. The Court confirmed that the phrase "in connection with" is "very sweeping in scope" (*id.* at 1345, quoting *RAMCOR Services Group, Inc. v. United States*, 185 F.3d 1286, 1289 (Fed. Cir. 1999)) and the definition of "procurement or proposed procurement" should be given the definition under 41 U.S.C. § 403(2). That definition includes "all stages of the process of acquiring property or services, beginning with the process for determining a need for property or services and ending with contract completion and closeout." *Id.* Because the agencies' RFI started the process for determining the agencies' need for the software, at first to be procured directly from vendors and changed to an indirect procurement through SRA, the Federal Circuit held that the decision to change course was made in connection with a proposed procurement. *Distributed Solutions, Inc.*, 539 F.3d at 1346.

B. Google And Onix Are Prospective Bidders

The Dismissal Motion notably avoided decisions on pre-award bid protests based upon this third category ("in connection with a procurement or proposed procurement"). Rather, Defendant-Intervenor relies upon a slew of post-award protests that have limited relevance to the

facts in this case.[8] Defendant-Intervenor's focus on these cases evidences a fundamental misunderstanding of what Google and Onix are protesting. Whether Google or Onix submitted a proposal or intended to submit a proposal in response to the actual RFQ (that was restricted to offers of a Microsoft product) is irrelevant. Indeed, Defendant-Intervenor's position is illogical since neither Google nor Onix supplies the specified Microsoft product and any proposal from them obviously would be rejected as noncompliant.

Just as the agencies in *Distributed Solutions, Inc.* initiated market research by soliciting RFI responses from software vendors, DOI initiated market research and had discussions with Google wherein Google repeatedly expressed its interest and commitment to provide its messaging solution to DOI. *See* AR Tabs 6 and 32; Complaint ¶¶ 3-4 (stating that "Google licenses its products and solutions to customers either through direct agreements or Google's licensed resellers" and identifying Onix as a licensed reseller); *see also* AR Tab 31, pp. 881-882 (reflecting an industry practice that even where an agency contracts through resellers, it enters licensing agreements with the manufacturer); SOF ¶ 2 ([redacted]"). Thus, Google and Onix were prospective suppliers for a proposed procurement that was not restricted to the proposal of the Microsoft BPOS-Federal solution.

It matters not that DOI ultimately implemented its Limited Source Justification through a solicitation that was restricted to GSA Schedule 70 contract holders. Despite Defendant-

[8] Post-award protests relied upon heavily by Defendant-Intervenor in this argument include: *Rex Service Corp. v. United States*, 448 F.3d 1305, (Fed. Cir. 2006); *MCI Telecommunications Corp.* v. *United States*, 878 F.2d 362 (Fed. Cir. 1989); *Pure Power!, Inc. v. United States*, 70 Fed. Cl. 739 (2006); *Myers Investigative & Sec. Servs. v. United States*, 275 F.3d 1366 (Fed. Cir. 2002). *See* Defendant-Intervenor's Motion to Dismiss at 5-8.

Intervenor's argument to the contrary, *Savantage Financial Services, Inc. v. United States*, 81 Fed.Cl. 300, 306 (2008), addressed remarkably similar circumstances. Savantage argued that the Department of Homeland Security ("DHS") violated statutes and regulations in connection with a "Brand Name Justification" to migrate the DHS agency components to a single financial management system. The DHS implemented the Brand Name Justification through a solicitation that was restricted to offerors with Enterprise Acquisition Gateway for Leading-Edge Solutions ("EAGLE") IDIQ contracts. Savantage did not have an EAGLE IDIQ contract or license its software through any reseller with an EAGLE contract, but it supplies a software product that competes with those chosen in the Brand Name Justification. The Court held that Savantage had standing to protest the Brand Name Justification. The Court concluded that Savantage was a prospective bidder because it supplied a competitive product to those selected in the Brand Name Justification, and DHS knew Savantage could have competed. *Id.* at 306. DOI's implementation of the Limited Source Justification through an RFP restricted to Schedule 70 contract holders presents the same situation confronted by the Court in *Savantage*, and the result on the jurisdiction and standing issues should be the same. [9]

Similarly, in *Distributed Solutions, Inc.*, the Court declined to narrow the standing requirements under this third category of bid protests based on the government's ultimate choice of a particular contract method, *i.e.*, through SRA's GWAC contract. The Court held that the

---

[9] Defendant-Intervenor also intermittently attempts to distinguish *Savantage* because Savantage was an incumbent that had previously supplied software for six of the twenty-two DHS components. However, there is simply no support in *Savantage* that incumbency is a prerequisite to qualifying as a "prospective offeror" for standing purposes. Although the Court stated that Savantage "clearly could have competed" because it was the incumbent (*id.*), Google also made it abundantly clear that it could have competed in a proper competition. *See* AR Tabs 6 and 32. Further, there is no indication that the protesters in *Distributed Solutions, Inc.* were incumbents; rather, they established their prospective offeror status by responding to market research. *Distributed Solutions, Inc.*, 539 F.3d at 1344-1345.

vendors were prospective bidders simply because they had responded to an RFI in the initial market research phase[10] and were prepared to submit bids pursuant to an anticipated competitive solicitation. In a decision involving similar facts, this Court aptly described why protesters in the same situation as Google and Onix qualify as "prospective bidders:"

> As explained above, applying Section 3551(2)'s definition of "interested party" to Section 1491(b) would limit potential plaintiffs thereunder to actual and prospective bidders, but there is no indication in the working of Section 3551(2) that Congress intended to go further and exclude from the scope of "prospective bidders" those parties that intended to present a bid but were prevented from so doing in violation of controlling statutes and regulations. Defendant has not presented a viable rationale based in sound contracting policy for Congress to have intended such a result and allow a contracting officer to make a legally erroneous decision not to entertain an offer from a party seeking to compete for contract work, and then to rely upon that decision as the basis for concluding that the party was not an "interested party."

ATA Defense Industries, Inc. v. United States, 38 Fed.Cl. 489, 495 (1997).

Finally, Defendant-Intervenor also claims that *CCL, Inc.* v. *United States,* 39 Fed. Cl. 780 (1997) ("*CCL*") is no longer good law because it applied a somewhat different definition of "interested party." Although Defendant-Intervenor is correct that *CCL* predates *Am. Fed'n of Gov't Employees v. United States*, 258 F.3d 1294, 1300-02 (Fed. Cir. 2001) ("*AFGE*"), the *AFGE* Court did not overrule *CCL*. In fact, *CCL* also relied upon the CICA definition of "interested party" to frame its result. *CCL,* 39 Fed.Cl. at 790 ("The thrust of the GAO definition, however, is clearly relevant."). Moreover, there is absolutely no indication the result would have been different under the *AFGE* Court's definition because the Federal Circuit has cited *CCL's* jurisdictional result approvingly. *See Distributed Solutions, Inc.*, 539 F.3d at 1345, n.1.

