

TABLE OF CONTENTS

STATEMENT OF THE ISSUES..... 1

STATEMENT OF THE CASE. 2

 I. Nature Of The Case. 2

 II. Statement Of Facts..... 3

ARGUMENT..... 10

 I. Standard Of Review For Preliminary Injunctions. 10

 II. Standard For Procurement Challenges..... 11

 III. Plaintiffs Cannot Demonstrate That They Are Likely To Succeed On The Merits
 Because DOI Properly Determined Its Minimum Needs And Possessed A Rational
 Basis To Partially Restrict Competition Through A Brand Name Procurement. . 13

 A. DOI Did Not Issue A Sole-Source Award To Microsoft..... 14

 B. DOI Properly Determined Its Minimum Requirements..... 15

 1. DOI's requirements are rationally based upon valid
 security concerns. 16

 2. DOI's determination that its minimum requirements will only be
 satisfied by a DOI- or Federal-only cloud is rationally based upon
 extensive market research. 19

 3. DOI reasonably relied upon the CSA Guidance in determining
 its risk tolerance..... 21

 4. DOI was not required to follow NIST procedures when selecting
 its cloud deployment model because they are only applicable to
 specific security controls and impose baseline requirements rather
 than a limitation upon a requirement for enhanced security. 23

 5. DOI rationally concluded that cloud-based email messaging is the
 best way to satisfy its minimum needs..... 24

 C. DOI Rationally Concluded That Google Cannot Meet Its Minimum
 Requirements..... 25

D.	DOI Properly Determined That Microsoft BPOS-Federal Is The Only Product Currently Available That Meets DOI's Minimum Requirements And, Therefore, DOI Possessed A Rational Basis To Issue The Limited Source Justification.	28
1.	BPOS-Federal offers a dedicated solution that does not share infrastructure with private parties.	28
2.	DOI's requirement for a dedicated email messaging service through a private external cloud contemplates post-award FISMA certification.	30
3.	Storage of non-messaging data is irrelevant to DOI's security requirements.	30
IV.	Plaintiffs Have Failed To Demonstrate They Will Suffer Irreparable Harm If This Court Does Not Grant Its Motion For A Preliminary Injunction.	31
V.	Plaintiffs Have Not Demonstrated That The Harm To The Government From Granting The Plaintiffs' Motion For A Preliminary Injunction Would Be Less Than The Harm To Plaintiffs If The Court Denied Plaintiffs' Motion.	33
VI.	Plaintiffs Have Not Demonstrated That It Is In The Public Interest To Grant Plaintiffs' Motion For A Preliminary Injunction.	35
	CONCLUSION.	35

TABLE OF AUTHORITIES

CASES

<u>Aero Corp. v. United States</u> , 38 Fed. Cl. 237 (1997).	30
<u>Akal Security Inc. v United States</u> , 87 Fed. Cl. 311 (2009).	11, 29
<u>Baird Corp. v. United States</u> , 1 Cl. Ct. 662, 664 (1983).	10
<u>Banknote Corp. of Am., Inc. v. United States</u> , 365 F.3d 1345 (Fed. Cir. 2004).	12
<u>Bannum, Inc. v. United States</u> , 404 F.3d 1346 (Fed. Cir. 2005).	11
<u>Bromley Contracting Co. v. United States</u> , 15 Cl. Ct. 100, 105 (1988).	11
<u>Burlington Truck Lines v. United States</u> , 371 U.S. 156, 168 (1962).	11
<u>Campbell v. United States</u> , 2 Cl. Ct. 247, 249 (1983).	11
<u>Cincom Systems, Inc. v. United States</u> , 37 Fed. Cl. 266 (1997).	10
<u>Cincom Systems, Inc. v. United States</u> , 37 Fed. Cl. 663 (1997).	10
<u>Citizens to Preserve Overton Park, Inc. v. Volpe</u> , 401 U.S. 402 (1971).	10
<u>Cobell v Salazar</u> , 573 F.3d 808 (D.C. Cir. 2009).	passim

<u>Emery Worldwide Airlines, Inc. v. United States,</u> 264 F.3d 1071 (Fed. Cir. 2001).	11
<u>Eskridge Research Corp. v. United States,</u> 92 Fed. Cl. 88 (2010).	29
<u>FMC Corporation v. United States,</u> 3 F.3d 424 (Fed. Cir. 1993).	9
<u>Heritage of Am., LLC v. United States,</u> 77 Fed. Cl. 66 (2007).	27
<u>Holloway & Co., PLLC v. United States,</u> 87 Fed. Cl. 381 (2009).	30
<u>Impresa Construzioni Geom. Domenico Garufi v. United States,</u> 238 F.3d 1324 (Fed. Cir. 2001).	passim
<u>Intel Corp. v. ULSI Sys. Tech., Inc.,</u> 995 F.2d 1566 (Fed. Cir. 1993).	9
<u>Lermer Germany GmbH v. Lermer Corp.,</u> 94 F.3d 1575 (Fed. Cir. 1996).	9
<u>M.W. Kellogg Co. v. United States,</u> 10 Cl. Ct. 17, 23 (1986).	10
<u>NVT Techs., Inc. v. United States,</u> 370 F.3d 1153 (Fed. Cir. 2004).	12
<u>National Steel Car, Ltd. v. Canadian Pac. Ry., Ltd.,</u> 357 F.3d 1319 (Fed. Cir. 2004).	9
<u>Overstreet Elec. Co. v. United States,</u> 47 Fed. Cl. 728 (2000).	28
<u>PGBA, LLC v. United States,</u> 57 Fed. Cl. 655 (2003).	28, 30

