



THE UNITED STATES COURT OF FEDERAL CLAIMS
BID PROTEST

GOOGLE, INC., et al,)
)
 Plaintiff,)
)
 v.)
)
 UNITED STATES,)
)
 Defendant,)
 and)
)
 SOFTCHOICE CORPORATION)
)
 Intervenor-Defendant.)

Defendant's
Proposed
Redactions

No. 10-743C
(Judge Braden)

**DEFENDANT’S CROSS-MOTION FOR JUDGMENT UPON THE
ADMINISTRATIVE RECORD AND RESPONSE TO PLAINTIFF’S
MOTION FOR JUDGMENT UPON THE ADMINISTRATIVE RECORD**

OF COUNSEL:

TONY WEST
Assistant Attorney General

MICHAEL F. HERTZ
Deputy Assistant General

KIRK T. MANHARDT
Assistant Director

CHARLES M. KERSTEN
Trial Attorney
Commercial Litigation Branch
Civil Division
Department of Justice

CHRISTOPHER L. KRAFCHEK
Trial Attorney
Commercial Litigation Branch
Civil Division
U.S. Department of Justice
1100 L Street, N.W.

SHERYL RAKESTRAW
Attorney Advisor
Department of the Interior

Washington, D.C. 20530



December 17, 2010

Attorneys for Defendant

TABLE OF CONTENTS

STATEMENT OF THE ISSUES. 2

STATEMENT OF THE CASE. 2

 I. Nature Of The Case. 2

 II. Statement Of Facts. 4

ARGUMENT. 15

 I. Standard of Review. 15

 II. Plaintiffs Cannot Establish Prejudice. 20

 III. DOI Did Not Pre-Select Microsoft BPOS – Federal And
 Did Not Create An Implied-In-Fact Partnership With
 Microsoft When Establishing Its Minimum Requirement For A
 Unified Messaging System 20

 A. DOI Neither Engaged In Pre-Selection Of Microsoft
 BPOS-Federal Nor Engaged In Bad Faith. 21

 IV DOI Conducted Thorough Market Research By
 Consulting Industry Reports, Meeting with Vendors, and
 Hiring Independent Third-Party Researchers. 24

 V. DOI Conducted A Rational Risk Assessment. 29

 VI. DOI Rationally Determined That It Required A
 DOI-Only Or Federal-Only Cloud. 32

 VII. DOI Rationally Considered The Requirements Of FISMA. 37

 VIII. DOI Rationally Determined That BPOS-Federal Met
 Its Minimum Requirements. 40

IX. Plaintiffs Are Not Entitled To Permanent Injunctive Relief 44

A. Plaintiffs Have Not Established Success Upon The Merits.. . 45

B. Plaintiffs Have Not Demonstrated That They
Will Be Irreparably Harmed If A Permanent
Injunction Is Denied. 45

C. Plaintiffs Have Not Demonstrated That Their Harm Is Greater
Than The Harm To DOI. 47

D. Plaintiffs Have Not Demonstrated That A Permanent
Injunction Would Serve The Public Interest. 47

CONCLUSION. 49

TABLE OF AUTHORITIES

CASES

<u>Aero Corp. v. United States</u> , 38 Fed. Cl. 237 (1997).....	46
<u>Assessment and Training Solutions Consulting Corp. v. U.S.</u> , 92 Fed.Cl. 722 (2010).....	23
<u>Baird Corp. v. United States</u> , 1 Cl. Ct. 662 (1983).....	43
<u>Bannum, Inc. v. United States</u> , 404 F.3d 1346 (Fed. Cir. 2005).....	16
<u>BioFunction, LLC v. United States</u> , 92 Fed. Cl. 167.....	22
<u>Bowman Transp., Inc. v. Arkansas-Best Freight Sys., Inc.</u> , 419 U.S. 281 (1974).....	15
<u>Califano v. Sanders</u> , 430 U.S. 99 (1977).....	15
<u>Chapman Law Firm Co. v. United States</u> , 67 Fed. Cl. 188 (2005).....	44
<u>Cincom Systems, Inc. v. United States</u> , 37 Fed. Cl. 266 (1997).....	43
<u>Cincom Systems, Inc. v. United States</u> , 37 Fed. Cl. 663 (1997).....	16
<u>Citizens to Preserve Overton Park, Inc. v. Volpe</u> , 401 U.S. 402 (1971).....	15, 16
<u>Cobell v Salazar</u> ,	

573 F.3d 808 (D.C. Cir. 2009).....	passim
<u>CS-360, LLC v. United States,</u> 94 Fed. Cl. 488 (2010).....	18
<u>Data Gen. Corp. v. Johnson,</u> 78 F.3d 1556 (Fed. Cir. 1996).	16
<u>eBay, Inc. v. MercExchange, LLC,</u> 547 U.S. 388 (2006).....	44, 45
<u>Electro-Methods, Inc. v. United States,</u> 7 Cl. Ct. 755, 762 (1985).	15
<u>Emery Worldwide Airlines, Inc. v. United States,</u> 264 F.3d 1071 (Fed. Cir. 2001).	passim
<u>Fort Carson Support Serv., v. United States,</u> 71 Fed. Cl. 571 (2006).....	31
<u>Four Points By Sheraton v. United States,</u> 63 Fed. Cl. 341 (2005).	16
<u>Gadsden v. United States,</u> 111 Ct. C 78 F.Supp. 126 (1948).....	21
<u>Impresa Construzioni Geom. Domenico Garufi v. United States,</u> 238 F.3d at 1332 (citations).....	passim
<u>Government Travel, Inc. v. United States,</u> 61 Fed. Cl. 559 (2004).	43
<u>Info. Tech. & Applications Corp. v. United States,</u> 316 F.3d 1312 (Fed.Cir.2003).	17
<u>JWK Int'l Corp. v. United States,</u> 52 Fed. Cl. 650 (2002), <i>aff'd</i> , 56 Fed. Appx. 474 (Fed. Cir. 2003).	15

<u>Kalvar Corp. v. United States,</u> 543 F.2d at 1302.	21
<u>Krygoski Constr. Co. v. United States,</u> 94 F.3d 1537 (Fed. Cir. 1996).	21
<u>LABAT-Anderson, Inc v. United States,</u> 65 Fed. Cl. 570 (2005).	46
<u>Labatt Food Service, Inc. v. United States,</u> 577 F.3d 1375 (Fed. Cir. 2009).	18
<u>Lermer Germany GmbH v. Lermer Corp.,</u> 94 F.3d 1575 (Fed. Cir. 1996).	43
<u>Linc Gov't Servs., LLC v. United States,</u> 2010 WL 4484021 (Fed. Cl. Oct. 22, 2010).	17
<u>Morris v. United States,</u> 33 Fed. Cl. 733 (1995).	19
<u>Morris v. United States,</u> 39 Fed. Cl. 7 (1997).	19
<u>Ramcor Servs. Group, Inc. v. United States,</u> 185 F.3d 1286 (Fed. Cir. 1999).	15
<u>Redland Genstar, Inc. v. United States,</u> 39 Fed. Cl. 220 (1997).	16
<u>San Diego Beverage & Kup v. United States,</u> 997 F. Supp. 1343 (S.D. Cal. 1998).	44
<u>Saratoga Dev. Corp. v. United States,</u> 21 F.3d 445 (D.C. Cir. 1994).	15
<u>Savantage Financial Services, Inc v. United States,</u>	

595 F.3d 1282 (Fed. Cir. 2010).	passim
<u>Sofamor Danek Group, Inc. v. DePuy-Motech, Inc.</u> , 74 F.3d 1216 (Fed. Cir. 1996).	43
<u>T&M Distributors, Inc. v. United States</u> , 185 F.3d 1279 (Fed. Cir. 1999).	19
<u>Tenacre Foundation v. INS</u> , 78 F.3d 693 (D.C. Cir. 1996).....	44
<u>Torncello v. United States</u> , 681 F.2d 756, 231 Ct. (1982).....	19, 20
<u>USfalcon, Inc. v. United States</u> , 92 Fed. Cl. 436 (2010).	17
<u>Virginia Railway Co. v. Systems Federation No.40, 300</u> , U.S. 515 (1937).....	43
<u>Weeks Marine, Inc. v. United States</u> , 575 F.3d 1352 (Fed. Cir. 2009).	passim
<u>Wisconsin Gas Co. v. FERC</u> , 758 F.2d 669 (D.C. Cir. 1985).....	44
<u>Yakus v. United States</u> , 321 U.S. 414 (1940).....	43

STATUTES

5 U.S.C. §§ 702.....	15
5 U.S.C. § 706 (2)(a).....	14
15 U.S.C. § 278g-3.	36

28 U.S.C. § 1491(b)(1).	14
44 U.S.C. § 3541.....	12
44 U.S.C. § 3541(1).	35
44 U.S.C. § 3544(a).	36

**IN THE UNITED STATES COURT OF FEDERAL CLAIMS
BID PROTEST**

GOOGLE, INC., et al,	*	
	*	
	*	
Plaintiff,	*	No. 10-743C
	*	
v.	*	
	*	Judge Braden
THE UNITED STATES,	*	
	*	
Defendant,	*	
	*	
and	*	
	*	
SOFTCHOICE CORPORATION,	*	
	*	
Intervenor-Defendant.	*	
	*	

**DEFENDANT’S CROSS-MOTION FOR JUDGMENT UPON THE
ADMINISTRATIVE RECORD AND RESPONSE TO PLAINTIFF’S
MOTION FOR JUDGMENT UPON THE ADMINISTRATIVE RECORD**

Pursuant to Rule 52.1 of the Rules of the United States Court of Federal Claims and the Court’s order dated November 30, 2010, defendant, the United States, respectfully requests that the Court enter judgment upon the administrative record in favor of the United States and dismiss the plaintiffs’ complaint. As demonstrated below, plaintiffs’ motion for judgment upon the administrative record should be denied because they are unable to demonstrate success on the merits of their protest, because they cannot demonstrate irreparable harm, and because the harm to the Government and the public interest of granting a permanent injunction outweighs any alleged harm to the plaintiffs.

[REDACTED] [REDACTED]

STATEMENT OF THE ISSUES

1. Whether the United States Department of the Interior (“DOI”) acted arbitrarily and capriciously or without a rational basis when determining its minimum requirements for an email messaging solution.
2. Whether the limited source justification solution issued by DOI in support of the decision to conduct a brand-name procurement was irrational or not in accordance with applicable law.
3. Whether plaintiffs are entitled to a permanent injunction enjoining DOI from awarding a contract for an email message solution.

STATEMENT OF THE CASE

I. Nature Of The Case

This case is a pre-award bid protest filed by Google and Onix (“plaintiffs”), regarding Request for Quotation No. 503786 (“RFQ”) issued by DOI for the acquisition of hosted messaging and collaboration services to support approximately 88,000 users across all DOI bureaus and offices. The RFQ contemplates award of a single, firm-fixed-price Blanket Purchase Agreement to a General Services Administration (“GSA”) Federal Supply Schedule 70 contract holder. Plaintiffs seek to invalidate a standardization decision and limited source justification issued by DOI for a unified messaging system.

Plaintiffs challenge DOI’s decision to limit competition to resellers of the Microsoft Business Productivity Online Suite – Federal (“BPOS-Federal”) solution. Plaintiffs contend, essentially, that DOI’s procurement is a sham designed to support an alleged pre-selection of Microsoft’s product. Plaintiffs further contend that DOI’s market research, risk assessment, and justifications for its standardization decision and limited source procurement were post hoc and

tailored to support an improper pre-selection. Pl. MJAR, pp. 34-41.¹ Plaintiffs also contend that DOI failed to reasonably consider Google's Google Apps – Government messaging service as a viable alternative to Microsoft's product. Next, Google blatantly attempts to put its judgment in place of DOI's and argues that DOI improperly addressed security risks. Pl. MJAR, pp. 42-49. Finally, Google contends that DOI irrationally selected Microsoft BPOS-Federal. Pl. MJAR, pp. 49-53.