---

[10] Although the vendors had submitted "proposals" in the initial market research, the RFI had made it clear that the proposals were "for market research purposes only" and would "not result in a contract award." *Id.* at 1342.

Accordingly, *CCL* remains good law and provides additional support for the conclusion that Google and Onix qualify as prospective offerors.

C. Google And Onix Have A Direct Economic Interest In The Procurement

The Court also must reject Defendant-Intervenor's argument that the standard in *Weeks Marine, Inc. v. United States*, 575 F.3d 1352, 1361-62 (Fed. Cir. 2009) ("*Weeks Marine*") should not apply because it was limited to pre-award cases where there were no bids or offers submitted. In *Weeks Marine*, a contractor filed a pre-award protest alleging that the agency's decision to seek negotiated proposals rather than sealed bids violated the CICA. The Court recognized that there are various tests to determine whether a protester has a direct economic interest in a procurement and explained that the "substantial chance test" (advocated by Defendant-Intervenor) has a strange application in a pre-award context because "there have been neither bids/offers, nor a contract award. Hence, there is no factual foundation for a 'but for' prejudice analysis." *Id.* at 1361. Accordingly, the Court upheld the determination that "direct economic interest" could be shown by a "non-trivial competitive injury which can be addressed by judicial

relief." *Weeks Marine* at 1362[11]; *see also Magnum Opus Technologies, Inc.*, 94 Fed. Cl. at 530-31 (elaborating on the impracticalities of the "substantial chance test" when the protester alleges a violation of law in a "proposed procurement" and adopting the *Weeks Marine* standard); *Distributed Solutions, Inc.*, 539 F.3d at 1345 ("The contractors also possess a direct economic interest in the government action at issue in that they were...deprived of the opportunity to compete for the provision of [the services].")

Defendant-Intervenor advocates for the standard typically adopted in post-award protests. *See Allied Materials & Equipment Co., Inc. v. United States*, 81 Fed.Cl. 448, 456-457 (2008) (comparing the test ultimately adopted by *Weeks Marine* to the "substantial chance test"). Essentially, Defendant-Intervenor argues that Google and Onix do not possess a direct economic interest in DOI's messaging procurement because neither had a "substantial chance" of receiving a contract to provide Microsoft products. *See* Dismissal Motion at p. 8. Defendant-Intervenor has conveniently ignored the second half of the test it seeks to apply, *i.e.*, "that there was a 'substantial chance' that it would have received the contract award but for the alleged error in the procurement process." *Information Tech. & Applications Corp. v. United States*, 316 F.3d 1312,

---

[11] Defendant-Intervenor's reliance on a recent decision, *CS-360, LLC v. United States*, 94 Fed.Cl. 488 (2010), for the proposition that the "substantial chance" test should apply in this case is misplaced. While the Court did ponder whether the *Weeks Marine* test may only apply to pre-award protests where no bids or offers have been submitted, we contend that such a narrow reading of that case would emasculate the rationale for applying a different test in a pre-award protest involving challenges to solicitation improprieties. Although GAO regulations and court precedent require that such protests must be filed before proposals are due in order to be timely, agencies are not required by CICA to stop the submission of bids/offers or to refrain from evaluating those bids/offers while a timely protest is pending. Only the award is stayed automatically by CICA or, in a protest before this Court, if an injunction is issued. It would be wholly unjust and irrational then to subject protesters in the same boat as Plaintiffs (*i.e.*, precluded from competing because of the challenged restrictions in a solicitation) to the "substantial chance" test, especially in light of the fact that the protester in *Weeks Marine*, which was held to the less stringent "non-trial competitive injury" test, was not precluded from competing by the terms of the challenged solicitation.

1319 (Fed.Cir. 2003) (citations omitted) (emphasis added). Thus, even assuming *arguendo* that the "substantial chance test" should be applied in this case, Google and Onix could satisfy it. If the Limited Source Justification did not improperly restrict the product offering to the BPOS-Federal solution, Google contends that it would offer a messaging solution with more functionality at far less cost, which features clearly would give Google a substantial chance for award.

Finally, Plaintiffs have satisfied the requirement to demonstrate prejudicial harm resulting from DOI's actions. "A deprivation of an opportunity to compete is sufficient economic harm to demonstrate prejudice for purposes of standing." *Magnum Opus, supra,* 94 Fed.Cl. at 533, citing *Distributed Solutions,* 539 F.3d at 1345.

For the foregoing reasons, the Court should deny Defendant-Intervenor's Dismissal Motion. Under the circumstances of this case and based on applicable precedent, Plaintiffs have standing to file their protest and the Court has jurisdiction to decide this case.

III. DEFENDANT'S PROCUREMENT ACTIONS VIOLATED STATUTORY AND REGULATORY REQUIREMENTS

The record establishes that, without doubt, DOI selected the Microsoft product in 2009, long before any justifications were prepared as required by CICA and FAR Subpart 6.3 to use other than full and open competition for the procurement of a unified messaging solution.[12] Everything DOI did in 2010 assumes the validity of the 2009 selection of Microsoft [redacted]. If that selection was improper, the whole house of cards falls. Even if the Court lends credence to the [redacted] DOI in

[12] It is obvious from the record that DOI's selection was [redacted]. SOF ¶ 1. It is not [redacted] role, however, to define DOI's minimum needs or to determine that an exception to CICA's competition mandate is justified.

2010 to support its 2009 pre-selection, DOI's support for determining that only the Microsoft BPOS-Federal solution will satisfy DOI's minimum needs lacks a rational basis for several reasons.

First, DOI's market research was [redacted]. Second, DOI's alleged minimum need for an external private cloud for its messaging solution lacks a rational basis because, in actuality, the Microsoft computing and data storage cloud to be furnished is not private and DOI did nothing to assess the security of a federal-government-only community cloud versus that of a federal/state/local-government-only community cloud. Moreover, despite repeated offers by Google, DOI never reviewed Google's FISMA package to ascertain the security controls and processes implemented by Google to mitigate security risks. Had DOI done so as part of its market research, it would have learned that an independent auditor's report included the results of nearly 1,000 test cases performed against the Google Apps platform in addition to vulnerability and penetration testing, and found Google's overall level of operational risk to federal agencies to be "low." Finally, DOI's justifications cannot be deemed rational since the very product DOI is to obtain, BPOS-Federal, does not satisfy DOI's alleged minimum needs as reflected in the Risk Assessment and DOI's various justification documents.