<u>Protection Strategies, Inc. v. United States,</u> 76 Fed. Cl. 225 (2007).	29
<u>Ramcor Servs. Group, Inc. v. United States,</u> 185 F.3d 1286 (Fed. Cir. 1999).	10
<u>Redland Genstar, Inc. v. United States,</u> 39 Fed. Cl. 220 (1997).	10
<u>Savantage Financial Services, Inc v. United States,</u> 595 F.3d 1282 (Fed. Cir. 2010).	passim
<u>Sierra Military Health Services, Inc. v. United States,</u> 58 Fed. Cl. 573 (2003).	27
<u>Tech. Sys., Inc. v. United States,</u> 50 Fed. Cl. 216 (2001).	12
<u>Virginia Railway Co. v. Systems Federation No. 40,</u> 300 U.S. 515 (1937).	10
<u>Yakus v. United States,</u> 321 U.S. 414 (1940).	10

STATUTES

5 U.S.C. § 5521.....	7
5 U.S.C. § 702.....	10
5 U.S.C. § 706.....	12
5 U.S.C. § 706(2)(A).	10, 12
15 U.S.C. § 278g-3 (2006).....	21
18 U.S.C. §1831.....	17
18 U.S.C. §1905.....	17
28 U.S.C. § 1491(b)(1).	10

28 U.S.C. § 1491(b)(4). 10, 12
44 U.S.C. § 3541..... 7

MISCELLANEOUS

FAR § 8.405-6(c)..... passim

[REDACTED]
[REDACTED]
when determining its minimum requirements for an email messaging solution.

2. Whether plaintiffs have demonstrated that they are likely to prove that 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 have demonstrated that they are likely to prove that DOI's decision to procure an email message solution from the General Services Agency Federal Supply Schedule pursuant to FAR § 8.405-6(c)(ii) was irrational and prejudicial.

4. Whether plaintiffs have demonstrated that they are entitled to preliminary injunctive relief because they have shown that: 1) they are likely to succeed on the merits of their claims; 2) they will suffer irreparable harm if the Court does not enjoin the Government from awarding a contract to the successful offeror under Request for Quotation No. 503786 ("RFQ") on January 26, 2010; 3) the harm to DOI from granting preliminary injunctive relief would be outweighed by the harm to plaintiffs if the Court denied the motion; and 4) that it is in the public interest to issue a preliminary 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 (collectively, "plaintiffs"), regarding the 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 solicits quotes for the purpose of DOI's award of a single, firm-fixed-price Blanket Purchase Agreement to a

[REDACTED]
[REDACTED]

General Services Administration (“GSA”) Federal Supply Schedule 70 contract holder. Under the RFQ, the procurement would have a stated budget ceiling of \$59.3 million over the five-year contract term.

Plaintiffs protest DOI’s decision to limit competition for DOI’s requirements to resellers of the Microsoft Business Productivity Online Suite — Federal (“BPOS-Federal”) solution. Plaintiffs allege that DOI has established requirements that exceed the agency’s minimum needs in order to justify its decision to standardize on a BPOS-Federal solution and exclude other products from consideration. Plaintiffs also allege that the BPOS-Federal product is an “unproven” solution that fails to satisfy the RFQ’s requirements. Plaintiffs seek to enjoin award of the contract for email messaging services under the RFQ and contend that DOI’s determination of its minimum requirement unduly restrict competition without a rational basis. As we demonstrate below, plaintiffs’ contentions are wholly lacking in merit and are belied by the record. Therefore, this Court should deny plaintiffs’ motion for a preliminary injunction.

II. Statement Of Facts

In 2002, the Science Applications International Corporation implemented a DOI 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. Id. In its place, DOI provided policy guidance to the 13 bureaus and bureau officers to begin migration of their existing email system to Microsoft

[REDACTED]
[REDACTED]

Exchange on a bureau-by-bureau basis by the end of fiscal year 2009. Id. On April 9, 2008, after the passage of 18 months, progress of the email migration varied by bureau and DOI elected to review the 2006 policy. Id. DOI officially selected William Corrington to lead a DOI email team tasked with reviewing DOI's messaging policy. AR2.

DOI's email team began assessing the viability of implementing a single email system, known as unified messaging, for its 13 bureaus in late 2007. AR175. DOI embarked upon an extensive and exhaustive market research program to develop a recommended approach for implementing the unified messaging system. Id. As part of its research, DOI relied upon information provided by [REDACTED] a leading Information Technology ("IT") firm, the

[REDACTED] ([REDACTED] the [REDACTED]

[REDACTED] See AR175-185. DOI officials also met with potential vendors, such as Microsoft and Google, to provide the vendors with the opportunity to explain how they would satisfy DOI's business requirements. AR184.