Throughout their brief, plaintiffs repeatedly accuse DOI of engaging in bad faith and demonstrating a bias toward Microsoft's product, even going so far as to accuse Government counsel of "selectively" describing the facts contained in the administrative record. Pl. MJAR, p. 2. Plaintiffs' allegations of bad faith underline all of their remaining contentions. *See* Pl. MJAR at 27 (alleging abdication of responsibility of defining minimum needs), 28 (accusing DOI of engaging in "superficial" market research, tailored to support a preordained result, and "cherry-picking" information in "generic third-party reports"), 30 (alleging that DOI pre-selected Microsoft's product in 2009), 33 (accusing DOI of tailoring its market research and risk assessment to conform to Microsoft's products), 34 (accusing William Corrington, the Chief Information Officer tasked with leading the project, of "misleading" DOI's Assistant Secretary).

Plaintiffs' contentions are nothing more than innuendo and speculation because they entirely fail to point to any hard facts or evidence that demonstrate an institutional animus against Google's Google Apps – Government cloud service or a bias toward Microsoft. In fact, plaintiffs' entire pre-selection argument relies almost exclusively upon the absurd notion that DOI's June

¹ "Pl. MJAR" refers to plaintiffs' motion for judgment upon the administrative record.

2009 project plan is tantamount to a sole-source award to Microsoft. We are unaware of any law, statute, or regulation supporting the proposition that an acquisition plan, in this case a project plan, constitutes award of a contract. Moreover, this contention wholly ignores the fact that when the project plan was initially drafted, June 2009, initial market research indicated that “Microsoft was the only one on the short list using a standardized service offering or cloud-based delivery model.” AR176. Continuing on this frivolous theme, plaintiffs also assert that the project plan and DOI’s correspondence with Microsoft during the market research evince that an implied-in-fact contract existed between DOI and Microsoft. Pl. MJAR at 30-33. As we demonstrate below, plaintiffs’ contentions are wholly lacking in merit and are belied by the record and, therefore, this Court should deny plaintiffs’ motion for judgment upon the administrative record, dismiss the complaint, and grant our motion for judgment upon the administrative record.

II. Statement Of Facts

In 2002, DOI implemented an Information Technology Management Reform study to assess the state of DOI’s information technology environment for potential improvement. AR1. As a result of that study, DOI initiated a project to consolidate its email messaging service for its 13 bureaus into a single DOI-wide system. Id. This project, identified as the Enterprise Messaging Service Initiative, was cancelled on September 28, 2006 and DOI provided policy guidance to its 13 bureaus to begin migration of their existing email system to Microsoft Exchange on a bureau-by-bureau basis by the end of fiscal year 2009. Id. On April 9, 2008, progress of the email migration varied by bureau and DOI elected to review the 2006 policy, appointing William Corrington to review DOI’s messaging policy. AR2.

DOI’s email team began assessing the viability of implementing a single email system,

[REDACTED] [REDACTED]

known as unified messaging, for its 13 bureaus in late 2007 by conducting extensive market research. AR175. As one aspect of its research, DOI consulted numerous technological reports created by [REDACTED] a leading Information Technology firm, and also engaged [REDACTED] analysts to discuss the full range of issues associated with creating and using a unified messaging service. Id. Discussions with [REDACTED] occurred at various times during the market research period, beginning on November 29, 2007 and concluding on June 25, 2010. AR175-177. During these discussions, [REDACTED] repeatedly recommended that DOI standardize to a single messaging system and establish a “specific product/version standards, e.g. Microsoft Exchange Service Pack 1.” AR175-176. In support of this recommendation, [REDACTED] specifically recommended that DOI “only consider Microsoft’s single tenant model.” AR176.

On April 15, 2009, representatives from DOI held another discussion with [REDACTED] concerning implementation of a unified messaging system. Id. During that discussion, [REDACTED] recommended, among other things, that GSA “should lead the implementation of a cloud email service that would support Federal civilian agencies (this is known as a “Community Cloud” in the NIST parlance),” that the DOI Chief Information Security Officer (“CISO”) “be engaged in conversations regarding the possible use of a cloud model to ensure that any security concerns were addressed as soon as possible,” and that “DOI conduct a „Proof of Concept“ with a cloud deployment model.” AR176.

On April 27 and May 14, 2009, DOI held discussions with [REDACTED] concerning potential vendors capable of providing “hosted Exchange services.” Id. During these discussions, [REDACTED] commented that “there was a „short list“ of vendors that could provide hosted Exchange services,” that “Microsoft was the only one on the short list using a standardized service offering or cloud-

[REDACTED] [REDACTED]

based delivery model,” and that other vendors such as “[REDACTED]” were all „traditional“ outsourcers.” *Id.* On May 28, 2009, DOI and [REDACTED] discussed models for external provisioning of services, i.e. traditional outsourcing versus cloud model and within the cloud mode, single-tenant versus multi-tenant deployment. AR177. [REDACTED] commented that “multi-tenant cloud model may provide better economies of scale” and “predicted that prices for cloud services will continue to go down and recommended that any contract for external services include guarantees that future price reductions will be passed on to DOI.” *Id.*

The record demonstrates that DOI reviewed numerous research reports and presentations from [REDACTED] [REDACTED]. *See* AR175-185. DOI officials also met with potential vendors, such as Microsoft and Google, to provide them with the opportunity to explain how they would satisfy DOI’s minimum requirements. AR184.

DOI representatives began a discussion with Google, via conversations and electronic messages, concerning DOI’s requirements for an email messaging system shortly before June 17, 2009. AR59, 66. On July 30, 2009, David Standish, of Google, sent DOI’s Chief Information Officer (“CIO”) a report that calculated costs to run Google Apps rather than a traditional email approach and an article about a group who migrated from Lotus, an email message provider, to Google Apps. AR66. DOI and Google communicated via electronic mail through June - December, 2009; February, 2010; and April - August, 2010. *See* AR60-117.

On May 6, 2010, David Standish followed up a conversation with DOI’s Assistant Director concerning the email messaging requirement and noted that there were three “next steps”

[REDACTED] [REDACTED]

to take in the continuing dialogue between DOI and Google. AR100. Of particular note, Mr. Standish indicated DOI informed Google that:

DOI Contracting confirmed on Tuesday 5/4/10 that there is no active procurement for Messaging. **A messaging RFP which is product specific is being readied and we're following up to learn more detail about specific market research and product selection process.** Given that there is not an active procurement we hope more detailed discussion can be had directly with the appropriate folks.

Id. (emphasis added).

DOI representatives met with Google on two occasions, February 18, 2010 and June 9, 2010. AR184. At the February 18, 2010 meeting, Google stated that “no single tenant or „private cloud“ would be available for cloud-based email services.” *Id.* At the June 9, 2010 meeting, when asked if it could provide dedicated infrastructure, Google indicated that it was “incapable of supporting a dedicated solution and proceeded to argue about the merits of a dedicated infrastructure.” Id. Google also stated that “elements of the community cloud offering would be available in the third quarter of 2010, but declined to provide any specific dates on when the solution would be ready, or which elements would be available.” AR185.

On June 14, 2010, DOI issued Modification No. 3 to Contract No. GS35F4072D / NBCF09382 to purchase Microsoft Business Online Suite - Federal (“BPOS-Federal”) from Dell Marketing, LP (“Dell”) for 5000 email users in the Bureau of Indian Affairs. AR855-856. This “proof of concept” modification of Dell’s contract constituted an initial step in DOI’s plan to migrate to a single messaging service. *See* AR1002a-1002f.

On June 24, 2010, Google notified DOI that part of its Government-only cloud, which includes Federal, State, and Local agencies, was completed earlier than expected. AR116.

Specifically, Google indicated that “[t]he elements of the government-only cloud that are now available are messaging and calendaring, and additional collaboration elements will be added later this year. Based on our understanding from your letter dated May 27 and our meeting on June 9, those additional collaboration capabilities are not in the scope of the planned messaging solicitation.” *Id.*

On June 28, 2010, Mr. Corrington completed a risk assessment for DOI’s unified messaging service. AR158-168. In so doing, Mr. Corrington adopted the CSA’s risk assessment process and he noted that the goal of the risk assessment was “*not* to determine the technical superiority of one model over the other. Rather, it [was] to evaluate the tolerance of a given organization for moving a given asset to a cloud computing model.” AR158.² DOI’s risk assessment explained the background of DOI’s messaging service, adopted CSA’s suggested five-step analysis, considered cloud security and risks as defined in the current market, and reviewed the various types of cloud deployment models. AR158-163. Research revealed that, as defined by the NIST, the following four types of cloud models are currently available:

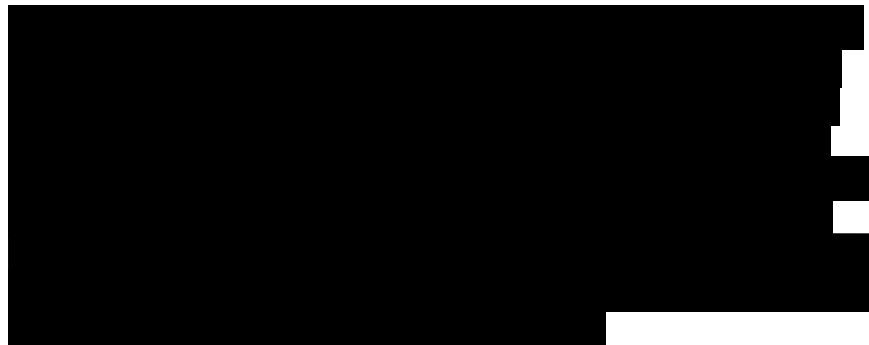
- Private cloud: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared 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

² The CSA is a non-profit organization whose mission is to “promote the use of best practices for providing security assurance within Cloud Computing.” AR158-68; *see also* AR 549-51

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).

AR162. DOI's research indicated that the key difference between the types of clouds is the number of customers that are served by a given cloud deployment. *Id.* A private cloud deployment serves a single organization, a public cloud deployment is not limited in the organizations that it may serve, and a community cloud sits in the middle, serving two or more organizations that have common interests and requirements. *Id.* The scope of users served by a given cloud deployment is a function of the level of "multi-tenancy" that the deployment utilizes. *Id.* Multi-tenancy is a term that relates to the level of sharing of infrastructure, services, data, metadata and applications across different consumers of a cloud service. Cloud providers with multiple tenants may achieve economies of scale by serving multiple customers with the same infrastructure. DOI's risk assessment specifically addressed the type of cloud Google provides as follows:



AR162-163.

Next, DOI examined the security risks in migrating to a cloud deployment model. AR163-

[REDACTED]

164. DOI also determined that it possesses a low tolerance for risk due, in part, to *Cobell v Salazar*, 573 F.3d 808 (D.C. Cir. 2009), which was filed because of concerns regarding DOI's information security and its responsibility to manage sensitive information such as Indian trust data and law enforcement data. AR164165. The risk assessment contains a chart stating "[REDACTED]" AR166. The point of the chart, and its relevance to DOI's risk assessment, is explained on the preceding page as:



AR165, *see also* AR654-663.

After fully considering the different types of clouds, DOI moved away from labels such as "public" and "private" and focused upon the specific attributes that comprise a cloud model that would be acceptable to DOI based upon its minimum requirements and risk tolerance level.

AR167. DOI specifically evaluated vendor offerings against its specific requirements and determined that the following mix of attributes represented an acceptable tradeoff of the benefits,

risks and organizational maturity as they relate to the movement of enterprise email and collaboration services to a cloud deployment model:

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

AR167. Consequently, an external private cloud model or an external private Federal community

[REDACTED] [REDACTED]

cloud was recommended to best meet DOI's security and risk tolerance minimum requirements. AR167.

On June 29, 2010, [REDACTED] a firm that provides acquisition support and market research, completed its analysis of 13 firms that provide messaging and collaboration systems, including Google, to determine if they met DOI's requirements. AR169-172, 1152, 1173. [REDACTED] solicited product and Federal security compliance information from vendors, trusted third party research, and other Federal Government informational resources. AR170. [REDACTED] concluded that only Microsoft's BPOS-Federal Suite met all of DOI's technical and security requirements. AR171. To complete its research for DOI, [REDACTED] assigned a project team with over 50 years of experience that was led by former Strategic Sourcing experts from [REDACTED] AR173-174

On July 15, 2010, the Assistant Secretary for Policy, Management and Budget approved a standardization decision establishing Microsoft's BPOS-Federal as the DOI-wide standard for messaging and collaboration services. AR748-756. DOI relied upon the foregoing NIST definitions of cloud models, and reports from both [REDACTED] and CSA in its consideration of risks associated with each of these models. AR755. In so doing, DOI adopted CSA's risk-assessment approach for the various cloud deployment models. *Id.* DOI's standardization decision reflects that the Assistant Secretary considered DOI's historical challenges in implementing an email messaging system, multiple approaches to remedy the problem, an alternative assessment, and DOI's risk tolerance and concerns. AR751-754.