DOI and Microsoft have been collaborating closely and extensively for more than a year to implement DOI's improper sole-source procurement of a unified messaging solution, all the while as DOI was falsely assuring Google that a messaging solution had not been chosen and that a full and open competition would be conducted. DOI's conduct should not be condoned by the Court.

A. Standard of Review

The Tucker Act, as amended by the Administrative Dispute Resolution Act, Pub. L. No. 104-320, § 12, 110 Stat. 3870, 3874 (Oct. 19, 1996), authorizes the U.S. Court of Federal Claims to review agency decisions under the standards of the Administrative Procedure Act, 5 U.S.C. § 706 (the "APA"). 28 U.S.C. § 1491(b)(4). In a bid protest action, the Court may set aside an agency decision that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A); *see Centech Group, Inc. v. United States*, 554 F.3d 1029, 1037 (Fed. Cir. 2009). Under this standard, the Court may set aside a procurement if "(1) the procurement official's decision lacked a rational basis; or (2) the procurement procedure involved a violation of regulation or procedure." *Id.* (quoting *Impresa Construzioni Geom. Domenico Garufi ("Impresa") v. United States*, 238 F.3d 1324, 1332 (Fed. Cir. 2001).

When the Court reviews a challenge brought on the first ground, it is obliged "to determine whether the contracting agency provided a coherent and reasonable explanation of its exercise of discretion." *Impresa*, 238 F.3d at 1332-1333 (citations omitted). "[T]he disappointed bidder thus bears a heavy burden of showing that the award decision had no rational basis." *Id.* Furthermore, courts have set aside agency decisions where the agency "entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise." *Ala. Aircraft Indus. Inc.-Birmingham v. United States*, 586 F.3d 1372, 1375 (Fed. Cir. 2009) (quotation marks and citations omitted). "When a challenge is brought on the second ground, the disappointed bidder must show a clear and prejudicial violation of applicable statutes or regulations." *Impresa*, 238 F.3d at 1333 (quotation marks and citations omitted).

Courts apply these same review standards when considering protests against solicitation requirements alleged to be unduly restrictive of competition and in violation of CICA. *E.g., CHE Consulting, Inc. v. United States,* 552 F.3d 1351, 1354 (Fed.Cir. 2008). When considering whether an agency's restrictive specifications are reasonably necessary, this Court has observed:

> While the court "recognize[s] the relevant agency's technical expertise and experience, and defer[s] to its analysis unless it is without substantial basis in fact," *Federal Power Comm'n v. Florida Power & Light Co.,* 404 U.S. 453, 463, 92 S.Ct. 637, 644, 30 L.Ed.2d 600 (1972), the court must also perform an informed review of even technical decisions in order to meaningfully exercise its jurisdiction. *Prineville Sawmill Co., Inc. v. United States,* 859 F.2d 905, 910-11 (Fed. Cir. 1988). Furthermore, "[e]xpertise is a rational process and a rational process implies expressed reasons for judgment." *Mid-State Fertilizer v. Exchange Nat'l Bank,* 877 F.2d 1333, 1339 (7th Cir. 1989) (quoting *Federal Power Comm'n v. Hope Natural Gas Co.,* 320 U.S. 591, 627, 64 S.Ct. 281, 299-300, 88 L.kEd. 333 (1944) (Frankfurter, J., dissenting)). The court "must ensure that the agency has 'examin[ed] a satisfactory explanation for its action including a rational connection between the facts found and the choice made.'" *Rainbow Navigation, Inc. v. Department of Navy,* 783 F.2d 1072, 1080 (D.C. Cir. 1986) (Scalia, J.) (quoting *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Automobile Ins. Co.,* 463 U.S. 29, 43, 103 S.Ct. 2856, 2866-67, 77 L.Ed.2d 443 (1983) (citation omitted).

Redland Genstar, Inc. v. United States, 39 Fed.Cl. 220, 231 (1997).

B. DOI Pre-selected Microsoft in Violation of CICA and FAR Subpart 6.3

CICA requires federal agencies to "obtain full and open competition through the use of competitive procedures" unless certain limited exceptions apply. 41 U.S.C. § 253(a)(1)(A). FAR Subpart 6.3 implements CICA's requirements and describes the process to be followed by agencies in order to properly invoke one of the limited exceptions. Agencies must justify in writing the use of noncompetitive procedures, as required by the process laid out in FAR Subpart 6.3, prior to entering into a contract. *ATA Defense Industries, Inc. v. United States, supra,* 38 Fed.Cl. at 498.

This case is unusual in that the facts show that, [redacted], 6.303-1, 6.303-2 and 6.304, DOI chose the Microsoft solution [redacted]. SOF ¶ 2. Then, for the next [redacted] which all other DOI users subsequently will be migrated pursuant to the contract awarded in response to the RFQ. The record does not contain a [redacted].[13]

If it does not violate the letter of FAR Subpart 6.3, this DOI/Microsoft collaboration clearly violates the spirit of those requirements. DOI determined in September 2009 that it needed a single e-mail system furnished by an external service provider, and it identified the Microsoft product as that single e-mail system. SOF ¶ 2. There is [redacted] or [redacted], that explains why Microsoft is the "only responsible source" of, or has a "unique capability" to provide, a single e-mail system.

---

[13] The numerous [redacted]. This Court and the Federal Circuit (and its predecessor) have recognized the existence and enforceability of implied-in-fact contracts where the requisite factors have been met. *E.g., BioFunction, LLC v. United States,* 92 Fed.Cl. 167, 172 (2010), citing *Sommers Oil Co. v. United States*, 241 F.3d 1375, 1378 (Fed. Cir. 2001); *see also Russell Corp. v. United States*, 537 F.2d 474, 482 (Ct.Cl. 1976). Moreover, there may be a [redacted]. *See* AR Tab 32, p. 1051 ([redacted]); AR Tab 33, p. 1106 ("[redacted]").

Nor is there a [redacted]. The only "justifications" for DOI's selection of the Microsoft product were its previous establishment of "Microsoft Exchange as the agency standard" and [redacted]." SOF ¶ 2.

These are not legally-sufficient justifications for avoiding CICA's requirement for full and open competition. The fact that DOI standardized to the Microsoft Office suite in 2002, or to Microsoft Outlook in 2006, does not dictate a "once Microsoft, forever Microsoft" result. While Microsoft's products likely were the industry standard in 2002, technological advancements in the computing industry have exploded and new, capable competitors have entered the market since then. Moreover, since most organizations have been using one or more Microsoft products because there used to be few alternatives, competitors such as Google have made their software products compatible with Microsoft applications. It is also noteworthy that, according to DOI's [redacted], the majority of DOI's bureaus and users were [redacted]. AR Tab 33, p. 1097 ("[redacted]"). Finally, since DOI made no attempt to [redacted].