Early in its research, DOI learned that a cloud-based messaging system would best meet its needs. AR752-754. Cloud computing is a relatively new model for procuring computer services in a convenient, efficient, and elastic manner. See AR 436. Instead of purchasing its own computer infrastructure, many organizations are now buying just the computing service, usually from a third-party with its own off-site infrastructure. IT experts often compare cloud computing to a utility service. AR317. Just as an organization can choose between owning its own electric generator or purchasing electricity from a utility company, now an organization can

[REDACTED]

choose between owning its own computer servers, applications, storage, etc. or buying computing services from a cloud provider. These services can be readily delivered to the procuring organization over the Internet.

DOI representatives met with Google multiple times prior to selecting Microsoft BPOS-Federal its standard email messaging service. AR175. During a February 18, 2010 meeting, Google advised DOI that “no single tenant or ‘private cloud’ would be available for cloud-based email services.” Id. At follow-up meeting on June 9, 2010, when asked if they could provide dedicated infrastructure, Google advised DOI that they were “incapable of supporting a dedicated solution and proceeded to argue about the merits of a dedicated infrastructure.” AR184-185. 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 is the first step in DOI’s plan to migrate to a single messaging service. See AR1002.1-1002.6.

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

[REDACTED]

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 of cloud deployment models. AR158-168. 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 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 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 DOI’s responsibility to manage sensitive information such as Indian trust data and law enforcement data. Accordingly, a private cloud model was selected to best meet DOI’s security and risk tolerance requirements. AR164, 166.

██
██

On June 29, 2010, ██████ completed an analysis of 13 firms that provide messaging and collaboration systems, including Google, to determine if they met DOI's requirements. AR169-172. ██████ solicited product and Federal security compliance information from vendors, trusted third party research, and other Federal Government informational resources. AR170. ██████ concluded that only Microsoft's BPOS-Federal Suite met all of DOI's technical and security requirements. AR171. To complete its research for DOI, ██████ assigned a project team with over 50 years of experience that was led by former Strategic Sourcing experts from ██████ Federal Consulting Practice. 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 ██████ definitions of cloud models, and reports from both ██████ in its consideration of risks associated with each of these models. AR755. In so doing, DOI adopted ██████'s risk-assessment approach for the various cloud deployment models. Id. Specifically, DOI concluded that the following attributes of a cloud computing deployment define DOI's current requirements for the implementation of an enterprise e-mail and collaboration system:

1. Collaboration services provided by an external vendor as a standardized service offering;
2. Ability to comply with security requirements defined by the Federal Information Security Management Act ("FISMA");
3. Data storage infrastructure that is solely dedicated (both physically and logically) to DOI or to DOI and other Federal government customers only;
4. Computing infrastructure that is solely dedicated (both physically and logically) to

██
██
DOI or to DOI and other Federal government customers only; and

5. Implementation of a minimum of two data centers located within the continental United States.

AR755. 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.

DOI conducted a market survey of GSA Schedule 70 and identified nine vendors capable of meeting the requirement for Microsoft BPOS-Federal. AR769. ██████████ independently confirmed that at least five GSA FSS vendors are capable of meeting the requirement to provide Microsoft BPOS-Federal. AR171.

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.

On August 20, 2010, in response to Google's announcement, DOI completed supplemental market research to determine any effect the Google development had upon DOI's July 15, 2010 standardization decision. AR783-785. DOI determined that ██████████

[REDACTED]
[REDACTED]
[REDACTED] AR784. Specifically, DOI determined that Google's proposed government-only, multi-tenant approach [REDACTED]

[REDACTED] d. Moreover, DOI's research discovered that even [REDACTED]

[REDACTED] 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 FISMA certification for Google Apps and determined that, [REDACTED]

[REDACTED] AR784-785. In reaching this conclusion, DOI relied upon the research efforts of its Chief Information Officer, Chief Technology Officer, Gartner, 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.

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 transitioning from a disparate and disjointed email message system to one that is consolidated and secure, to wit: 1) unified email system; and 2) enhanced security. Id.

[REDACTED]

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.

ARGUMENT

I. Standard Of Review For Preliminary Injunctions

“A preliminary injunction is a ‘drastic and extraordinary remedy that is not to be routinely granted.’” *National Steel Car, Ltd. v. Canadian Pac. Ry., Ltd.*, 357 F.3d 1319, 1324 (Fed. Cir. 2004) (quoting *Intel Corp. v. ULSI Sys. Tech., Inc.*, 995 F.2d 1566, 1568 (Fed. Cir. 1993)).

Because the grant of an injunction is “extraordinary relief,” the Court applies “exacting standards.” *Lermer Germany GmbH v. Lermer Corp.*, 94 F.3d 1575, 1577 (Fed. Cir. 1996). To obtain the extraordinary relief of an injunction prior to trial, the movant must establish the following:

- 1) the movant is likely to succeed on the merits at trial,
- 2) the movant will suffer irreparable harm if preliminary relief is not granted,
- 3) the balance of the hardships tips in the movant’s favor, and
- 4) a preliminary injunction will not be contrary to the public interest.