On July 22, 2010, Google publically announced the availability of a Government-only version of its Google Apps Service, a direct competitor with Microsoft BPOS-Federal. AR783.

As explained by Google, this service provides a “multi-tenant” or “community cloud” as defined by NIST and it shares computing infrastructure amongst multiple customers. *Id.* The announcement also indicated that Google defines “Government-only” as “Federal, State, and Local Government” within the community cloud. AR783-784. Google also announced that its Government-only version received certification pursuant to the Federal Information Security Management Act (“FISMA”) of 2002, 44 U.S.C. § 3541. *Id.*³

On August 20, 2010, in response to Google’s announcement, DOI conducted supplemental market research to determine the impact upon DOI’s July 15, 2010 standardization decision. AR783-785. DOI determined that Google’s multi-tenant cloud is unacceptable from a risk tolerance perspective. AR784. Specifically, DOI determined that Google’s proposed government-only, multi-tenant approach “remained an issue” because it includes “state and local government . . . entities that do not have the same security issues [as] DOI.” *Id.* DOI also considered the impact of the FISMA certification for Google Apps and determined that, by itself, this fact did not indicate that Google Apps satisfies DOI’s enhanced security requirements. AR784-785. In reaching this conclusion, DOI relied upon the research efforts of [REDACTED] and the testimony of the Director of Information Technology Laboratory at NIST before the United

³ On December 16, 2010, counsel for the Government learned that, notwithstanding Google’s representations to the public at large, its counsel, the GAO, and this Court, it appears that Google’s Google Apps for Government does not have FISMA certification. See Attachments 1-5 to this motion. We immediately contacted counsel for Google, shared this information and advised counsel that we would bring this to the Court’s attention. According to the GSA, Google’s Google Apps Premier received FISMA certification on July 21, 2010. However, Google intends to offer Google Apps for Government as a more restrictive version of its product and, Google is currently in the process of finishing its application for FISMA certification for its Google Apps for Government. See Attachment 3. To be clear, in the view of GSA, the agency that certified Google’s Google Apps Premier, Google does not have FISMA certification for

States House of Representatives Committee on Oversight and Government Reform on “Cloud Computing: Benefits of Moving Federal IT into the Cloud. AR785.

On August 19, 2010, DOI initially approved a Limited Sources Justification (“justification”), pursuant to FAR § 8.405-6(a)(2), for the brand-name procurement of Microsoft BPOS-Federal from authorized resellers on the GSA FSS. AR844. As noted in the justification, Microsoft BPOS-Federal is a messaging and collaboration solution specifically designed to meet the Federal Government's security requirements. *Id.* By acquiring Microsoft BPOS-Federal, DOI will receive two features that are critical to transition from a disparate and disjointed email message system to one that is consolidated and secure: 1) A unified email system; and 2) enhanced security. *Id.*

On August 30, 2010, DOI issued the RFQ on GSA eBuy to solicit quotes from authorized GSA FSS vendors. AR786. The RFQ contemplated award of a blanket purchase agreement to the successful offeror. *Id.* On October 29, 2010, plaintiffs filed a complaint, a motion for a temporary restraining order, and a motion for a preliminary injunction with the Court seeking to enjoin award of a contract under the RFQ. The RFQ’s Statement of Work defines DOI requirements as follows:

DOI’s organizational and regulatory requirements were analyzed through a risk assessment following the CSA approach. The conclusion of this risk assessment is a determination that the following attributes of a cloud computing deployment meet DOI’s current requirements for the implementation of an enterprise e-mail and collaboration system:

- Compliance with security requirements defined by the Federal Information Security Management Act (FISMA) along with

- enhanced DOI- specific security requirements;
- Dedicated data storage infrastructure (both physically and logically) to DOI or to DOI and other Federal government customers only;
 - Dedicated computing infrastructure (both physically and logically) to DOI or to DOI and other Federal government customers only;
 - Implementation of at least two data centers located within the continental United States; and
 - Enterprise e- mail and collaboration services provided by an external vendor as a standardized service offering.

Using the NIST terminology, these attributes represent an “external private cloud” deployment model.

AR800.

ARGUMENT

I. Standard of Review

The Court possesses jurisdiction to entertain this action pursuant to the bid protest jurisdiction of the Tucker Act, 28 U.S.C. § 1491(b)(1). Section 1491(b)(4) requires the Court to “review the agency’s decision pursuant to the standards set forth in section 706 of Title 5,” the Administrative Procedure Act (“APA”). This Court reviews bid protest actions pursuant to the standards set forth in the APA. *Impresa Construzioni Geom. Domenico Garufi v. United States*, 238 F.3d 1324, 1332 (Fed. Cir. 2001). In particular, the Court must determine whether the agency’s actions were “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.” 5 U.S.C. § 706. Therefore, a procurement decision may be set aside “if either: (1) the procurement official’s decision lacked a rational basis; or (2) the procurement procedure involved a violation of regulation or procedure.” *Garufi*, 238 F.3d at 1332 (citations omitted). It is well-settled that the APA does not permit the Court to undertake a de novo review of agency action. Rather, it limits the Court to a consideration of whether the action was

“arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law,” based solely upon the record before the agency. 5 U.S.C. §§ 702, 706(2)(A).

In evaluating whether an agency official’s actions were rational, the “„disappointed bidder bears a „heavy burden“ of showing that the award decision „had no rational basis.”” *Garufi*, 238 F.3d at 1333 (quoting *Saratoga Dev. Corp. v. United States*, 21 F.3d 445, 456 (D.C. Cir. 1994), see also *Citizens to Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 402, 416 (1971), overruled on other grounds, *Califano v. Sanders*, 430 U.S. 99 (1977); *Ramcor Servs. Group, Inc. v. United States*, 185 F.3d 1286, 1290 (Fed. Cir. 1999)). Courts have recognized that contracting officials may properly exercise wide discretion in applying procurement regulations. See *id.* at 1332; *Electro-Methods, Inc. v. United States*, 7 Cl. Ct. 755, 762 (1985). The arbitrary and capricious standard, by definition, acknowledges a “zone of acceptable results in a particular case and requires only that the final decision reached by an agency be the result of a process which consider[s] the relevant factors and is within the bounds of reasoned decision making.” *JWK Int’l Corp. v. United States*, 52 Fed. Cl. 650, 654 n. 8 (2002), *aff’d*, 56 Fed. Appx. 474 (Fed. Cir. 2003) (quotation omitted). In this regard, the Court cannot substitute its judgment for that of the agency, even if reasonable minds could reach differing conclusions. *Bowman Transp., Inc. v. Arkansas-Best Freight Sys., Inc.*, 419 U.S. 281, 285-86 (1974). Therefore, as long as a rational basis is articulated and relevant factors are considered, the agency’s action must be sustained. *Id.*

When a protestor asserts a violation of regulation or procedure, “the disappointed bidder must show „a clear and prejudicial violation of applicable statutes or regulations.”” *Garufi*, 238 F.3d at 1333 (quoting *Kentron Haw., Ltd. v. Warner*, 480 F.2d 1166, 1169 (D.C. Cir. 1973)); see also *Data Gen. Corp. v. Johnson*, 78 F.3d 1556, 1562 (Fed. Cir. 1996) (“[T]o prevail in a protest,

[REDACTED] [REDACTED]

the protester must show not only a significant error in the procurement process, but also that the error prejudiced it.” “[T]o establish prejudice, a protestor must show that, had it not been for the alleged error in the procurement process, there was a reasonable likelihood that the protestor would have been awarded the contract.” *Data Gen. Corp.*, 78 F.3d at 1563; *see also Four Points By Sheraton v. United States*, 63 Fed. Cl. 341 (2005). Additionally, if the protestor can show any errors in the procurement process, the protestor must then show that it was “significantly prejudiced” by those errors. *Bannum, Inc. v. United States*, 404 F.3d 1346, 1357 (Fed. Cir. 2005). To establish significant prejudice, the protestor must show that “there was a „substantial chance“ it would have received the contract award but for the [agency] errors in the bid process.” *Id.* at 1358 (citations omitted).

In reviewing the agency’s procurement decisions, the Court should recognize that the decision is entitled to a “presumption of regularity,” *Citizens to Preserve Overton Park*, 401 U.S. at 415 (citations omitted), and that the Court should not substitute its judgment for that of the agency. *Redland Genstar, Inc. v. United States*, 39 Fed. Cl. 220 (1997); *Cincom Systems, Inc. v. United States*, 37 Fed. Cl. 663, 672 (1997) Thus, the protester “bears a heavy burden,” and the procurement officer is “entitled to exercise discretion upon a broad range of issues confronting [her].” *Impressa*, 238 F.3d at 1332 (citations and quotes omitted).

Deference to an agency is particularly great when the protester challenges the agency’s determination of its own requirements. “[C]ompetitors do not dictate an agency’s minimum needs, the agency does.” *Savantage Financial Services, Inc v. United States*, 595 F.3d 1282, 1286 (Fed. Cir. 2010). Moreover, “determining an agency’s minimum needs is a matter within the broad discretion of agency officials . . . and is not for [the] court to second guess.” *Id.*

(internal quotations omitted). A court will uphold the agency's decision unless the protester can show that it lacks a rational basis - even if that determination leads to a sole-source procurement. *Emery Worldwide Airlines, Inc. v. United States*, 264 F.3d 1071, 1086 (Fed. Cir. 2001). To pass rational-basis review, the agency need only "articulate a rational connection between the facts found and the choices made." *Id.* (citing *Burlington Truck Lines v. United States*, 371 U.S. 156, 168 (1962)).

II. Plaintiffs Cannot Establish Prejudice

Plaintiffs' entire case hinges on the question of whether DOI properly exercised its discretion in determining its own security needs. Though they have raised other issues, plaintiffs will be unable to demonstrate prejudice unless they can prove that DOI acted irrationally.

"In order to have standing to sue as an 'interested party' under § 1491(b)(1), a disappointed offeror must show that it suffered competitive injury or 'prejudice' as a result of the challenged agency decisions." *Linc Gov't Servs., LLC v. United States*, 2010 WL 4484021 (Fed. Cl. Oct. 22, 2010) (citing *Info. Tech. & Applications Corp. v. United States*, 316 F.3d 1312, 1319 (Fed.Cir.2003)). The Court of Federal Claims considers the question of prejudice twice in a case: first at the outset to determine standing, and then after the merits to assess whether relief is appropriate. *See, e.g., USfalcon, Inc. v. United States*, 92 Fed. Cl. 436, 450 (2010). A party may be able to show prejudice for the purposes of standing (because the court assumes all of its allegations are assumed to be true), but fail to show prejudice on the merits because the court did not find one or more of its allegations to be true. *Id.*

The courts have evinced some confusion over the proper standard for determining prejudice. The traditional rule is that "[a] party has been prejudiced when it can show that but for

the error, it would have had a substantial chance of securing the contract.” *Labatt Food Service, Inc. v. United States*, 577 F.3d 1375, 1378 (Fed. Cir. 2009). However, the Federal Circuit recently indicated that, for at least some pre-award protests, the appropriate measure is “a non-trivial competitive injury which can be redressed by judicial relief.” *Weeks Marine, Inc. v. United States*, 575 F.3d 1352 (Fed. Cir. 2009); *see also CS-360, LLC v. United States*, 94 Fed. Cl. 488, 495 n.6. (2010) (interpreting *Weeks Marine* to limit its standard to a particular subset of pre-award protests).