In sum, DOI's decision in September 2009 that only the Microsoft messaging solution would satisfy DOI's need for a unified secure e-mail system was clearly contrary to law. The Court could – and we believe should – end its inquiry here. Even if the Court were to conclude that DOI complied with the requirements for a properly-authorized, written justification because it did so prior to the award of any contract, DOI's [redacted] are nonetheless factually and legally flawed.

C. DOI's *Post Hoc* Actions And Justifications Were Tailored To Support Its Improper Pre-Selection And Were Not Rationally Based

The logical gaps and inconsistencies in the AR prove that DOI's alleged market research and its resulting Risk Assessment were transparent byproducts of DOI's pre-selection of the BPOS-Federal community cloud. The contractually stated "objective" of the firm conducting market research for DOI was [redacted], and DOI's additional market research simply consists of [redacted]. Even when DOI eventually conducted its "Risk Assessment" – [redacted] – the assessment repeatedly referenced sources out of context and applied the CSA "framework" illogically. As a result, DOI failed to consider whether Google's government community cloud actually posed any more security risk than Microsoft's government community cloud. Furthermore, DOI's selection of BPOS-Federal arbitrarily sacrifices DOI's underlying concerns for enhanced security (*i.e.*, demonstrated FISMA compliance) as well as its alleged "need" for a federal-government-only cloud because it is ultimately obtaining a messaging solution with some elements hosted in public clouds. These compromises were made for a simple reason, namely, to conform to what Microsoft could provide.

1. DOI's *Post Hoc* Market Research

DOI's [redacted] a misleading story about DOI's market research, explaining that DOI tasked [redacted]. SOF ¶ 26. The AR tells a different story. Section Two of [redacted] Statement of Work clarifies the "Objective" of its contract with DOI:

[redacted]

AR Tab 36, p. 1173. This leaves no doubt that DOI merely contracted with [redacted] to create a paper trail to support the decision already made by DOI to procure the Microsoft solution. This alone undermines the value of any purported "research" by [redacted] and makes DOI's motives in creating "extensive" research utterly transparent.

Given the objective of its task, it is not surprising that [redacted] provided DOI with [redacted]. SOF ¶ 25. In [redacted] brief analysis (including the cover and appendix), [redacted]. AR Tab 12, p. 171. The only [redacted]. *Id.*, p. 172. Even with respect to its review of Microsoft's BPOS offering, [redacted]." *Id.*, p. 171. Microsoft's solution is not

FISMA-certified and, thus, [redacted]. *Id.*

In addition to the [redacted] analysis, DOI claims it conducted its own market research by reviewing industry and government reports on cloud computing. AR Tab 15, p. 756. Surprisingly, DOI did not prepare an analysis of these reports and how they guided DOI's product selection; instead, DOI [redacted] that superficially supported DOI's determination that it required a private cloud. DOI produced a plethora of third-party reports in the AR, which mostly provide generic considerations for technology professionals but certainly do not compare the security of Google's government cloud model against Microsoft's government cloud model. *E.g.*, AR Tab 14A ([redacted]); Tab 14B ([redacted]). Only one report, [redacted], comes close to a relevant discussion on specific cloud models. AR Tab 14U, p. 424 ("[redacted]"). However, that report was issued in June 2009, several months before Google's or Microsoft's government clouds were even announced. Moreover, the report [redacted].

Another [redacted] report discusses general risks that are unique to all governmental entities, but never indicates that sharing a cloud with state or local governments creates additional risk. AR Tab 14R, p. 293. Indeed, under the heading "[redacted]y. AR Tab 14R, p. 298, Note 2 ([redacted]

[redacted]).[14] Similarly, the summary notes of DOI's discussions [redacted]. AR Tab 14, pp. 175-185.

The [redacted] reports also include a few general discussions on Google, but there are no analyses or commentaries stating that a cloud including state and local government customers increases security risk. *See* Tab 14AA ([redacted]); Tab 14FF (a [redacted]); Tab 14HH ([redacted]). Thus, DOI's alleged "extensive" market research avoided any analysis of Google's government cloud, its features, or its FISMA-certified security controls. Consequently, DOI's market research failed to examine all relevant data and it failed to articulate "a satisfactory explanation for its action including a rational connection between the facts found and the choice made." *Redland Genstar, Inc. v. United States, supra,* 39 Fed.Cl. at 231 (holding that agency's restrictive specification was invalid because, *inter alia,* the reports and analyses relied upon by the agency did not support the choice made by the agency).

[14] The only other [redacted] report included in the AR that includes substantive commentary on government cloud computing is at Tab 14JJ. That report lists [redacted].

2. DOI's Requirement for a Federal-Government-Only Cloud (Often Mistakenly Referred To As A Private Cloud)

DOI supposedly eliminated Google from consideration because [redacted] market research concluded that Google did not offer a "private cloud." SOF ¶ 25. DOI's Risk Assessment and justifications identified DOI's actual requirement as a "data storage [and computing] infrastructure that is solely dedicated to DOI or DOI and other Federal government customers only." AR Tab 11, p. 156; Tab 15, p. 755; Tab 27, p. 847. As demonstrated below, DOI irrationally and arbitrarily conducted its Risk Assessment to reach this "minimum need" well after it had chosen and contracted for the Microsoft product. Even more importantly, however, DOI's stated requirement is not for a private cloud; rather, it is for a government community cloud, an infrastructure that is not rationally distinguishable from the infrastructure offered by Google's government community cloud.

i. Types of Computing Clouds

Defendant and Defendant-Intervenor imprecisely refer throughout their briefs to DOI's requirement for an infrastructure that is shared by DOI and other Federal government customers as one for a "private cloud." Def. Opp. at pp. 6, 18, 19, 24, 28, 30 (and in several headings); Int. Opp. at pp. 8, 18-20. In so doing, Defendant and Defendant-Intervenor have blurred the distinctions among defined cloud models in order to make the reports which compare "private" and "public" clouds appear relevant and, ultimately, to lend support to DOI's decision to reject Google's government cloud solution.

As defined by NIST, there are four different types of cloud models:

> *Private cloud.* The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

> *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). It may be managed by the organizations or a third party and may exist on premise or off premise.
>
> *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.
>
> *Hybrid cloud.* The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

AR Tab 14V, p. 437; Tab 11, p. 162; Def. Opp. at p. 6.

If DOI had defined a need for an infrastructure that was solely dedicated to DOI, it would be requiring a "private cloud." Although the BPOS-Federal solution might be available for purchase in a "private cloud," DOI's requirement was not so limited. Since DOI allows the infrastructure (owned and managed by Microsoft) to be shared among any Federal government customers, it is procuring a "community cloud." By comparison, Google Apps for Government shares its infrastructure among Federal, state and local government customers of Google, a limited community with common security and privacy concerns. Thus, Google Apps for Government is also a "community cloud."