FMC Corporation v. United States, 3 F.3d 424, 427 (Fed. Cir. 1993). Failure to meet the criteria of any one factor may require denial of the request for a preliminary injunction:

[REDACTED]

No one factor, taken individually, is necessarily dispositive. If a preliminary injunction is granted by the trial court, the weakness of the showing regarding one factor may be overborne by the strength of the others. If the injunction is denied, the absence of an adequate showing with regard to any one factor may be sufficient, given the weight or lack of it assigned to the other factors, to justify the denial.

Id. (citation omitted) (emphasis added).

The party seeking preliminary 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).

II. Standard For Procurement Challenges

The standard of review in a bid protest is whether the agency action was arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law. 28 U.S.C. § 1491(b)(1), (4); 5 U.S.C. §702, 706(2)(A); *Impressa Construzioni Geom. Domenico Garufi v. United States*, 238 F.3d 1324, 1332 (Fed. Cir. 2001); 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).

[REDACTED]

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); see also *M.W. Kellogg Co. v. United States*, 10 Cl. Ct. 17, 23 (1986) (holding that “deference must be afforded to an agency’s . . . procurement decisions if they have a rational basis and do not violate applicable law or regulations”). 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). This burden “is not met by reliance on [the] pleadings alone, or by conclusory allegations and generalities.” *Bromley Contracting Co. v. United States*, 15 Cl. Ct. 100, 105 (1988); see also *Campbell v. United States*, 2 Cl. Ct. 247, 249 (1983).

This deference 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)).

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).

III. Plaintiffs Cannot Demonstrate That They Are Likely To Succeed On The Merits Because DOI Properly Determined Its Minimum Needs And Possessed A Rational Basis To Partially Restrict Competition Through A Brand Name Procurement

In general, “[a] plaintiff must show a reasonable probability of success on the merits to justify a preliminary injunction.” *Akal Security Inc. v United States*, 87 Fed. Cl. 311, 317 (2009) (internal quotations omitted). This Court's limited review of agency procurement decisions is set forth in the Administrative Procedure Act (“APA”), 5 U.S.C. § 706. See 28 U.S.C. § 1491(b)(4); *NVT Techs., Inc. v. United States*, 370 F.3d 1153, 1159 (Fed. Cir. 2004). The APA provides that an agency's decision is to be set aside only if it is “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.” 5 U.S.C. § 706(2)(A); *Banknote Corp. of Am., Inc. v. United States*, 365 F.3d 1345, 1350 (Fed. Cir. 2004); *Tech. Sys., Inc. v. United States*, 50 Fed. Cl. 216, 222 (2001). In other words, an agency action “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.” *Impresa Construzioni Geom. Domenico Garufi v. United States*, 238 F.3d 1324, 1332 (Fed.Cir.2001). Therefore, in the context of this bid protest, plaintiffs must

[REDACTED]

demonstrate the likelihood that DOI's standardization decision and subsequent limited source justification issued with the RFQ were improper. As we establish below, plaintiffs cannot meet this burden.

Plaintiffs challenge the rationality of DOI's decision to standardize its email messaging system to Microsoft BPOS-Federal and the subsequently issued limited source justification issue with the RFQ. When placing orders on a Federal Supply Schedule, a procuring agency may limit its consideration to brand name items if "the particular brand name, product, or feature is essential to the Government's requirements, and market research indicates other companies' similar products, or products lacking the particular feature, do not meet, or cannot be modified to meet, the agency's needs." FAR § 8.405-6(a)(2). DOI issued its Limited Source Justification pursuant to this subsection of the FAR.

A. DOI Did Not Issue A Sole-Source Award To Microsoft

Plaintiffs repeatedly attempt to characterize DOI's limited source justification as a "sole source award." Pl. Memo. 25. As an initial matter, this argument is nonsensical and belied by the record. FAR § 2.101 defines a sole source award as "a contract for the purchase of supplies or services that is entered into or proposed to be entered into by an agency after soliciting and negotiating with only one source." *Id.* Here, DOI solicited multiple sources by issuing a RFQ to holders of the GSA Schedule 70 contract. Accordingly, plaintiffs' attempts to redefine the agency's procurement decision, by repeatedly referring to the limited source justification as a sole source award, is simply wrong on its face. Moreover, DOI's actions are clearly consistent

[REDACTED]

with those outlined in FAR § 8.405-6(a)(2)¹ and are properly referred to as a “limited source justification” or a brand-name procurement.

B. DOI Properly Determined Its Minimum Requirements

Contrary to the efforts of the plaintiffs in this case, “competitors do not dictate an agency's minimum needs, the agency does.” Savantage, 595 F.3d at 1286. 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). Here, despite this well-known precedent, plaintiffs are unabashedly asking this Court to second guess and dictate DOI’s minimum needs. As we demonstrate below, irrespective of whether plaintiffs or this Court may second-guess or dictate an agency’s minimum needs, the record in this case unequivocally establishes that DOI’s determination of its minimum needs is rationally based upon extensive market research and valid security concerns.