Regardless of the standard employed, however, plaintiffs will be unable to demonstrate prejudice on the merits unless this Court finds that DOI irrationally determined its security needs. If DOI properly exercised its discretion in requiring a DOI-only or Federal-only cloud, then no relief fashioned by the Court will aid the plaintiffs. This is because Google has categorically refused meet DOI’s stated requirements by providing an isolated server or to limit its community cloud to Federal civilian agencies. Accordingly, even if the Court found some other defect in the procurement and remanded the matter back to the agency, plaintiffs would have no chance of winning, or even being eligible to compete in the follow-on procurement because they refuse to offer a product that meets DOI’s needs. Consequently, plaintiffs would have *no* chance of securing the contract, let alone a substantial one. *Cf. Labatt Food Service*, 577 F.3d at 1378.

Moreover, even if the Court employs the lower *Weeks Marine* standard, the result is the same because if the Court concludes that DOI properly determined that minimum requirements, in this case restricting access to its email messaging service to either DOI-only or Federal civilian agencies only, then no other alleged error in the procurement will give rise to a non-trivial competitive injury. So long as plaintiffs refuse to meet DOI’s stated needs, they are not in

competition for the contract and cannot suffer a competitive injury.

III. DOI Did Not Pre-Select Microsoft BPOS – Federal And Did Not Create An Implied-In-Fact Partnership With Microsoft When Establishing Its Minimum Requirement For A Unified Messaging System

As we explain above, there can be little debate that plaintiffs’ contentions concerning DOI’s market research, risk assessment, misleading of the Assistant Secretary before she signed the standardization memorandum, and overall tone throughout their brief are allegations of bad faith and pre-text. First, in light of the fact that plaintiffs have wholly failed to cite any evidence supporting its various contentions, this Court should categorically reject these arguments because DOI officials are entitled to the presumption that they acted in good faith in carrying out their responsibilities. *See T&M Distributors, Inc. v. United States*, 185 F.3d 1279, 1285 (Fed. Cir. 1999) (“[G]overnment officials are presumed to act in good faith, and „it requires well-nigh irrefragable proof“ to induce a court to abandon the presumption of good faith.”) (citing *Kalvar Corp. v. United States*, 211 Ct. Cl. 192, 543 F.2d 1298, 1301-02 (1976), *cert. denied*, 434 U.S. 830 (1977)). To overcome the presumption of good faith, a plaintiff must “present „clear and strong proof of specific acts of bad faith,“ demonstrating that a Government official acted with malice or a specific intent to injure the plaintiff.” *Morris v. United States*, 39 Fed. Cl. 7, 15 (1997) (quoting *Morris v. United States*, 33 Fed. Cl. 733, 752 (1995) (citing *Torncello v. United States*, 681 F.2d 756, 771, 231 Ct. Cl. 20 (1982))). Certainly, plaintiffs have made no such showing.

Second, rather than providing support for plaintiffs’ allegations, the administrative record wholly belies each of their points. For instance, to support the contention that there is a partnership between Microsoft and DOI, plaintiffs’ cite the September, 2009 version of the

project plan, at AR1051 and a January 8, 2010 email from Microsoft to DOI, at AR1106. Pl. MJAR, pp. 31, n. 13. First, nothing at either of these pages in the administrative record suggests that DOI and Microsoft intended to create a partnership to make the project plan become a reality as plaintiffs contend. Second, plaintiffs offer no explanation how these two documents create or evince a partnership. Third, there is nothing in January 8, 2010 email that indicates the communication applies to the project plan. *See* AR1051. Indeed, when read in context of the preceding emails, the referenced comments apply to a messaging technical workshop attended by Microsoft and Google on January 7, 2010. AR1052-1055.

A. DOI Neither Engaged In Pre-Selection Of Microsoft BPOS-Federal Nor Engaged In Bad Faith

Plaintiffs“ allege that DOI engaged in pre-selection, intentionally misled Assistant Secretary Suh, created *post hoc* rationalizations and market research for the singular purpose of serving as “back-up” documents. Pl. MJAR, pp. 27-48. These contentions are unquestionably allegations of bad faith. Notwithstanding the severity of these allegations, plaintiffs offer no “hard facts” or “evidence” supporting their claims. Rather, “there is myriad case law in this court and the Federal Circuit to establish that „it requires „well-nigh irrefragable proof“ to induce the court to abandon the presumption of good faith dealing traditionally afforded to the government.” *Torncello*, 681 F.2d at 770. To meet this burden, plaintiffs must show evidence of “some specific intent to injure the plaintiff.” *Id.* The type of government actions that have been deemed to rise to the level of this specific intent include those “motivated alone by malice;” *Gadsden v. United States*, 111 Ct. Cl. 487, 78 F.Supp. 126, 127 (1948); “actuated by animus toward the plaintiff;” *Kalvar Corp.*, 543 F.2d at 1302 and those the government enters “with no intention of

fulfilling its promises;” *Krygoski Constr. Co. v. United States*, 94 F.3d 1537, 1545 (Fed. Cir. 1996).

In this case, none of the facts relied upon by plaintiffs: (1) drafting and following a project plan that evinces an intent to award a contract to the only offeror capable of meeting the particular’s specific requirements; (2) working closely with industry (in this case both Microsoft and Google) while conducting market research; or (3) failing to issue a justification and approval as allegedly required by FAR §§ 6.3, 6.303-2, or 6.304 prior to issuing an unsigned project plan support an allegation of bad faith. As noted above, the project plan does not constitute an award of a contract. Moreover, the fact that the project plan was continuously updated as DOI’s market research evolved makes clear that it was nothing more than how the agency expected the procurement to turn out. AR1580. It was not a final decision on the agency’s procurement.

In making its various arguments, plaintiffs ignore the fact that DOI also worked closely with Google from as early as June 17, 2009 and continued to do so until February 18, 2010 when Google indicated that it would not provide an isolated physical server or a DOI-only private external cloud or a Federal-only community cloud. *See* AR59, 66, 150-151, 184. Remarkably, notwithstanding Google’s statement that it could not and would not meet DOI’s requirements at the February 18, 2010, DOI afforded Google another opportunity to participate in the implementation of a unified messaging service on June 9, 2010. Thus, according to plaintiffs’ logic, if the relationship between DOI and Microsoft is properly characterized as a “partnership,” then the relationship between Google and DOI must also be defined as a partnership. Of course, the assertion that an implied-in-contract is developed, or that a partnership arises when the

[REDACTED] [REDACTED]

Federal Government works closely with industry, is specious on its face.⁴

Even if we assume that the pre-selection claims are not allegations of bad faith, there is no evidence in the record that suggests that DOI determined “once Microsoft, forever Microsoft” when it drafted its project plan as plaintiffs allege. Pl. MJAR, p.32. In fact, DOI repeatedly met with Google to discuss its proposed clouds to ensure that all possible solutions were considered. Plaintiffs would have this Court find that DOI simply went through the motions when meeting with Google and when reviewing reports by [REDACTED] [REDACTED]. However, plaintiffs have offered no plausible explanation why DOI officials continued to review the aforementioned reports. The simple answer is that plaintiffs cannot avoid the inescapable fact that DOI’s follow-on market research demonstrates that DOI did not make a final decision on its unified message service procurement until after it considered all viable alternatives. Again, as reflected by DOI’s market research in June and September, 2009, at the time the project plan was drafted, Microsoft BPOS-Federal was the only unified messaging solution capable of meeting DOI’s requirements. AR175-177. Moreover, the market research that occurred after September 2009, including representations from Google itself, confirmed that no other unified message provider is capable of meeting DOI’s minimum requirements that call for a physically and logically isolated server. AR Tab 14.

Finally, the concept of “once Microsoft forever Microsoft” suggested by Plaintiff is belied by the Agency’s procurement approach as noted in the Limited Source Justification and the

⁴ To determine that an implied-in-fact contract existed, there must be: (1) mutuality of intent to contract, (2) consideration, (3) lack of ambiguity in offer and acceptance, and (4) authority to bind the Government. Nothing in the record suggests that these elements were met here. *BioFunction, LLC v. United States*, 92 Fed. Cl. 167. (citations omitted).

contracting vehicle itself. The Limited Source Justification includes the following statement: “All services required under this solicitation are available through numerous resellers. With the progression and development of technology, DOI will continue to perform market research of the industry solutions that are available.” AR848. *See also* AR 849 (stating “... because of the rapidly changing nature of information technology , DOI will periodically evaluate the marketplace for externally hosted email and collaboration services to identify alternative sources for these services.”). Moreover to further ensure that the Department has flexibility to respond to technological advances, the RFQ indicates that the Department will enter into a Blanket Purchase Agreement (“BPA”). AR786. This vehicle requires annual review, and in connection with annual reviews, requires that the Contracting Officer “[m]aintain awareness of changes in market conditions, sources of supply, and other pertinent factors that *may warrant making new arrangements with different suppliers or modifying existing arrangements.*” FAR 13.303-6(b)(2) (emphasis added); *see also* AR 818 (requiring annual contractor self-assessment). Accordingly, this Court should find that DOI did not pre-select the Microsoft BPOS-Federal solution and reject plaintiffs’ various claims to the contrary.

IV. DOI Conducted Thorough Market Research By Consulting Industry Reports, Meeting with Vendors, and Hiring Independent Third-Party Researchers

Contracting officers have broad discretion in conducting market research. The FAR instructs them to perform market research “appropriate to the circumstances” of the acquisition. FAR § 10.001(a)(2). The regulation goes on to note that “[t]he extent of market research will vary, depending on such factors as urgency, estimated dollar value, complexity, and past experience.” FAR § 10.002(b)(1). The Court of Federal Claims has accorded due deference to

[REDACTED] [REDACTED]

the contracting officer's expertise in executing this broad mandate. *See Assessment and Training Solutions Consulting Corp. v. U.S.*, 92 Fed.Cl. 722, 731 (2010).

Here, DOI conducted comprehensive market research to determine its needs and the offerings in the commercial marketplace. As part of its research, DOI relied upon information provided by [REDACTED] See AR175-185. The AR contains nearly 600 pages of industry reports discussing various topics in the field of cloud computing and enterprise messaging. AR186-747. DOI drafted its own market research analysis, which summarized the major points of these articles and discussed how they influenced the agency's thinking. AR177-184. This report includes synopses of eight telephone conversations between DOI and [REDACTED] concerning the agency's plans for a unified messaging system. AR175-177. Furthermore, DOI also reasonably relied upon the market research of [REDACTED] AR170-172.

In addition to reviewing numerous industry reports, DOI also spoke directly with vendors to learn about their capabilities. In particular, DOI met with Google on four separate occasions. AR150-151. These exchanges covered a variety of topics but focused upon whether Google could meet DOI's stated requirements. During these discussions, Google unequivocally told the agency that it could not or would not meet its stated requirements. For instance, in a February 18, 2010 meeting, Google representatives indicated that Google would not offer a single tenant solution. AR150. Google repeated this refrain in a meeting on June 9, 2010, where it also tried to convince DOI that its government-wide cloud would meet its needs. AR151.

DOI and Google also corresponded extensively via letters and emails. See AR3-6, 47-117, 152, 1007-1038. In a June 17, 2010 letter, Google said that it "intends to offer messaging

services hosted in a Government-only cloud” and complained that restricting the solicitation to a private cloud “would arbitrarily exclude Google from the competition.” AR50. Similarly, in its June 24, 2010 email, Google argued that “the DOI’s security requirements can be stated . . . without requiring a particular infrastructure or computing delivery model,” such as a dedicated cloud. AR115. Google has never indicated that it could meet DOI’s stated requirements. Instead, Google decried DOI’s stated minimum requirements as unnecessary and tried to convince the agency that its own government-wide cloud was sufficient to meet the agency’s minimum needs.

Despite this well-documented process, plaintiffs have leveled a number of challenges to DOI’s market research. None of these challenges comes close to demonstrating that DOI abused its discretion in conducting market research. *See* FAR § 10.001(a)(2).

Plaintiffs attack the market research conducted by ██████ by claiming that “DOI merely contracted with ██████ (in October 2009) to create a paper trail to support the decision already made by DOI to procure the Microsoft solution.” Pl. MJAR 34. To support this accusation, plaintiffs cite a line from ██████’s Statement of Work ██████”] which states, “The objective of this task order is to provide [DOI] with acquisition support services that shall provide for the successful creation of an acquisition package to foster the successful competition and award of a DOI-wide hosted Microsoft Exchange infrastructure.” This argument fails for two reasons.