Defendant's and Defendant-Intervenor's attempts to mischaracterize the cloud model being procured by DOI and to then compare public and private clouds to support the pre-selection of the Microsoft product are misleading and irrelevant. The record shows that DOI never considered whether Google's community cloud product would satisfy DOI's essential needs.

ii. DOI's Risk Assessment

DOI conducted the Risk Assessment at Tab 11 to establish its need for a cloud that shares infrastructure among only DOI and other Federal government customers. As the record reflects, this Risk Assessment represents nothing more than a *post hoc* justification for a choice made long before its creation. The Risk Assessment was completed on [redacted]. *C.f.*, SOF ¶ 17 ([redacted]), SOF ¶ 24 (dated June 29, 2010), SOF ¶ 12 ([redacted]). Oddly, the Risk Assessment was completed [redacted]. SOF ¶ 25. Consequently, there is no way [redacted]. Finally, the Risk Assessment post-dated DOI's [redacted], wherein the Microsoft solution was pre-selected [redacted].

Turning to the substance of the report, DOI's Risk Assessment selectively quotes statements, and takes others out of context, in the [redacted] so as to render questionable the value of the conclusions reached by DOI. For example, under the heading "[redacted]," DOI cites a [redacted]e. DOI's Risk Assessment reads:

[redacted]."

AR Tab 11, p. 163. However, that [redacted], included at Tab 14W, shows that DOI, for reasons that are obvious now, omitted the statement between the two quoted above, which reads: "[redacted]." AR Tab 14W, p. 472.[15]

The Risk Assessment goes on to state that "[redacted]." AR Tab 11, p. 163. The quotation that follows simply does not support DOI's assertion. DOI quotes [redacted]." *Id.* However, the context of that quote in the [redacted] at Tab 14R makes it clear that [redacted]. AR Tab 14R, p. 295.[16]

---

[15] The Risk Assessment cites this document as [redacted]." AR Tab 14W, p. 441.

[16] The pattern of taking quotes out of context is prevalent throughout the Risk Assessment. DOI quotes a [redacted]." DOI ignores the point of this paragraph by omitting the next sentence which reads: "[redacted]." AR Tab 14II, p. 686. And again, [redacted].

The only time the Risk Assessment mentions Google is when it references [redacted]. AR Tab 11, p. 162 ("[redacted]"). It does not discuss Google's [redacted].

Even the CSA "framework" applied by DOI to analyze its risk tolerance was applied incorrectly. Proper utilization of the CSA's framework would have required DOI to [redacted]. AR Tab 14Y, pp. 549-550 ("[redacted]"). This expected in-depth analysis would have allowed DOI to determine whether, for example, [redacted]. Instead of following the CSA guidelines, DOI [redacted]. *See* AR Tab 11, pp. 159-161. The result was that DOI unnecessarily and illogically determined that [redacted]. The point of CSA's Step Three is to choose an acceptable cloud model for each asset (AR Tab 14Y, p. 550 ("[redacted])); however, DOI [redacted]." The [redacted]," which DOI concluded was not

compatible with DOI's "appetite for risk." AR Tab 11, pp. 165-166. There is no substantive explanation accompanying this [redacted] selection.

Thus, the many flaws and omissions in the Risk Assessment are explained by DOI's obvious goal of defining its minimum needs around the Microsoft solution.

iii. DOI Did Not Rationally Consider Whether Sharing A Cloud With State And Local Governments Would Be An Acceptable Alternative To A Cloud With Only Federal Government Customers

Nowhere in the AR is there an assessment, analysis or even discussion of the reason why DOI rejected Google's government community cloud, namely, whether there are any unacceptable (or even increased) risks resulting from sharing a cloud with state and local government entities. Defendant's and Defendant-Intervenor's respective counsel have recognized this yawning gap in the record and have made up their own reasons for why Google's community cloud represents an unacceptable security risk. *See* Def. Opp. at p. 19; Int. Opp. at p. 13). Counsel, however, cannot supplement the record with retroactive justifications for DOI's decision. *See 210 Earll, L.L.C. v. United States*, 77 Fed. Cl. 710, 721-722 (2006) ("The APA requires a reasoned analysis at the time of the decision. It does not require a reasoned analysis only when the Contracting Officer's decision is challenged in court."); *Reilly's Wholesale Produce v. United States*, 73 Fed. Cl. 705, 713 n.12 (2006) ("In many ways, the *post hoc* invocation of these make-weight limitations only serves to amplify that [the agency's] original rationale for overriding the stay has a decidedly hollow ring.").

Even if the Court considers these arguments by counsel, the arguments are not substantively sound. Defendant's counsel claims that Federal computer users "will have passed background checks, completed basic information security training, and been instructed to follow Federal data safeguards." Def. Opp. at p. 19. However, there is no citation to demonstrate that

this is true, that it was considered important by DOI, or that Microsoft will guarantee that all Federal customers with data in its cloud will have complied with these same requirements. Moreover, there is no evidence in the record suggesting that every single user with access to DOI's e-mail system (which would include employees, contractors, and even volunteers)[17] will have undergone and passed background checks and completed security training. The same is true with respect to other Federal agencies whose end-users have access to the cloud. The security proficiency of the end-user should not be a consideration since the security controls to protect the confidentiality, integrity and availability of the data in the messaging solution are operated by the cloud provider, not the end-user.

Defendant also cites the Economic Espionage Act (18 U.S.C. § 1831, *et seq.*), the Freedom of Information Act (5 U.S.C. § 552), and the Federal Trade Secrets Act (18 U.S.C. § 1905) as laws peculiarly applicable to Federal employees, as opposed to state and local government employees. These laws bear no relationship to the security of any cloud computing model. The Economic Espionage Act applies to anyone, even state and local government employees. The Freedom of Information Act mandates disclosure of government records to the public unless specific exemptions apply, and has no relevance to security requirements related to such records. Finally, there is no indication in the record that the Federal Trade Secrets Act (a criminal law) would give DOI any right of action to force another Federal agency to maintain any security controls or to not disclose "trade secret" information. We would also note that most, if not all, states have enacted comparable FOIA and trade secret protection statutes that apply to their organizations and citizens.

---

[17] *See* AR Tab 24, p. 823, ¶ 10.10, describing the many types of "DOI Personnel" that will have access to DOI's e-mail system.