¹ Pursuant to FAR § 8.405-6(a)(2), Federal agencies are required to issue a limited source justification “when restricting consideration . . . [t]o an item peculiar to one manufacturer (e.g., a particular brand name, product, or a feature of a product, peculiar to one manufacturer). A brand name item, whether available on one or more schedule contracts, is an item peculiar to one manufacturer. Brand name specifications shall not be used unless the particular brand name, product, or feature is essential to the Government’s requirements, and market research indicates other companies’ similar products, or products lacking the particular feature, do not meet, or cannot be modified to meet, the agency’s needs.” Accordingly, it is technically incorrect to refer to this as a “sole source” award as plaintiffs repeatedly do throughout their brief.

[REDACTED]
[REDACTED]

1. DOI's requirements are rationally based upon valid security concerns

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. AR 169-172.

To help determine the cloud model best suited to its needs, DOI used the basic framework provided in the [REDACTED] [REDACTED]). AR158-168, 549-551. The [REDACTED] is a non-profit organization whose mission is to "[t]o promote the use of best practices for providing security assurance within Cloud Computing." AR158, 305. Under the auspices of the [REDACTED] DOI systematically analyzed its security needs. In the first step of this process, DOI identified the assets it was deploying to the cloud: email messages; instant messages; calendars; schedules; distribution lists; personal contact lists; information stored in Sharepoint portal sites; and programs that handle the aforementioned data. AR159. DOI determined that its assets ranged from mundane intra-office

[REDACTED]
[REDACTED]

communications to “a variety of sensitive information types that can include Federal records and Personally Identifiable Information.” AR159.

In the second step of this process, DOI analyzed the probable impact if its data or programs were somehow compromised. AR159-161. Specifically, DOI examined how the Department would be harmed if: 1) its data were made public; 2) an employee of the cloud provider accessed the data; 3) if its messaging programs were manipulated by an outsider; 4) if its messaging programs stopped working; 5) if its data were unexpectedly changed due to a system failure; or 6) if its data were unavailable for a period of time. Id. DOI determined that, in four of these scenarios, the potential impact to the Department would be very serious - including loss of mission-critical data, court-imposed fines, and improper direction of DOI resources. AR161.

In the third step, DOI assessed its risk tolerance and concluded that it was risk-averse in light of its history and the sensitive nature of the information it maintains. AR164. DOI’s risk aversion is based partially upon *Cobell v. Salazar*, a case in which the United States District Court for the District of Columbia ordered the Secretary of the Interior to disconnect large numbers of DOI employees from the Internet, resulting in a loss of Internet privileges for seven years, i.e., DOI employees could not access the Internet for seven years. AR164. After this experience, DOI has become particularly vigilant to any potential security risks to its data. AR164-65.

DOI next considered the various types of clouds to find a model that fit its security requirements. AR161-66. In weighing the benefits and liabilities of private, community, and

██████████
██████████
██████████” AR161. Nonetheless, given the value of its data and its own low tolerance for risk, DOI determined that a private external cloud represented “an acceptable tradeoff of the benefits, risks and organizational maturity.” AR165.

2. DOI’s determination that its minimum requirements will only be satisfied by a DOI or Federal-only cloud is rationally based upon extensive market research

Plaintiffs allege that DOI’s requirements are irrational because DOI failed to explain “why a community cloud that includes State and local government customers is any less secure than a cloud that includes several Federal government customers.” Pl. Memo. at 29. This argument ignores the significant differences in the legal standards and security requirements for Federal agencies and State or local entities as well as the security issues inherent with sharing information within a cloud of that size and diversity.

The record reflects that DOI insisted on a Federal-only cloud because it wanted to ensure a uniformly high standard for the cloud’s security and a lower risk of sensitive information being released outside of the Federal Government. AR 183. Though State and local governments may employ greater safeguards than commercial companies, these entities nonetheless “do not have the same security requirements as Federal agencies.” AR784. By restricting cloud membership to Federal agencies, DOI can count on the other users meeting basic Federal security requirements. These users will have passed background checks, completed basic information security training, and been instructed to follow Federal data safeguards. They will also be subject to Federal information disclosure laws such as the Federal Trade Secrets Act 18 U.S.C. §1905, the Economic Espionage Act 18 U.S.C. §1831, et seq. , and FOIA 5 U.S.C. §552 (which State

[REDACTED]

and local governments are not held to). Sharing an infrastructure with State and local users increases the risk that sensitive Federal data will be accessed by individuals not governed by Federal information security requirements, statutes, and regulations.

Similarly, DOI possesses a rational basis to determine that State and local governments would not “face the same potential impacts from security issues that DOI would face.” AR784. Like other Federal agencies, DOI must protect data of national importance: Indian trust accounts; information about its own \$12 billion budget; and Departmental policies that touch every state in the Union. AR164-65. The possible consequences of a security breach are sweeping, as evidenced in the seven-year moratorium on Internet use in the aftermath of *Cobell v. Salazar*. AR164. Other Federal agencies can be counted on to take security as seriously as DOI does, because they have a similar stake in protecting their own data. State and local entities simply are not held to the same standard.