First, plaintiffs’ reliance on the ██████ is wholly misplaced. Plaintiffs point to this document as the smoking gun which shows that DOI hired ██████ to ensure that Microsoft was selected instead of another competitor. Yet even a cursory examination of the ██████

[REDACTED] [REDACTED]

reveals that this is not case. Rather, DOI hired [REDACTED] to assist the Department in acquiring a unified messaging system, which DOI assumed (at the time) would be a Microsoft solution. Under this contract, [REDACTED] had facilitated that acquisition in a variety of ways, none of them as sinister as plaintiffs imply: formulating acquisition strategy, developing the SOW, drafting the RFI, supporting the solicitation, and conducting market research. AR1173. The document provides no evidence whatsoever to support plaintiffs' claim that [REDACTED] was charged with creating a paper trail.⁵

Second, plaintiffs have failed to identify any flaw in [REDACTED]'s research or analysis. Plaintiff alleges that [REDACTED] should have looked at Google Apps for Government before determining that the company could not meet DOI's private-cloud requirement. Pl. MJAR 34. Indeed, the record establishes that Google Apps for Government was not even operational until almost a month after [REDACTED] submitted its market research report. *Compare* AR169 with AR108. More importantly, even if [REDACTED] had considered Google Apps for Government, its conclusion would not have changed: it is undisputed that Google Apps for Government is *not* a private cloud, but rather a multi-tenant cloud that hosts Federal, state, and local entities. Moreover, Google's refusal to provide a physically isolated server violates DOI's requirements for a dedicated server and violates the requirement that any and all information stored in the cloud be located in a data center within the continental United States. AR167, 755, 800. Thus [REDACTED]

⁵ Moreover, even if DOI hired [REDACTED] to justify its decision to award to Microsoft, [REDACTED] analysis could still be valid. The Federal Circuit has upheld the rationality of such market research in similar circumstances. *See Emery Worldwide Airlines, Inc. v. U.S.*, 264 F.3d 1071, 1087 (Fed. Cir. 2001) ("While the trial court determined that the USPS had the objective of awarding FedEx the contract and hired PwC to justify that decision, PwC's Analysis and the USPS's decision were nonetheless rational.").

[REDACTED] [REDACTED]

would have found that Google failed to meet DOI's private-cloud requirement even if [REDACTED] had given greater consideration to Google Apps for Government.

Plaintiffs' only other complaint with [REDACTED]'s market research is that [REDACTED] found that BPOS-Federal satisfied DOI's security needs despite not being FISMA-certified. Pl. MJAR 34-35, 49. This claim is baseless. DOI never mentioned pre-FISMA certification as one of its requirements. *See* AR170-171. Rather, its requirements merely note DOI's obligation to meet FISMA and other security requirements. The agency's Limited Source Justification explains that DOI merely wanted to establish the vendor's "[a]bility to comply with security requirements defined by FISMA." AR847 (emphasis added). Indeed, as is discussed below, a dedicated cloud would never be FISMA-certified prior to its procurement and implementation.⁶ [REDACTED] simply determined that Microsoft was capable of meeting FISMA standards – a finding that has been borne out by subsequent events.⁷

Plaintiffs also challenge DOI's own market research. Plaintiffs boldly assert that "DOI's alleged „extensive“ market research avoided any analysis of Google's government cloud." Pl. MJAR 36. Plaintiffs also complain that the industry reports in the AR "do not compare the security of Google's government cloud model against Microsoft's" and "do not address any differences between a cloud that shares infrastructure with state and local governments and one that is available only to Federal agencies." Pl. MJAR 35-36. These claims fail for two reasons.

First, plaintiffs ignore the numerous meetings and conversations it had with DOI

⁶ *See infra* Section VI.

⁷ The United State Department of Agriculture recently granted FISMA certification and an to Microsoft's cloud. See <http://www.usda.gov/wps/portal/usda>.

concerning its government-wide cloud. *See* AR150-152. Moreover, the record shows that not only did DOI consider materials supplied by Google (AR at 108), but also materials supplied by Google on its own website as well as other sources. AR at 783-785. Thus, contrary to plaintiffs' assertions, DOI's market research fully considered Google Apps and Google Apps for Government. An agency does not fail to consider relevant data simply because it obtains that information in-person instead of from a report. *See* FAR §§ 10.002(b)(2)(i), 10.002(b)(2)(viii). An agency may also review generally available product literature, including that available on-line as part of its market research. *See* FAR § 10.002(b)(2)vii.

Second, plaintiffs conveniently overlook the fact that its government-wide cloud had *not even launched* by the time DOI finished its market research. *Compare* AR175 *with* AR 108. Moreover, there is no evidence in the record that another company offered a government-wide cloud at the time when DOI was conducting its market research. Thus one should not be surprised that DOI's industry reports do not provide an in-depth analysis of the pros and cons of government-wide clouds, since they did not even exist until after DOI finished their market research.

V. DOI Conducted A Rational Risk Assessment

To the extent that plaintiffs argue that DOI's risk aversion is either unreasonable or lacks a rational basis as their brief implies, this is categorically wrong and inconsistent with binding precedent. As the Federal Circuit recently held, Federal agencies have "**no obligation to point to past experiences substantiating its concerns in order to survive rational basis review....** Indeed [the agency] has a responsibility to assess risks and avoid them before they become a historical fact." *Weeks Marine, Inc. v. United States*, 575 F.3d 1352, 1370 (Fed. Cir. 2009)

(emphasis added) (citing *CHE Consulting v. United States*, 552 F.3d 1351, 1355 (Fed. Cir. 2008)).

DOI rationally determined its minimum requirements for an email messaging system by methodically analyzing: 1) what data would be housed in the cloud; 2) the sensitivity of that data; 3) its risk tolerance, and 4) the benefits and liabilities of each cloud model. See AR158-168. Throughout this process, the agency was informed by extensive market research conducted by itself and third parties. AR175-185, 167-747. At the end of this risk assessment, DOI concluded that it would require five attributes for its cloud. AR168. Two of these attributes were that the cloud's infrastructure be logically and physically dedicated to the DOI or Federal agencies. AR168. Such a requirement is not unreasonable, and the market is fully capable of meeting this need. AR169-172.

Though plaintiffs quibble with details in DOI's assessment, at no point do they ever demonstrate that DOI acted irrationally in determining its minimum needs. *See* Pl. MJAR 39-42. In fact, rather than challenge the overall reasonableness of the Risk Assessment, plaintiffs resort to critiquing minor points contained within. In one instance, plaintiffs claim DOI manipulated the meaning of a quote by failing to cite an accompanying sentence from a slide. Pl. MJAR 39-40.⁸ In another, they disagree about the proper context of a particular quote. Pl. MJAR, p. 40.⁹

⁸ Plaintiffs argue that DOI should have included the line, "This doesn't say anything about actual security." Pl. MJAR, p. 40. Yet the language quoted by DOI captures the meaning of the report perfectly: a private cloud affords the user with greater *control* over security. AR163.

⁹ The risk assessment states that "[redacted] has raised similar concerns regarding sharing of data amongst multiple customers of a cloud provider and the ability to identify the exact location of an organization's data within a cloud deployment." Plaintiffs claim that DOI's position is unsupported by the quote from "[redacted]" "Sensitive or confidential data that is processed beyond the government's control or by nongovernmental employees or contractors can increase the level

[REDACTED] [REDACTED]

And in one place, plaintiffs accuse DOI of ignoring the context of a quotation but admit that the disputed passage is only tangentially related to the issues in this protest. Pl. MJAR, p. 40, n.16 (noting that the quotation “is not particularly pertinent to DOI’s requirement for a government community cloud”).

The petty nature of these contentions becomes even more apparent when contrasted to the portions of the Risk Assessment that plaintiffs do *not* debate. Plaintiffs do not dispute DOI’s quotation from NIST that “private clouds may have less threat exposure than community clouds which have less threat exposure than public clouds.” AR163 (quoting AR471). Plaintiffs do not question DOI’s citation to [REDACTED] for the proposition that “the private model [of cloud deployment] represents the least amount of risk and . . . the public model represents the highest level of risk.” AR163 (citing AR654-663). Nor do plaintiffs challenge DOI’s quotation from the [REDACTED] that NIST’s “existing guidance is not specific to cloud computing issues, and it has only begun plans to issue cloud-specific security guidance.” AR163 (quoting AR718). These are the concerns that gave rise to DOI’s preference for a private cloud or a strictly-defined community cloud, and plaintiffs cannot rebut them.

Plaintiffs’ only substantive challenge to DOI’s Risk Assessment is the manner in which DOI used the [REDACTED] [REDACTED] See AR541-616. Plaintiffs appear to have dropped their original arguments concerning the [REDACTED] Guidance in favor of a new one: “DOI unnecessarily and illogically determined that all e-mail and other computing assets needed to be in the same, more restrictive

of risk” Yet it seems incontrovertible that risk generated by “process[ing] data beyond the Government’s control” should have some relationship to “the ability to identify the exact location

[REDACTED] [REDACTED]

type of cloud.” Pl. MJAR, p. 41. Plaintiffs argue that DOI should have broken down “its various computing assets . . . to determine the appropriate cloud model, from a risk standpoint, for each asset.” *Id.*

This position is wholly without merit. The entire purpose of the unified messaging project is to acquire a single communications system for DOI. Yet, plaintiffs chastise DOI for not considering whether it ought to procure separate clouds for each of its seven assets. *See* AR159 (listing the data assets for cloud deployment as email messages, instant messages, calendars, schedules, distribution lists, personal contact lists, and information stored in Sharepoint portal sites). Nor does this deviation from the [REDACTED] guidance render its conclusion irreparably flawed, as plaintiffs suggest. The drafters of the CSA guidance are clear that “[o]ur goal in this Guidance isn’t to tell you exactly what, where, or how to move into the cloud, but to provide you with practical recommendations and key questions to make that transition as securely as possible, on your own terms.” AR549. DOI followed these practical recommendations within the overarching framework of acquiring a single unified messaging system.

VI. DOI Rationally Determined That It Required A DOI-Only Or Federal-Only Cloud

Contrary to the efforts of the plaintiffs in this case, “competitors do not dictate an agency's minimum needs, the agency does.” *Savantage Financial Services, Inc v. United States*, 595 F.3d 1282, 1286 (Fed. Cir. 2010). Moreover, “determining an agency's minimum needs is a matter within the broad discretion of agency officials . . . and is not for [the] court to second guess.” *Id.* (internal quotations omitted); *see also Fort Carson Support Serv., v. United States*,

of an organization’s data within a cloud deployment.

71 Fed. Cl. 571, 586 (2006) (“The determination of the agency's needs and the best method of accommodating them are solely within the agency's discretion.”). A court will uphold the agency’s decision unless the protester can show that it lacks a rational basis - even if that determination leads to a limited-source procurement. *Cf. Emery Worldwide Airlines, Inc. v. United States*, 264 F.3d 1071, 1086 (Fed. Cir. 2001). Here, despite this well-known precedent, plaintiffs are unabashedly asking this Court to second guess and dictate DOI’s minimum needs.

DOI arrived at its requirements after conducting thorough market research and performing a risk assessment in accordance with the CSA guidance. *See* AR175-185, 158-168. The agency noted its strong risk-aversion and the potential pitfalls posed by multi-tenant clouds. AR164-166; *see also* AR177-184. Given these factors, DOI determined that it needed a cloud that was dedicated either to DOI alone or to DOI and other Federal agencies. AR168. A DOI-cloud is a “private cloud” in NIST parlance. DOI’s market research found that private clouds have less threat exposure, are less complex, and grant customers greater control over security than other types of clouds. AR163-164, 175-183. A Federal-only cloud is a type of “community cloud” under the NIST taxonomy. Although community clouds have more risk than private ones, DOI determined that it could tolerate such risk if the community cloud were limited to Federal agencies and contained on a physically isolated server located in a data center that is maintained in the continental United States.