In addition, State and local governments process many of the same types of data that DOI processes, including a significant amount of sensitive and confidential data such as financial and budget information, personal identification information, and internal policy information. There is no evidence in the AR that state and local governments are less compelled to protect the information of their constituents than the federal government. Further, there is no evidence supporting the conclusion that a private cloud *per se* is more secure than a community or public cloud. The only way to make such a determination is to assess the security controls, processes and operations within a given cloud. Defendant-Intervenor's argument that "by restricting the cloud to Federal agencies, DOI has ensured that the other cloud users will have met fundamental Federal security requirements" (Int. Opp. at p. 13) is superficially misleading. The security consciousness of the end-user has little relevance to the security of the cloud solution. As anyone who has ever used e-mail knows, with a click of the mouse even the most security-conscious user (even those who have passed background checks) can mistakenly send a sensitive e-mail to the wrong person(s). In sum, the type of customer data stored in a cloud solution, and the type of user having access to the cloud, do not determine its security posture – security is a byproduct of the controls and processes implemented by the vendor.

Even though Google Apps for Government was announced in September 2009, the only time DOI appears to have even acknowledged Google's government community cloud was in an August 20, 2010 memorandum. SOF ¶ 29. This memo was written after DOI had contracted to migrate 5,000 BIA users to BPOS-Federal, after [redacted] had reported its market research, after DOI had conducted its Risk Assessment, after the Microsoft standardization justifications were issued, after the Limited Source Justification was written, and only six business days before the RFQ was released. Long before August 20, 2010, DOI had plotted its course of action, and the

memo was created as another after-the-fact "backup" document, the purpose of which was to denigrate Google's significant achievements.[18]

The limited explanations cited in the August 20 memo to brush aside Google's messaging solution were meaninglessly broad. The [redacted]." SOF ¶ 29. Neither of these broad statements reflects any actual consideration of why state and local data could not exist in the same cloud as Federal data; DOI does not recite any security requirements that differ among state, local or Federal agencies, and the AR includes no such information. In fact, there exists no evidence in the AR that a state or local government customer's having different security requirements or facing different impacts would create additional risk to the security of DOI's data. Indeed, each and every Federal agency is likely to face different impacts from a security breach. The [redacted] explanation for disregarding Google's FISMA-certified government community cloud is baseless, but it is apparent that DOI's management accepted it at face value.

Finally, the [redacted] reference to a news article about [redacted] does not establish the truth or accuracy of the article's contents. Moreover, DOI made no attempt to seek verification from Google, probably because

[18] The memo at Tab 21, titled "[redacted]". The document misleadingly characterizes Google's government cloud and FISMA certification as events first happening after the July 15, 2010 determination; however, Google announced the creation of its government cloud and the progress on its FISMA certification as early as September 2009 (SOF ¶ 6) and had updated DOI officials regarding the status on many occasions.

DOI had no interest in knowing whether the article was correct. In sum, the [redacted] explanation of why Google's FISMA certification did not impact the Microsoft selection is simply not credible.

iv. How Security Risk Should Be Assessed And The Significance Of FISMA

The [redacted] included at Tab 14KK confirms that the security of a cloud model is not defined solely by its classification as a public, private, community, or hybrid cloud. Rather, "[redacted]." AR Tab 14KK, p. 696. Table Three in that report lists [redacted]. AR Tab 14KK, p. 717, Table 3.

The [redacted] emphasis on vendor security controls is based on FISMA and applicable NIST standards. AR Tab 14KK, pp. 702-05 (describing policies, procedures and required controls established to protect Federal information and information systems). Pursuant to FISMA, NIST has published mandatory guidance for examining security controls, which is outlined in NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems." *Id.*, p. 704. This process includes categorization of information under Federal Information Processing Standards Publication ("FIPS") 199 and then the selection of controls pursuant to FIPS 200 and NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," which states at Section 2.2:

> A significant challenge for organizations is to determine the appropriate set of security controls, which if implemented and determined to be effective, would most cost-effectively mitigate

> risk while complying with the security requirements defined by applicable federal laws, Executive Orders, directives, policies, standards, or regulations (e.g., FISMA, OMB Circular A-130). Selecting the appropriate set of security controls to adequately mitigate risk by meeting the specific, and sometimes unique, security requirements of an organization is an important task—a task that clearly demonstrates the organization's commitment to security and the due diligence exercised in protecting the confidentiality, integrity, and availability of organizational information and information systems.[19]

Once the set of security controls is selected, the next steps are security control implementation, security control assessment, information system authorization, and security control monitoring. AR Tab 14KK, p. 704. The NIST SP 900-37 framework includes "the preparation of a security assessment and authorization package." *Id.* After thorough examination and testing of these controls, a vendor may receive FISMA certification of its product(s) based on a thorough and compliant C&A package prepared by the vendor.

According to [redacted]." *Id.*, p. 720. DOI apparently disagrees, having irrationally determined that Google's FISMA-certified government cloud is less secure than Microsoft's untested, non-certified government cloud. In fact, Defendant admits, astonishingly, that "[redacted]." Def. Opp., p. 23.

[19] *See* www.nist.gov/publication/nistpubs/800-53.

Although the CTO's August 20 memo correctly states that [redacted][20], it does not follow that the current guidance (followed by Google in preparing its FISMA C&A package) is inadequate for purposes of cloud computing deployments. AR Tab 14KK, p. 725 ("[redacted]").

There are no documents in the AR reflecting DOI's consideration of specific security controls or processes pursuant to FISMA and NIST standards for either Google's or Microsoft's government cloud solutions. On several occasions, Google offered its FISMA C&A package for DOI's review to enable DOI to assess the security of Google's government cloud pursuant to recognized government standards. *E.g.,* AR Tab 32, pp. 1023, 1005-1006. DOI rebuffed Google's offers. *Id.*[21] Even when Google announced it was the first cloud model to receive a FISMA certification, DOI still did not wish to consider Google's solution. SOF ¶ 30. DOI's conduct is particularly disturbing -- indeed alarming -- given the historically abysmal security of its bureaus' and offices' e-mail systems. *See* AR Tabs 41 – 46 (DOI OIG FY 04 – FY 09 FISMA Reports); *Cobell v. Norton,* 394 F.Supp.2d 164, 170-85 (describing FISMA and NIST requirements), 185-247 (detailing security deficiencies identified during DOI OIG FISMA

[20] In fact, such supplemental guidance was recently issued. The Federal Risk and Authorization Management Program (FedRAMP) was established to provide a standard approach to assessing and authorizing cloud computing services and products. A Proposed Security Assessment and Authorization for U.S. Government Cloud Computing was prepared by an inter-agency team, in collaboration with State and Local Governments, Private Sector, NGO's and Academia, and was published on November 2, 2010 for government and industry comments. *See* www.FedRAMP.gov.