Despite Google’s contention, DOI’s security concerns are rational and supported by the record. Indeed, NIST lists security as one of the archetypal attributes for defining membership in a community cloud. AR177 (describing a community cloud as one in which “infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations).” State and local government do not share these security concerns with DOI, at least not to the same extent as Federal agencies. Given the risks inherent in multi-tenant clouds, it is only logical that DOI should require a cloud whose tenants regard security as highly as DOI does. Tenants, it should be noted, who fall within the same organizational structure, the Federal Government.

[REDACTED]

[REDACTED]

3. DOI reasonably relied upon the CSA Guidance in determining its risk tolerance

DOI had good reason to look to the CSA Guidance in its risk assessment. The document was highlighted as one of the two leading guidelines for cloud-specific security in the GAO’s report on cloud computing. AR 705-07. Moreover, neither NIST nor the Office of Management and Budget has developed a strategy to address the information security issues related to cloud computing. AR 163. Given the relative silence of Federal authorities, DOI prudently looked to the CSA as one source of guidance in evaluating its cloud alternatives.

Yet, plaintiffs contend that DOI’s determination is irrational because it relied upon the CSA in its risk assessment and “[t]he CSA Guidance was not designed to be used in the manner described by the DOI in the [Limited Source] Justification.” Pl. Memo. 31. Plaintiffs attempt to support their argument by citing a number of passages from the CSA Guidance. *Id.* Plaintiffs, however, cite the CSA guidance out of context and the record reveals that that DOI used the guide precisely as intended by its authors. For instance, plaintiffs cite the CSA Guidance: “Our goal 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 securely as possibly on your own terms.” Pl. Memo. 31 (citing AR 547). This, however, is exactly how DOI relied upon the CSA Guidance. Indeed, the record is devoid of any evidence suggesting that DOI improperly relied upon the CSA Guidance for specific instructions as to what, where, and how it should move its data to a cloud. Rather, DOI answered the questions posed by the CSA Guidance to determine its minimum requirements. AR159-161. Plaintiffs’ argument also ignores that DOI

[REDACTED]

relied upon comprehensive market research to determine which cloud model best satisfied its email messaging system requirements. AR162-64, 175-185. Lastly, DOI considered its own risk tolerance to ensure that internal stakeholders would be comfortable with the chosen cloud model. AR 165-67. Far from relying upon the CSA Guidance to provide a cookie-cutter solution, DOI used it as a springboard for its own analysis.

Plaintiffs also quote the CSA Guidance as stating that the framework “is not a full risk assessment framework, nor a methodology for determining all your security requirements. It’s a quick method for evaluating your tolerance for moving an asset to various cloud computing models.” Pl. Memo. 31. Again, DOI complied with the CSA Guidance. DOI did not rely upon the CSA Guidance to act as a full risk assessment framework or to determine all its security requirements. To the contrary, during the risk assessment process DOI consulted a wide variety of other sources, including Gartner, NIST, and the GAO. AR175-185. Furthermore, the RFQ requires a full risk assessment and analysis of security requirements once the cloud has been set up. AR817-18. DOI merely used the CSA Guidance as one source to “determine[] its risk tolerance for implementing current solutions in light of its goals, objectives, and mission.” AR847.

The only other item plaintiffs have marshaled to support their unavailing contention is a quote stating that the CSA Guidance “may be used solely for personal, information, non-commercial use.” Pl. Memo. 31 (citing AR 542). This language is taken directly from the copyright boilerplate of the document. AR 542. When the passage is read in this context, it becomes apparent that the text is aimed at controlling how the document is downloaded, linked,

[REDACTED]

and redistributed. It is not to discourage commercial IT professionals from using the CSA Guidance in their work.

4. DOI was not required to follow NIST procedures when selecting its cloud deployment model because they are only applicable to specific security controls and impose baseline requirements rather than a limitation upon a requirement for enhanced security

Plaintiffs argue that DOI should have used NIST procedures in ascertaining its security needs. Pl. Memo. 30-31. Specifically, plaintiffs claim that DOI should have relied upon Federal Information Processing Standards (“FIPS”) 199, FIPS 200, and Special Publication (“SP”) 800-53. *Id.* Plaintiffs contend that these regulations do not call for the enhanced security safeguards required by DOI. *Id.* 31-32.

Plaintiffs’ contentions fail for two reasons. First, FIPS 199, FIPS 200, and SP 800-53 are irrelevant to the decision faced by DOI because they provide highly detailed guidelines for establishing proper security controls for an information system. *See, e.g.*, SP 800-53 at 2-6 (listing eighteen families of security controls, ranging from access control to program management). However, DOI has yet to begin establishing detailed security controls for its information system. Rather, DOI has merely determined the general attributes for its future cloud. AR 847. The NIST provides little insight into this topic and, more importantly, the NIST itself has acknowledged that its guidance is lacking in the area of cloud computing; the organization recently launched an initiative to begin developing standards for this new technology. AR784-85. In any event, DOI fully intends to comply with NIST guidance once the awardee begins to establish its cloud. AR817-18 (requiring compliance with FIPS 199, FIPS

[REDACTED]
[REDACTED]
200, SP 800-53, SP 800-53A, along with seven other FISMA documents after award).