Plaintiffs create a furor in their brief over the correct nomenclature for DOI’s cloud. The Government acknowledges that certain documents in the record contain different definitions of the varying cloud models and some of them refer to a Federal-only cloud as private. Contrary to plaintiffs’ insinuations, however, DOI was not “attempt[ing] to mischaracterize the cloud model

[REDACTED] [REDACTED]

being procured by DOI and . . . support the pre-selection of the Microsoft product.” Pl. MJAR, p. 28. Rather, the improper terminology appears attributable to the evolving refinement of the requirements and to the inherent vagueness in the NIST definitions. In fact, in defining its requirements, DOI eschewed NIST jargon altogether and simply said that it needed an “infrastructure that is solely dedicated (both physically and logically) to DOI or to DOI and other Federal government customers only.” AR168; *see also* AR167 (“At this point DOI will move away from labels such as „public“ and „private“ and focus on the specific attributes that comprise a cloud model that is acceptable to DOI based on our current requirements and risk tolerance level.”).

Indeed, if anyone is guilty of manipulating the cloud categories to its advantage, it is the plaintiffs. They attempt to equate Google’s cloud with Microsoft’s because both are community clouds. Not all community clouds, however, are created equal. Importantly, the community on Google’s government-wide cloud is much broader than would be on a Federal-only cloud: Google includes state and local entities on its network, greatly expanding the pool of potential customers. Contrary to plaintiffs’ contentions, DOI discusses why Google’s government-wide cloud was unacceptable in a memo from August 20, 2010. AR783. The agency decided to conduct supplemental research after Google publically announced the availability of its government-wide cloud and that it had allegedly received FISMA certification from GSA. *Id.* DOI determined that Google’s government-wide cloud remained unacceptable from a risk tolerance perspective. AR784. Specifically, DOI said that Google’s proposed government-wide approach “remained an issue” because “state and local government . . . entities do not have the same security requirements as Federal agencies, nor would they face the same potential impacts

from security issues that DOI would face.” *Id.*

Moreover, DOI’s research discovered that even local government customers of Google Apps were not necessarily satisfied with its security measures. AR784. The City of Los Angeles delayed its transition to Google’s cloud because of its police department’s unease over the reliability of the cloud’s security. *Id.* DOI also considered the effect of the alleged FISMA certification for Google Apps for Government and determined that, by itself, this fact did not indicate that the cloud satisfied DOI’s enhanced security requirements. AR784-785. In reaching this conclusion, DOI relied upon the research efforts of its Chief Information Officer, Chief Technology Officer, ██████████ Inc. and the testimony of the Director of Information Technology Laboratory at NIST before the United States House of Representatives Committee on Oversight and Government Reform on “Cloud Computing: Benefits of Moving Federal IT into the Cloud.” AR785.

Plaintiffs claim that DOI’s explanations for rejecting Google’s government-wide cloud are overly broad. Pl. MJAR, p. 45.¹⁰ DOI’s reasoning is plain from the face of the August 20 memo. *See* AR784. Given the agency’s risk-averse nature, *see* AR164-166, DOI would only be willing to accept a multi-tenant cloud if all the customers shared basic security policies. While Federal agencies may have some variations among their security requirements, they are all bound

¹⁰ Previously, Google boldly claims that “[n]owhere 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.” Pl. MJAR, p. 42. This claim is utterly without merit. Plaintiffs may not regard DOI’s August 20 explanation at AR784 as satisfactory, but surely they cannot dispute its very existence. Google seems to concede the hyperbole of its original assertion just three pages later in its brief, when it attempts to dismiss as overly broad DOI’s discussion of why it would not accept a Google’s government-wide cloud. *See* Pl. MJAR, p. 45.

[REDACTED] * [REDACTED] [REDACTED] [REDACTED]

by Federal-wide security policies. FISMA is one example, but it is not the only one. State and local governments are simply not held to these standards.

Plaintiffs further complain that “DOI does not recite any security requirements that differ among state, local, or Federal agencies, and the AR includes no such information.” Pl. MJAR, p. 45. Plaintiffs miss the point of DOI’s concern. The agency is not worried about any one particular discrepancy in security requirements; rather it is concerned with the responsiveness and accountability of the cloud-provider in meeting present and future Federal requirements. DOI would justifiably feel safer storing its data in a cloud where all the customers will hold the vendor responsible for meeting those Federal security requirements. DOI trusts a Federal-only cloud more than a government-wide cloud because the former has a single constituency that is unified in its insistence on Federal security precautions.

Moreover, DOI was not required to “recite” specific security requirements in its memo to substantiate its reasoning. An agency is “not required to synthesize its thinking and its market research into a pre-litigation written explanation of the rationale for each of the solicitation requirements.” *Savantage Financial Services, Inc v. United States*, 595 F.3d 1282, 1287 (Fed. Cir. 2010). The Court can recognize the existence of differing security requirements between Federal agencies and state/local actors, even if DOI did not go the extra step of listing them out in its memo.

Similarly misguided is plaintiffs’ objection to DOI’s reliance on a newspaper article concerning the Los Angeles Police Department’s security concerns with Google’s cloud. Plaintiffs seem to argue that DOI should not have considered the piece without first “establish[ing] the truth or accuracy of the article’s contents.” Pl. MJAR, p. 45. They further

argue that DOI should have sought “verification” from Google. *Id.* Yet plaintiffs cite no authority that would impose such extraordinary requirements on an agency before it can rely on a piece from an established trade publication.¹¹ Nor have plaintiffs given any suggestion – let alone actual evidence – that this particular article is inaccurate.

VII. DOI Rationally Considered The Requirements Of FISMA

FISMA seeks to “provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.” FISMA § 301(b)(1), 44 U.S.C. § 3541(1). The requirements of FISMA are captured in a number of Special Publications (“SP”) and Federal Information Processing Standards (“FIPS”), published by the National Institute for Standards and Technology (“NIST”). *See* AR703-704.

Plaintiffs argue that DOI failed to pay sufficient attention to FISMA in conducting its procurement. *See, e.g.*, Pl. MJAR, pp. 46-50. This position overlooks critical features of the FISMA framework and is without merit. First and foremost, GSA’s certification of Google’s cloud does not mean that the cloud is secure enough for DOI. FISMA certification is made on an agency-by-agency basis. 44 U.S.C. § 3544(a); SP 800-37 at 3-34. Under FISMA, each organization is responsible for determining whether a given system’s security protocols are sufficient for its own needs. Even if one agency certifies a system as FISMA-compliant, another agency must still decide whether that same system is adequate for its own purposes.¹² Here,

¹¹ Needless to say, such a policy would prove an incredible burden on agencies; Google’s position would seem to mandate that DOI fact-check each of the thirty-seven articles, reports, and studies that comprised its market research. *See* Tabs 14A-14KK.

¹² Agencies can enter reciprocity agreements “to accept each other’s security assessments in order to reuse information system resources and/or to accept each other’s assessed security posture in order to share information.” SP 800-37 at 1-3 n.11. There is no evidence or

plaintiffs place great weight on Google's FISMA certification by GSA. *See, e.g.*, Pl. MJAR, p. 46.¹³ Yet that certification merely means that Google Apps for Government, assuming it even has FISMA certification, is secure enough *for GSA*. This fact has no direct impact upon whether the cloud's security is sufficient for DOI. Contrary to Google's suggestion, its FISMA certification is *not* a blanket endorsement of Google Apps across the entire Federal government. DOI acted rationally in refusing to treat it as such.

Second, DOI is fully entitled to constrain the cloud model it will accept even if FISMA does not dictate a particular model. FISMA establishes a bare *minimum* level of security for information systems. *See* FISMA § 303, 15 U.S.C. § 278g-3 (2006); *see also* FIPS 200 at v; SP 800-53 at 2-9. The law permits and encourages agencies to impose additional requirements to account for their own unique security needs. SP 800-53 at 1-4. And indeed, that is precisely what DOI did here. The agency recognizes that it must certify its messaging system under FISMA. The SOW plainly states that "the contractor must follow NIST SP 800-37, 800-18, 800-30, 800-60, 800-53A, Federal Information Processing Standard (FIPS) 199 and 200." AR816; *see also* AR817-818; AR1106; AR 1594. Yet DOI has also determined that its security requirements *exceed* the bare minimum mandated by FISMA; thus it also requires that the cloud be dedicated to either DOI or Federal agencies on a physically and logically server that in at least two data centers located within the continental United States. *See* AR168. Contrary to Google's contention, the FISMA certification process is not meant to override an individual agency's

suggestion that DOI has entered into such an agreement with GSA.

¹³ There is now serious question whether Google Apps for Government is actually certified by GSA at all. In fact, all evidence suggests that GSA certified Google Apps Premier (Google's public cloud) and *not* Google Apps for Government.

[REDACTED] [REDACTED]

security needs. AR784-785. DOI was wholly justified in insisting that Google offer a DOI-only or Federal-only cloud.

Moreover, DOI had good reason to require additional safeguards beyond those commanded by FISMA. One [REDACTED] analyst warned that “existing risk assessment frameworks such as NIST Special Publication 800-53 . . . do not address the complexity or risks associated with multi-tenant cloud computing models.” AR 784. The GAO noted that NIST guidance on cloud computing is “insufficient” and cautioned that agencies relying on it “may not have effective information security controls in place.” AR184. In fact, NIST itself appears uneasy about the applicability of its guidance to cloud computing. *See* AR784-785. It recently launched a new initiative to “address a widely acknowledged need in the development and implementation” of cloud computing. AR785. Under these circumstances, DOI certainly possessed a rational basis to exceed the minimum requirements outlined in NIST.

Third, DOI has no cause for alarm from the fact that its contemplated cloud will not be pre-certified by another agency. In their brief, plaintiffs suggest that Microsoft BPOS-Federal’s present lack of FISMA certification should weigh heavily on the agency’s decision-making. *See, e.g.,* Pl. MJAR 18, 47. Under FISMA, however, an information system can be certified only *after* its security controls have been implemented and assessed. SP 800-37 at 2-9. Here, DOI has commissioned the construction of a brand new cloud. DOI would also accept access to a pre-existing Federal-only cloud that met its other requirements. However, none of the offerors have proposed such a cloud; all have offered a private DOI-only cloud.

Because this cloud does not yet exist, there is no way that DOI (or any other agency) could have assessed its security controls. Thus the absence of FISMA certification is not a

glaring weakness in Microsoft BPOS-Federal, as plaintiffs suggest; rather, it is a necessary step in acquiring a dedicated cloud. The terms of the solicitation require the winning contractor to comply with FISMA mandates after award. AR816 -818. DOI has no reason to question the ability or willingness of the awardee to abide by these terms.¹⁴

At bottom, plaintiffs appear to believe that FISMA certification is the ultimate measure of cloud security. *See, e.g.*, Pl. MJAR 33 (“DOI’s selection of BPOS-Federal arbitrarily sacrifices DOI’s underlying concerns for enhanced security (i.e., demonstrated FISMA compliance) . . .”). Indeed, plaintiffs seem to think that Google’s purported certification by GSA ought to trump DOI’s own assessment that it requires a DOI-only or Federal-only cloud. *See, e.g.*, Pl. MJAR 47 (“DOI . . . irrationally determined that Google’s FISMA-certified government cloud is less secure than Microsoft’s untested, non-certified government cloud.”). Yet FISMA and the NIST guidance do not support this position. To the contrary, FISMA specifically *prohibits* DOI from relying entirely on GSA’s certification instead of conducting its own certification and accreditation process. Moreover, the law empowers agencies to set their own security standards. So long as DOI certifies that its cloud meets FISMA requirements prior to operating it, the agency is free to require additional safeguards, such as a DOI-only or Federal-only deployment model.

VIII. DOI Rationally Determined That BPOS-Federal Met Its Minimum Requirements

DOI’s determination that Microsoft BPOS-Federal is the only product currently available that satisfies all of its minimum needs is rationally based upon extensive market research and

¹⁴ Indeed, the U.S. Department of Agriculture is in process of certifying Microsoft’s cloud now. *See supra* n.7.

[REDACTED] [REDACTED]

Google's representation that it could not and would not provide a DOI- or Federal-only private external cloud. AR169-172. Nonetheless, plaintiffs claim that Microsoft's product fails to satisfy DOI's minimum requirements. Pl. MJAR, pp. 49-53. Specifically, they contend that BPOS-Federal will store protected information in a non-dedicated infrastructure.