[21] As stated at p. 28 above, if DOI had reviewed Google's FISMA certification package, it would have learned that, after rigorous testing, an independent audit found Google's overall level of operational risk to Federal agencies to be "low."

evaluations), and 247-271 (detailing numerous deficiencies in DOI's IT security program) (D.D.C. 2005). After the systemic security breaches in DOI's IT systems over the years, and the consequent tongue-lashing by Judge Lamberth in his *Cobell v. Norton* decisions, one would expect DOI to have proceeded "by the book" before deciding on its cloud computing solution. But that clearly did not happen, and there is simply no rational explanation for DOI's methodology for determining that only Microsoft's BPOS-Federal cloud deployment model will satisfy DOI's need for enhanced security.

3. DOI's Selection Of The BPOS-Federal Community Cloud Was An Irrational Choice

Based on DOI's purported requirements, as set forth in its *post hoc* Risk Assessment, the BPOS-Federal community cloud is an irrational choice. First, DOI has consistently professed its commitment to FISMA compliance. AR Tab 15, p. 750 ("Underlying all of the requirements described above is the need for DOI to meet the obligation to secure the messaging and collaboration system in compliance with the Federal Information Systems Management Act (FISMA) and other Federal security requirements..."); AR Tab 27, p. 846 (same). Notwithstanding this clear statement, the BPOS-Federal solution has not been FISMA certified, and there is no evidence in the AR that DOI ever evaluated the ability of the BPOS-Federal product to comply with FISMA-required controls and processes. Even when [redacted] allegedly conducted third-party market research on behalf of DOI, it only [redacted]. SOF ¶ 25.

According to Microsoft, the "[redacted]. SOF ¶ 5. Yet, DOI decided not to ensure that its "[redacted]" messaging solution to which it would standardize – at a cost of

approximately $59 million -- had a proven capability to achieve a FISMA certification.[22] This is true even though DOI has been repeatedly criticized for its failures to comply with FISMA. *See* AR Tab 37, p. 1205 ("The Department's CIO recently acknowledged, 'Interior is one of only five agencies still failing to comply with FISMA' and went on to state '5+ years – spent >$285 million and still getting failing grades on Congressional FISMA scorecard'... The Department's management of IT is rife with missed opportunities to improve and full of waste."); Tab 46, p. 1538, Figure 1 (showing FISMA certification as a constant problem issue for DOI); Tab 45, pp. 1497 (same) and 1503 ("Certification and accreditation of federal information systems is critical to securing the government's operations and assets."). Even though DOI's justification documents assert the ability to comply with FISMA and acknowledge that compliance through certification is the underlying security requirement, there is not a shred of evidence in the AR that DOI evaluated the ability of the unproven BPOS-Federal community cloud to achieve a FISMA certification.

Defendant admits that with the BPOS-Federal solution being obtained by DOI, the Microsoft management network, Office Live Meeting, and e-mail archiving will not be hosted in a computing and data storage infrastructure that is shared solely among DOI and other Federal customers. Def. Opp. at pp. 30-31. Defendant argues that the Microsoft management network and Office Live Meeting will not contain sensitive messaging information and cites to DOI's Risk Assessment at AR Tab 11, p. 167. The citation does not support the argument. As

---

[22] Unless and until the BPOS-Federal product is someday certified under the FISMA standards, DOI plans to rely upon SAS 70 security controls. AR Tab 24, p. 819. Ironically, DOI's own [redacted] market research indicates that [redacted]. AR Tab 14EE, pp. 661-662 ([redacted].")

mentioned above, DOI [redacted] during its Risk Assessment. DOI evaluated [redacted]." AR Tab 11, pp. 159-161. The public cloud these assets will be stored in [redacted]." DOI's Risk Assessment and justifications did [redacted], that required less security and could therefore reside in a public cloud. Indeed, it is readily apparent that DOI's cloud requirements have been evolving over time simply to fit the characteristics or limitations of the particular Microsoft product. For example, Microsoft's Office Live Meeting is on a separate infrastructure available to all Microsoft public and private customers.

Likewise, Defendant admits that archived e-mail messages will reside in a public cloud. Def. Opp. at p. 31. Defendant asserts that archived e-mail messages are not part of DOI's requirement for a federal-government-only community cloud. Defendant's argument is not supported by the record. The Risk Assessment provides that DOI's data storage infrastructure solely dedicated to DOI and other Federal government customers [redacted]. AR Tab 11, p. 167 (emphasis added). This clearly sets forth a requirement applicable [redacted]. Archived e-mail messages are nothing more than copies of messages that have been transferred to data storage to free up computing space.

The assertion that separate but adequate security measures apply to archived data, including stringent encryption (Def. Opp., p. 31), undermines DOI's stated reasons for requiring a computing and data storage infrastructure that is physically and logically isolated only for Federal government agencies. Encryption is a means of logically separating and securing data to prevent access by unauthorized users. "Logical" separation is achieved with software

applications and coding; for example, a bank's customers are prevented from accessing other customers' account information by such "logical" security measures even though all customer information physically resides on the bank's servers. DOI has set two different standards for security protection of the same messaging data – one for its online e-mail data (physically and logically isolated from all non-Federal users) and one for copies of the same e-mail data in an archiving system (encrypted and residing in a public cloud). Other than the inability of the proposed Microsoft solution to provide consistent security controls and protections for all messaging data – both archived and non-archived – DOI cannot explain or justify why these protections should be different, especially if both solutions are accessible online. As the recent WikiLeaks disclosures make vividly apparent, the risks presented by compromising messaging data would be the same regardless of the data's age or whether it is archived. Again, it is readily apparent that DOI has exempted archived e-mail messages from its restrictive requirements in order to accommodate shortcomings in Microsoft's products.

In summary, it is clear that the selection of BPOS-Federal was made by DOI long before any of the documents to support the decision were drafted. DOI's supporting documents do not provide a reasonable or rational analysis of its product selection and security considerations. Most importantly, nothing in the record demonstrates that DOI officials concluded (or even considered) whether sharing an infrastructure with state and local governments -- as opposed to sharing the infrastructure only with other Federal customers -- presented any unacceptable risks. Finally, the BPOS-Federal solution that DOI is acquiring does not satisfy DOI's stated "minimum needs," which are obviously a moving target in order to accommodate limitations of Microsoft's product offerings.

The Court should not condone DOI's clear attempts to circumvent CICA's mandate for full and open competition. DOI's documentation provides no rational basis to exclude the Google Apps for Government product from DOI's procurement of a unified, secure messaging solution. Plaintiffs respectfully submit that DOI's inconsistent and contradictory positions regarding its security requirements and which cloud deployment model it actually requires are clearly indicative of arbitrary and irrational decision-making regarding DOI's restrictive requirements and sole-source product selection. Accordingly, the Court should set aside DOI's decision to procure BPOS-Federal and require DOI to conduct a full and open competition based on its legitimate minimum needs.