Second, even if DOI were to try to apply the NIST guidance prematurely, the agency would still be free to impose higher standards than required by FIPS 199, FIPS 200, and SP 800-53. The NIST documents dictate a bare minimum level of security measures for Federal 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 foregoing provisions permit and encourage agencies to impose additional requirements to account for their own unique security needs. SP 800-53 at 1-4. 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. Under these circumstances, DOI possessed a rational basis to exceed the requirements outlined in NIST.

5. DOI rationally concluded that cloud-based email messaging is the best way to satisfy its minimum needs

Lastly, plaintiffs challenge DOI’s decision to procure a private external cloud on the grounds that the agency “does not justify why only a cloud-computing deployment would satisfy its objectives.” Pl. Memo. 30. Contrary to this assertion, DOI considered traditional, non-cloud messaging options but deemed them unacceptable. AR752-54. DOI’s market research established that “[REDACTED]

[REDACTED].”

[REDACTED]

AR180. DOI later calculated that it would save \$22.2 million over three years by switching from its traditional email model to a cloud-based messaging service. AR753. Furthermore, the agency found that “the use of a cloud-based e-mail service will result in faster implementation, reduced migration costs, reduced engineering risk, improved levels of service and a predictable cost model on an ongoing basis.” AR754. For these reasons, DOI’s determination that a cloud-based email messaging service best meets its minimum needs is rational.

C. DOI Rationally Concluded That Google Cannot Meet Its Minimum Requirements

DOI fully and fairly considered Google as a viable, competitive alternative to Microsoft BPOS-Federal until Google indicated that it could not and would not meet the agency’s minimum needs. AR150-152, 783-785. The record reflects that DOI met with Google prior to making the challenged standardization decision or approving the justification to conduct a brand-name procurement. In fact, DOI discussed Google Apps with Google in numerous meetings, letters, and emails. See AR3-6, 50-117, 1004-1038. The central theme throughout all these exchanges is that Google is unable and unwilling to meet DOI’s minimum requirements. 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. Again – Google’s approach is better described as a multi-government wide approach, as State and local governments are included within its cloud.

In its June 17, 2010 letter, Google indicated that it “intends to offer messaging services

[REDACTED]

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 multi-government-wide cloud is sufficient to meet the agency’s minimum needs.

DOI also considered Google Apps in its market research. See AR169-172, 279-281, 625-632, 664-674, 678-687, 763-764, 783-785. None of this research even remotely suggests that Google can meet DOI’s requirements. To the contrary, it confirms that Google’s proposed multi-government wide cloud would be open to State and local entities as well as Federal agencies. AR784. In fact, DOI learned that even Google’s local government customers were not satisfied with the security offered by its cloud. AR763-764, 784. The Los Angeles Police Department halted the City of Los Angeles’s migration to Google Apps over security concerns about how Google encrypted and stored their data. AR784. Although this incident involved Google’s commercial cloud, Police Department officials expressed doubts whether a multi-government-only cloud would fully address their concerns. AR764. DOI’s independent market research consultants likewise found that Google was unable to meet DOI’s needs. AR171.

Google’s FISMA certification by GSA did not change DOI’s underlying concerns. The FISMA certification reflects the fact that Google is allowed to store sensitive (not classified)

[REDACTED]

information due to its moderate level of security because the servers are in the United States and only citizens with proper clearance and authority can access them. Despite Google's FISMA announcement, DOI remained concerned because, even though the servers are in the United States, they still host both Federal and non-Federal users with widely divergent security standards. See AR 784-785. Moreover, DOI's research suggested that FISMA certification for clouds is not a full guarantee of security. See AR184, 784-785. Contrary to plaintiffs' implicit contention, the FISMA certification process is not meant to override an individual agency's security needs. AR784-785.

Despite this thoroughly documented analysis, plaintiffs nonetheless assert that Google Apps can meet DOI's minimum needs. Pl. Memo. 30. Plaintiffs contend that Google offered a DOI- or Federal-only cloud in an attachment to its June 17, 2010 letter. Pl. Memo. 29-30. Specifically, plaintiffs cite to a passage which states that Google can provide an underlying infrastructure operated solely for DOI. AR56. Plaintiffs argue that, given this information, DOI should have realized that Google Apps can meet its needs and, therefore, DOI should not have issued the limited source justification. Id.

A close reading of the two-sentence passage reveals that Google was not offering to satisfy DOI's requirements. Rather, Google's response constituted an attempt to redefine DOI's requirement. The plain language of Google's letter supports this: "[t]he service for DOI can be isolated to a single domain run on a logically separate network. Further Google can run service for DOI in a dedicated cloud run for U.S. Government customers only." AR56 (emphasis added). This first sentence does not indicate that Google can meet DOI's needs, because the

[REDACTED]
[REDACTED]

agency unequivocally indicates that it requires a logically and physically separate network.