In its risk assessment, DOI identified seven data assets that needed to be housed on a dedicated infrastructure: [REDACTED]

[REDACTED] AR167. Likewise, DOI required that the applications and processes that handle such data be hosted on a dedicated infrastructure as well. *Id.* If an asset or application does not fall into one of those seven categories, then a contractor would be free to host it on a non-dedicated infrastructure.

Despite this clear language, plaintiffs nonetheless assert that BPOS-Federal fails to meet these requirements because Microsoft management network and Office Live Meeting will be hosted on a non-dedicated infrastructure. Yet neither of these programs contains any of the seven data assets which DOI seeks to protect. *See* AR167. Office Live Meeting is a program whose primary purpose is to enable users to teleconference using Internet-based audio-video technology.¹⁵ Consequently, it does not implicate any of the seven text-based assets listed by DOI.¹⁶

¹⁵ Microsoft Office Live Meeting 2007: <http://office.microsoft.com/en-us/live-meeting/microsoft-office-live-meeting-2007-features-and-benefits-HA101791945.aspx>

¹⁶ "Moreover, plaintiffs' attempt to compare the Live Meeting to these assets is wholly misleading. DOI wants a dedicated cloud so that it can safely store emails, instant messages, calendars, etc. Although Live Meeting operates on a shared infrastructure, the teleconferences are not actually stored there. The system does not automatically generate a permanent copy of the video footage for later retrieval. In this sense, Live Meeting is more akin to a phone call than an email and does not entail the same security concerns as the latter."

Nor does the Microsoft management network process any of the seven protected data assets. Rather, it “contains the infrastructure that is shared across multiple customers, such as the Microsoft Online Services backup and monitoring systems. It also includes an Active Directory forest that contains the user accounts that are needed for operating the services and servers for the Management Network and Managed Network security zones.”¹⁷ Thus, the management network contains information that is meant to be shared among customers (e.g., monitoring systems) and special management user accounts; it does not handle the mundane communications, calendars, etc. that DOI wants to protect.

Google also accuses BPOS-Federal of violating DOI’s requirements by archiving communications in a non-dedicated cloud. Pl. MJAR 51. Google reasons that “[a]rchived e-mail messages are nothing more than copies of messages that have been transferred to data storage to free up computing space,” and so they must be hosted on a DOI-only or Federal-only cloud. *Id.* This position ignores critical distinctions between online email and archived messages which have led DOI to treat the two subjects differently throughout the procurement process. Whereas users have ready access to their online email, access to archived email is strictly controlled. Further, unlike online email, archived email is stored in an encrypted format. AR1003.9. The encryption process used is compliant with Federal standards defined by NIST and will receive its own FISMA certification, separate from the BPOS-Federal system.¹⁸

Contrary to Google’s assertion, encryption is not merely a form of logical separation. *See*

¹⁷ Found at <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=1290dbcb-2eed-441a-a5c0-f15f9647be6b>.

¹⁸ *See* FIPS 140-2, <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>; *see also* AR801 (requiring awardee to meet the standards in FIPS 140-2).

Pl. MJAR 51-52. Logical separation is a way of segregating different customers' data through software so that only authorized users can access it. Encryption is a different security measure altogether. NIST defines it as "the conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized people."¹⁹ In short, logical separation prevents unauthorized users from accessing data. Encryption prevents unauthorized users from *understanding* the data that they do manage to access. Thus it is possible, at least in theory, to have data that is encrypted but not logically separated.

DOI protects online email and archived messages differently because the two types of data serve different purposes. Online email facilitates communication by DOI's employees. In contrast, the primary reason agencies archive email is for e-discovery and other legal purposes. *See* AR170 ("DOI must be able to retain email and Instant Messages and subsequently search the retained messages to meet legal and regulatory requirements such as E-Discovery and legal holds."). If the agency ever has need for an old email, the message is located in the archive and must be decrypted before it can be accessed. AR1003.9. As a practical matter, encryption is not feasible for online email because of the immense processing power necessary to constantly encrypt and decrypt all the messages in the system.

In conclusion, archived email serves a different purpose and is protected in a different manner than normal, online email messages. DOI has consistently regarded archived email as a distinct security issue from active, online messages. In fact, the agency addresses email archival in an entirely different section of the SOW, with its own unique security requirements. *Compare*

¹⁹ NIST IR 7298, *Glossary of Key Information Security Terms* 29 (Apr. 25, 2006) http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf.

AR805-806 *with* 816-822. Nor did DOI fabricate this difference “in order to accommodate shortcomings in Microsoft’s products,” as plaintiffs suggest. *See* Pl. MJAR, p. 52. To the contrary, this distinction is based on the common-sense facts that 1) online emails must be accessed continuously while archived messages are only retrieved when necessary, and 2) archived emails are adequately protected by encryption, a feature that is not available for online email.

IX. Plaintiffs Are Not Entitled To Permanent Injunctive Relief

As we established above, plaintiffs have not demonstrated that DOI’s standardization decision, limited source justification, market research, or determination of its minimum requirements was arbitrary, capricious, lacked a rational basis, or violated statute or regulation. Consequently, plaintiffs are not entitled to injunctive relief in this case.

To obtain permanent injunctive relief, plaintiffs must demonstrate: (1) entitlement to relief on the merits; (2) irreparable harm would result if an injunction does not issue; (3) the harm suffered if injunctive relief is not granted will outweigh the harm to the Government and third parties if the temporary relief is granted; and (4) granting the injunction serves the public interest. *Sofamor Danek Group, Inc. v. DePuy-Motech, Inc.*, 74 F.3d 1216, 1219 (Fed. Cir. 1996).

The grant of an injunction is "extraordinary relief" and, therefore, the Court applies "exacting standards." *Lermer Germany GmbH v. Lermer Corp.*, 94 F.3d 1575, 1577 (Fed. Cir. 1996). For this reason, plaintiffs must point to clear and convincing evidence that each factor has been satisfied. *Government Travel, Inc. v. United States*, 61 Fed. Cl. 559, 574 (2004). The party seeking injunctive relief bears the extremely heavy burden of demonstrating its entitlement to this extraordinary relief by clear and convincing evidence. *E.g., Cincom Systems, Inc. v. United*

States, 37 Fed. Cl. 266, 268 (1997) (citing *Baird Corp. v. United States*, 1 Cl. Ct. 662, 664 (1983)). A party faces an even greater burden when it seeks injunctive relief, which, if granted, would interfere with Governmental operations. *Yakus v. United States*, 321 U.S. 414, 440 (1940); *Virginia Railway Co. v. Systems Federation No.40*, 300 U.S. 515, 552 (1937).

DOI's procurement activities were in accordance with applicable law, statute, and regulation. Accordingly, plaintiffs cannot demonstrate that they are entitled to permanent injunctive relief. Even if this Court were to find that the DOI in the procurement process, plaintiffs are not automatically entitled to the extraordinary relief they request.

A. Plaintiffs Have Not Established Success Upon The Merits

As we demonstrated above, DOI's standardization decision and limited source justification are rationally, reasonable, and consistent with applicable law, statute, and regulation. Accordingly, plaintiffs cannot meet the required legal burdens laid out above and, therefore, has failed to satisfy this prong of the Court's inquiry for permanent injunctive relief.

B. Plaintiffs Have Not Demonstrated That They Will Be Irreparably Harmed If A Permanent Injunction Is Denied

To constitute irreparable harm, plaintiffs' alleged injury must be "certain and great," not theoretical. *Tenacre Foundation v. INS*, 78 F.3d 693, 695 (D.C. Cir. 1996); *Wisconsin Gas Co. v. FERC*, 758 F.2d 669, 674 (D.C. Cir. 1985). Moreover, "[n]ormally, an injury is not considered „irreparable“ if the only injury alleged is monetary loss.” *Chapman Law Firm Co. v. United States*, 67 Fed. Cl. 188, 193 (2005). "In every procurement award there are generally more losers than winners. To find that a losing procurement participant suffers irreparable harm merely because it did not succeed with its contract proposal would create in

[REDACTED] [REDACTED]

the losing party an automatic right to injunctive relief.” *San Diego Beverage & Kup v. United States*, 997 F. Supp. 1343, 1347 (S.D. Cal. 1998).

Other than making a broad assertion of harm concerning a lost opportunity to compete, plaintiffs fails to make a showing that they will suffer irreparable harm if this Court does not issue a permanent injunction. As demonstrated above, DOI’s market research fully and fairly considered all viable alternatives to Microsoft BPOS-Federal and plaintiffs will not suffer harm as a result of DOI’s action. Furthermore, MVS’s allegation of irreparable harm is insufficient in light of the United States Supreme Court’s recent decision in *eBay, Inc. v. MercExchange, L.L.C.*, 547 U.S. 388 (2006).

In *eBay*, the Supreme Court held that the Federal Circuit’s “general rule” in patent disputes “that a permanent injunction will issue once infringement and validity have been adjudged” was improper, and reiterated that, in deciding whether to award permanent injunctive relief, courts must apply the traditional four-factor test applied by courts of equity. *eBay*, 547 U.S. at 392-93. If, in bid protest cases, the loss of the opportunity to compete in a fair and competitive bidding process amounts to irreparable harm, then a protestor’s success on the merits will always result in a finding of irreparable harm, and a portion of the four-factor injunctive relief test will effectively be eliminated. This is precisely what the Supreme Court held was improper. *eBay*, 547 U.S. at 392-93. Moreover, the opportunity to compete has a purpose, to win a contract and earn money by performing it. Competition is not an end to it itself, thus, plaintiffs’ claim of injury is a claim for economic loss. In making its bald assertion of irreparable injury, plaintiffs fail to make any account of the business opportunities they would be able to pursue with the resources that were not consumed by performing for DOI. In light of *eBay*, plaintiffs’ claim of irreparable harm

should be rejected as unsupported and illusory.

C. Plaintiffs Have Not Demonstrated That Their Harm Is Greater Than The Harm To DOI

The harm to the Government if the contract is enjoined would be substantial. The Government does not seek to purchase a unified messaging service for an abstract purpose, but to drastically improve DOI's communication system, significantly increase its ability to protect critical information that falls within its responsibility, and to save millions of tax-payer dollars. Moreover, the plaintiffs' unstated assumption is that, in the unlikely event this Court enjoins DOI from proceeding with the procurement, the minimum requirements calling for a physically and logically isolated server located within the continental United States will be deleted from the RFQ. Based upon the nature of DOI's security concerns, it is more likely that these requirements will not be relaxed. Thus, there is a chance that plaintiffs may again fail to comply with the RFQ's requirements and would be ineligible for award of the contract. Accordingly, even if we assume that all of the plaintiffs' allegations on the merits of this case are accurate, any harm they may suffer is illusory. Consequently, the very real harm DOI would suffer, continued threat exposure, mission-impact, and millions of lost tax-payer dollars outweigh the effects of a procurement error or procedural defect on plaintiffs.

D. Plaintiffs Have Not Demonstrated That A Permanent Injunction Would Serve The Public Interest

The public interest is served when the integrity of the procurement system is maintained. *LABAT-Anderson, Inc v. United States*, 65 Fed. Cl. 570, 581 (2005). "It is equally clear, however, that a procuring agency should be able to conduct procurements without excessive judicial infringement upon the agency's discretion." *Aero Corp. v. United States*, 38 Fed. Cl.

237, 242 (1997) (citation omitted. Plaintiffs have failed to show that the integrity of the procurement system has been compromised by DOI's activities during the procurement, or that the exaltation of a contractor's commercial interest should outweigh DOI's legitimate need to procure a unified messaging system. It is in the public's interest for DOI to complete the procurement. Indeed, if the Court were to permanently enjoin DOI from making award of the contract, the public interest would not be served because, as Mr. Corrington explains, the RFQ is "a fundamental component of DOI's strategy to address ongoing operational issues that reduce DOI's information security posture, negatively impact mission performance and result in excessive costs for delivering email services."²⁰ Without the award of the contract, DOI will suffer irreparable harm in three areas: 1) information security; 2) mission performance; and 3) excessive costs. *Id.* In fact, if permitted to award the contract, DOI's risk exposure from malware viruses will be lowered by approximately 150 million spam messages, DOI will have a consistent method of communicating with its 13 bureaus for the first time, and DOI will save approximately \$1.75M in excessive cost savings just in the first three months of performance. *Id.* pp. 2-6.