IV. PLAINTIFFS WILL SUFFER IRREPARABLE HARM IF THE INJUNCTION IS NOT GRANTED

The briefing schedule set forth in the Court's November 30, 2010 Order calls for the final filing in this matter to be made on January 11, 2011. Under the agreement reached by the parties, Defendant will not make an award under the RFQ before January 25, 2011. There is no guarantee that the Court is going to be able to issue a decision in this matter by January 25, 2011. Under the circumstances, Defendant would be free to make an award under the RFQ at any time after that date, and prior discussions with Defendant's counsel should serve to alert the Court that Defendant believes that moving forward on its implementation efforts by late January is critical to Defendant's interests. Were Defendant to proceed in this fashion, Plaintiffs' chances of ever obtaining Defendant's business would be irreparably harmed.

Defendant's and Defendant-Intervenor's attempts to distinguish this case from the decisions Plaintiffs have relied on demonstrates that they have either seriously misunderstood or are deaf to the essential thrust of those decisions, *i.e.*, that the loss of an opportunity to compete may constitute irreparable harm. This Court must act to prevent that from happening.

V. THE BALANCING OF HARM FAVORS ISSUANCE OF THE INJUNCTION

In deciding whether to grant a request for preliminary injunction, the Court must balance the harm that the Plaintiffs would suffer without injunctive relief against the harm a preliminary injunction would inflict upon the Defendant and Defendant-Intervenor. In this case, the balance of harm clearly favors Plaintiffs. Defendant is not in dire peril of losing its messaging capabilities—it merely wants to improve them at a purported lower cost. While these are both admirable and reasonable goals, they cannot be attained by circumventing applicable laws and regulations.

It is clear from the AR that the RFQ that prompted the filing of this protest has not been issued in the early stages of Defendant's procurement process, but is instead the final step of a process begun in 2009 without the benefit of competition or, perhaps more importantly, the appropriate internal review and approval process mandated by law and regulation. The AR shows that DOI and Microsoft [redacted]" (AR 1045-1046) since that time to provide one DOI component, the BIA, with a messaging system built around Microsoft's products. If all goes well in this so-called "proof of concept" at the BIA, the next step is to implement the new system agency-wide. This RFQ represents the "next step."

If the Court permits Defendant to make an award under the RFQ, Defendant will embark on the agency-wide implementation of its new system, and the likelihood of Plaintiffs having an opportunity to compete for this major contract will be extinguished.

VI. THE PUBLIC INTEREST FAVORS ISSUANCE OF AN INJUNCTION

The public interest will be served by granting the requested preliminary injunctive relief because it would preserve the Court's ability to fashion relief should the Court determine that Defendant's actions have violated the law. There is an overriding public interest in preserving

the integrity of the procurement system. *Advanced Systems Technology, Inc. v. United States*, 69 Fed. Cl. 474, 486 (2006); *see Cincom Sys., Inc. v United States*, 37 Fed. Cl. 266, 279 (1997), citing *Magellan Corp v. United States.*, 27 Fed. Cl. 448 (1993). At a minimum, agencies are expected to act in accordance with the statutes and regulations that govern them. When an agency acts surreptitiously and in flagrant disregard of those statutes and regulations, as has occurred here, the integrity of the procurement process is severely threatened, and this Court must intervene to prevent any further damage from occurring.

Without an injunction, Defendant will be in a position to implement the new Microsoft platform throughout the agency. Should Plaintiffs prevail on the merits of this protest, this Court would then be faced with the prospect of ordering Defendant to terminate the awarded contract and start from the beginning. The practical, logistical and financial implications of such a decision likely would weigh heavily on the Court's mind, and an injunction preserving the status quo would prevent the Court from being put in that position.

VII. CONCLUSION

The facts in this case reflect the type of collaborations and sole-sourcing that agencies engaged in with their favored contractors before the passage of CICA in 1984. As the foregoing demonstrates, Plaintiffs have met their burden of showing, by clear and convincing evidence, that Defendant has proceeded in a manner that ignored all applicable laws and regulations – at least until Google's May 17 and June 17, 2010 letters (AR Tabs 2 and 5) reminded DOI of its obligations under CICA. After that, DOI prepared its transparent Risk Assessment and [redacted] justifications in an effort to back up the sole-source selection made nine months earlier. The logical gaps and inconsistencies throughout those *post hoc* documents, however, only serve to expose the irrationality of DOI's conclusion that Microsoft's BPOS-Federal is the sole

messaging solution that can satisfy DOI's alleged minimum needs. Moreover, it is clear from these documents and the content of the RFQ that DOI crafted its "minimum needs" based on what a Microsoft product could offer as opposed to using a vendor-neutral process to find the product that best meets the security, operation and cost-saving needs of DOI.

Defendant's actions have prevented Plaintiffs, and perhaps others, of a fair opportunity to compete for this significant contracting opportunity. In so doing, Defendant has also deprived the public of the benefits that Congress intended to flow from CICA and its implementing regulations. As the record makes clear, all that Google asked for from the start was an opportunity to participate in a full and open competition, as it successfully was able to do in the recent GSA procurement, and that is all Plaintiffs are now seeking. This Court has the authority to grant such relief, and the facts to support such a finding. Accordingly, Plaintiffs respectfully

request that the Court deny Defendant-Intervenor's Dismissal Motion and grant Plaintiffs' motion for declaratory and injunctive relief.

Respectfully submitted,

/s/ Timothy Sullivan
Timothy Sullivan
1909 K Street, N.W., 6th Floor
Washington, DC 20006
(202) 585-6930 (tel.)
(202) 508-1028 (fax)

Attorney of Record for Plaintiffs Google, Inc. and Onix Networking Corporation

Of Counsel:

Katherine S. Nucci
Scott F. Lane
Thompson Coburn LLP

Dated: December 3, 2010

CERTIFICATE OF SERVICE

I hereby certify that on this 3rd day of December, 2010, a copy of the foregoing "Plaintiffs' Motion for Judgment on the Administrative Record, Reply to Defendant's and Defendant-Intervenor's Oppositions to Plaintiffs' Motion for Preliminary Injunction, and Response to Defendant-Intervenor's Motion to Dismiss" was filed electronically. I understand that notice of this filing will be sent to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

s/ Timothy Sullivan

PROTECTED INFORMATION TO BE DISCLOSED ONLY IN ACCORDANCE WITH THE U.S. COURT OF FEDERAL CLAIMS PROTECTIVE ORDER

EXHIBIT A

To Plaintiffs' Motion For Judgment On The Administrative Record, Reply To Defendant's And Intervenor's Oppositions To Motion For Preliminary Injunction, And Response To Intervenor's Motion To Dismiss Dated December 3, 2010

[REDACTED IN ITS ENTIRETY]