Plaintiffs have failed to show they will suffer any harm, let alone irreparable harm, whereas DOI will suffer irreparable harm in the form of approximately an additional 150 million spam attacks, continued risk of mission failure, and a net loss of at least \$1.75 million in excessive costs. There can be no real debate that that the balance of harms tips in favor of DOI and, therefore, a permanent injunction is not appropriate in this case. The public interest is best served

²⁰ See Atch. A. p.6, Defendant's Opposition To Plaintiffs' Motion For A Preliminary Injunction filed with the Court on November 19, 2010.

by allowing DOI to proceed with award of the contract.

CONCLUSION

For the foregoing reasons, the Court should deny plaintiffs' motion for judgment upon the administrative record and grant our cross-motion for judgment upon the administrative record.

Respectfully submitted,

TONY WEST
Assistant Attorney General

MICHAEL F. HERTZ
Deputy Assistant Attorney General

s/ Kirk T. Manhardt
KIRK T. MANHARDT
Assistant Director

OF COUNSEL
CHARLES M. KERSTEN
Trial Attorney
Commercial Litigation Branch
Civil Division
Department of Justice

SHERYL RAKESTRAW
Attorney Advisor
Department of the Interior

December 17, 2010

s/ Christopher L. Krafchek
CHRISTOPHER L. KRAFCHER
Trial Attorney
Commercial Litigation Branch
Civil Division
Department of Justice
1100 L Street, N.W.
Washington, D.C. 20005

Attorneys for Defendant



ATTACHMENT 1



ATTACHMENT 2



10
11



11
12





ATTACHMENT 3

[REDACTED] [REDACTED]

Corrington, William B

From: [REDACTED]
Sent: Thursday, December 16, 2010 12:44 PM
To: Corrington, William B; bo.berlas@gsa.gov
Subject: Re: ATO for Google Apps

The google for government does not have a c and a, yet. They are working on it and we expect them to submit documentation within the next 30 days or so.

Kurt Garbars, CISSP, CSW
Senior Agency Information Security Officer
[REDACTED]

From: "Corrington, William B" [REDACTED]
Sent: 12/16/2010 12:22 PM EST
To: Bo Berlas
Cc: Kurt Garbars
Subject: RE: ATO for Google Apps

Follow on question: Google has been talking about Google Apps for Government having a FISMA certification. However, the documents you sent last night appear to be for Google Apps. Is there a separate certification for Google Apps for Government? My understanding is that the Government version was supposed to be on different infrastructure so I would expect a separate certification package would be required.

Thanks

William Corrington, CISSP, PMP
Chief Technology Officer
Department of the Interior
[REDACTED]

From: [REDACTED]
Sent: Wednesday, December 15, 2010 7:14 PM
To: Corrington, William B
Cc: 'kurt.garbars@gsa.gov'
Subject: Re: ATO for Google Apps

Attached, please find the requested documents.

Bo Berlas, CISSP, PMP
Office of the Senior Agency Information Security Officer
[REDACTED]

<http://www.gsa.gov>

[REDACTED] [REDACTED]

[DH/DSS Fingerprint](#)

[45CF C880 5976 E544 8A7B 9CD1 31D9 782A 16D8 C775](#)

"Corrington, William B" [REDACTED]

[REDACTED]
Subject Re: ATO for Google Apps

12/15/2010 05:46 PM

Excellent! Thank you!

From: [REDACTED]
To: Corrington, William B
Cc: [REDACTED]
Sent: Wed Dec 15 17:23:58 2010
Subject: Re: ATO for Google Apps

Casey coleman (gsa cio) signed the ATO. I will Bo (cc'd above) send you the assessment and authorization letters.

Kurt Garbars, CISSP, CSW
Senior Agency Information Security Officer
[REDACTED]

From: "Corrington, William B" [REDACTED]
Sent: 12/15/2010 04:37 PM EST
To: Kurt Garbars
Subject: ATO for Google Apps

Hi Kurt,

I'm following up on the voice mail that I just left you...I understand that you led the evaluation of Google Apps earlier this year that resulted in the issuance of an ATO by GSA. I'm trying to find out who signed the ATO and if possible, to get a copy of the certification document (not the entire C&A package).

If you can help me out I'd greatly appreciate it.

Thanks

William Corrington, CISSP, PMP
Chief Technology Officer
Department of the Interior
[REDACTED]



ATTACHMENT 4

Washington Technology

The online authority for government contractors and partners

Google releases FISMA-compliant Apps for Government



Cloud-based suite meets federal regs; Microsoft looking to catch up

- By [Rutrell Yasin](#)
- Jul 26, 2010

After a year of working on security steps to comply with federal government regulations, Google today launched Google Apps for Government.

Google Apps for Government is the first suite of cloud computing applications to receive Federal Information Security Management Act (FISMA) certification and accreditation from the U.S. government, said David Mihalchik, Google's federal business development executive. The Google Apps platform consists of Google Docs, Gmail, spreadsheets, a video tool and Google Sites.

The General Services Administration has reviewed the documentation of the company's security controls and last Thursday issued an authorization to operate, Mihalchik said.

The move will almost certainly intensify the competition between Google and Microsoft to provide cloud-based e-mail service and productivity applications to the federal community, industry observers said.

"The federal government is the golden nugget everyone is chasing," said David Linthicum, chief technology officer and founder of Blue Mountain Labs.

"FISMA is always being brought up as a hindrance to the government moving to the cloud," Linthicum said. Google is basically saying that Google Apps is ready to go, he said.

GovernmentTrainingExchange.com

Related coverage:

[Are Google Apps and Microsoft headed for a showdown?](#)

[GSA Plans email system revamp](#)

"FISMA was a top priority for us," Mihalchik said. The certification was a very detail process that involved Google meeting 200 National Institute of Standards and Technology security controls, testing by an independent organization and a GSA review, he said. The review makes it easier for federal agencies to compare Google security features to those of their existing systems, Mihalchik said.

Microsoft says it is close to obtaining the same certification for a Web-based version of Exchange, a widely used program for managing e-mail that most organizations run on their own server systems, according to a [Wall Street Journal](#) article. Google and Microsoft are competing to provide e-mail to GSA.

The government defines cloud computing as an on-demand model for network access, allowing users to tap into a shared pool of configurable computing resources, such as applications, networks, servers, storage and services, that can be rapidly provisioned and released with minimal management effort or service-provider interaction.

Google Apps for Government is hosted in a multi-tenant cloud that conforms to NIST's definition of a community cloud, Mihalchik said.

Google will store Gmail and Calendar data in a segregated system located in the continental United States, exclusively for government customers. Other applications will follow in the near future. Mihalchik said.

The Energy Department's Lawrence Berkeley Laboratory starting deploying Google Apps for its 5,000 users early this year. Berkeley Labs is using Gmail, Docs, Sites and Calendar, with full deployment scheduled by the end of the year.

The Berkeley lab did its own security accreditation of Google Apps and reviewed Google's documentation before the company had completed its FISMA compliance, Mihalchik noted. The lab is expected to save \$1.5 million to \$2 million over five years by using Google Apps for Government, he said.

Google also announced that InRelief.org, a humanitarian relief organization funded by the U.S. Navy, is also using Google Apps for Government to provide users with more real-time collaboration capabilities during disasters.

Government movement to the cloud will continue to be an evolutionary process – agency by agency, division by division, Linthicum said. The offering of e-mail services, which falls into the software-as-a service cloud delivery model, is a logical place for many agencies to start, industry experts have observed.

FISMA compliance for infrastructure-as-a service and platform-as-a-service will be the next step for cloud providers, Linthicum said. FISMA compliance for these cloud delivery models will be more complex, Linthicum noted.

About the Author

Rutrell Yasin is senior technology editor for Government Computer News magazine.

**THE BUSINESS IMPLICATIONS
OF GOVERNMENT ACTION**

**Bloomberg
GOVERNMENT
BGOV.COM**



© 1996-2010 1105 Media, Inc. All Rights Reserved.



ATTACHMENT 5



Solutions

Products

How it works

Get started

Customers

Support

Secure applications to meet the needs of government.

Google Apps for Government, now with FISMA certification.

Contact Sales

Built with security and reliability in mind

With Google Apps for Government, agencies can benefit from the scale and redundancy of one of the most robust networks of distributed datacenters in the world. The protection of the data and intellectual property on these servers is our top priority, with extensive resources dedicated to maintaining data security. Google is committed to providing the best security in the industry on an ongoing basis.

First with FISMA certification

Obtaining Federal Information Security Management Act (FISMA) certification & accreditation for Google Apps is critical to our US federal government customers, who must comply with FISMA by law.

All customers – both public and private sector – benefit from this governmental review and certification of our security controls.

- Google is the first in the industry to complete FISMA certification for a multi-tenant cloud application.
- Google Apps has received an authority to operate at the FISMA-Moderate level; an independent auditor assessed the level of operational risk as Low.
- Google's FISMA documentation is available for review by interested agencies. This enables agencies to compare the security of Google Apps to that of existing systems. [Submit a request.](#)

“ In addition to empowering employees across the city, everyone will benefit from Google's security controls, which will provide a higher level of security for City data than exists with our current system.

- Randi Levin, CTO, City of Los Angeles

Learn more

- [FAQ](#)
- [Compare editions](#)

Additional resources:

- [Email security](#)
- [Security and privacy FAQs](#)
- [Security whitepaper](#)

Certifications:

FISMA



cloud security alliance™

Meeting unique government requirements

Google Apps for Government provides segregated systems for our US government customers. Government customer data is stored in the US only. This "community cloud" – as defined by the [National Institute of Standards and Technology](#) – is available now to any federal, state or local government in the United States.

Security & reliability advantages of the cloud



Switch to Google Apps

Learn how switching from

Google Apps brings you the latest technologies and some of the best practices in the industry for datacenter management, network application security, and data integrity.

- Prepare your agency with [best-in-class disaster recovery](#) at no additional cost.
- Protect against the latest threats with no scheduled downtime. Google's architecture enables rapid updates and configuration changes across the entire network as needed.
- Get 99.9% uptime with the Google Apps for Government service level agreement, giving you confidence that employees will have access whenever they need it.
- Reduce the risk of lost USB drives and laptops; employees can access information securely from anywhere.
- Benefit from our full-time information security team, including some of the world's foremost experts in information, application, and network security.

[Microsoft Exchange](#) or [Lotus Notes](#) helps you save money and reduce IT hassles.



Google Apps + Postini

Learn about Postini email [archiving and e-discovery](#) services.

Security FAQs

- [+ What is FISMA?](#)
- [+ Who owns the data that organizations put into Google Apps?](#)
- [+ Where is my organization's data stored?](#)
- [+ Is my organizations data safe from your other customers when it is running on the same servers?](#)
- [+ What does a Google Apps SAS70 Type II audit mean to me?](#)
- [+ Can my organization use our own authentication system to provide user access to Google Apps?](#)

Want More Apps?

Extend Google Apps with the [Google Apps Marketplace](#).



Solutions

[Google Apps \(Free\)](#)
[Google Apps for Business](#)
[Google Apps for Education](#)

Products

[Gmail for Business](#)
[Google Calendar](#)
[Google Docs](#)
[Google Groups](#)
[Google Sites](#)

How it works

[Benefits](#)
[Features & pricing](#)
[Mobile](#)
[Security](#)
[Privacy](#)

Get started

[30-day free trial](#)
[Contact sales](#)

Customers

[Success stories](#)

Support

[FAQ](#)
[Online support](#)
[Help center](#)
[Setup & deployment](#)
[Account management](#)

Google Apps for
Government

Google Video

Product videos

Email & phone support

Google Apps for Non-
profit

More Google
Applications

Chrome notebooks

Compare editions

Apps Marketplace

Become a reseller

Chrome browser

© 2010 Google

[Terms of Service](#)

[Program Policies](#)

[Help Center](#)



Search this site

[REDACTED] [REDACTED]

CERTIFICATE OF FILING

I hereby certify that on this 17th day of December 2010, a copy of the foregoing “DEFENDANT’S CROSS-MOTION FOR JUDGMENT UPON THE ADMINISTRATIVE RECORD AND RESPONSE TO PLAINTIFF’S MOTION FOR JUDGMENT UPON THE ADMINISTRATIVE RECORD” 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/ [REDACTED]