AR847 (emphasis added). The second sentence also attempts to redefine DOI's needs because it indicates that Google will provide email messaging service on a cloud dedicated to U.S.

Government customers, i.e., Federal, State, and local governments in the United States. This meaning is apparent from the rest of the letter, where Google stated that it would be "arbitrarily exclude[d]" if DOI did not accept its multi-government wide cloud. AR50. In short, this passage did nothing to alter the message that Google articulated to DOI, namely, that it could not meet DOI's needs.

D. DOI Properly Determined That Microsoft BPOS-Federal Is The Only Product Currently Available That Meets DOI's Minimum Requirements And, Therefore, DOI Possessed A Rational Basis To Issue The Limited Source Justification

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 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 its minimum requirements. Pl. Memo. 33-37. All of plaintiffs' arguments are based upon an obvious misunderstanding of BPOS-Federal and DOI's requirements.

1. BPOS-Federal offers a dedicated solution that does not share infrastructure with private parties

Plaintiffs allege that Microsoft BPOS-Federal fails to provide a DOI- or Federal only-cloud that meets DOI's requirements. Pl. Memo. 35. Plaintiffs attempt to support this allegation by relying upon Microsoft press releases which state that BPOS-Federal is "intended to assist US

[REDACTED]
[REDACTED]
Federal government agencies and commercial companies.” Id. (emphasis supplied by plaintiffs).

Plaintiffs reason that if BPOS-Federal is open to both agencies and businesses, it cannot possibly provide a DOI- or Federal-only cloud. Yet this contention is based on a flawed assumption of how BPOS-Federal is administered.

Plaintiffs’ argument presumes that BPOS-Federal is a multi-tenant solution, in which all the customers reside on a single infrastructure. However, BPOS-Federal is delivered as a dedicated single tenant solution. This is evident from the very press release quoted by plaintiffs, which describes BPOS-Federal as a specialized version of BPOS-Dedicated. Pl. Memo. 34. As its name suggests, BPOS-Dedicated is a single-tenant service: the user’s data resides on a private cloud that is dedicated to that particular customer. AR 911-12. This design is also apparent from DOI’s Statement of Work (“SOW”). See AR795-837. Section 10.5 of the SOW specifically calls for a dedicated (i.e., single tenant) implementation of BPOS-Federal. AR816. The awardee is responsible for providing a “[d]edicated computing infrastructure (both physically and logically) to DOI or to DOI and other Federal government customers only.” Id.

In light of the fact that BPOS-Federal is delivered as a single tenant solution, it is plain that there is no conflict between Microsoft’s press releases and DOI’s requirements. DOI commissioned an implementation of BPOS-Federal that is dedicated solely to DOI or other Federal customers. If a private company wants the higher security safeguards of BPOS-Federal, it can likewise commission its own implementation of BPOS-Federal. This implementation would be hosted on a dedicated server that is both logically and physically isolated for that customer. Both DOI and the commercial entity would be using Microsoft BPOS-Federal but

[REDACTED]

nonetheless be on entirely separate clouds. As this example demonstrates, BPOS-Federal is fully compliant with the agency's requirement for a private, DOI-only cloud.

2. DOI's requirement for a dedicated email messaging service through a private external cloud contemplates post-award FISMA certification

Plaintiffs accuse DOI of “excus[ing] or ignor[ing] the inadequacies of the Microsoft product” by permitting Microsoft and the awardee to “obtain[] a FISMA certification after contract award.” Pl. Memo. 35. As noted above, plaintiffs' accusation reflects an obvious misunderstanding of BPOS-Federal.

Pursuant to FISMA, an agency may certify and accredit the security of an information system after testing its controls to ensure they work properly. In soliciting a private external cloud, DOI is requesting offerors to propose implementation of its pre-existing technology to meet DOI's specific needs. Accordingly, it follows that such a cloud cannot possibly obtain certification or accreditation because it has not yet been implemented to meet DOI's needs or actually tested. Thus, the lack of FISMA certification for DOI's personalized cloud is not a sign of lax security, as plaintiffs suggest; rather, it is a necessary step in acquiring a dedicated cloud.

3. Storage of non-messaging data is irrelevant to DOI's security requirements

Plaintiffs allege that both the Microsoft management network and Microsoft Office Live Meeting are not provided on a dedicated infrastructure and, therefore, Microsoft BPOS-Federal does not meet DOI's requirements. Pl. Memo. 35. Plaintiffs allegations miss the substance of DOI's requirements, which are stated in terms of a dedicated messaging infrastructure. AR 167; AR 816. Neither the management network nor Live Meeting contain the sensitive messaging

[REDACTED]
[REDACTED]

data that DOI seeks to secure and therefore, it does not matter if they are hosted on a shared infrastructure. See AR167, 816.

Similarly, plaintiffs contend that BPOS-Federal does not meet DOI's requirements because it archives encrypted emails in a separate, non-dedicated data center. Pl. Memo. 37. This argument overlooks the fact that archiving is not part of the messaging system for which DOI requires a dedicated cloud. Indeed, archival of encrypted email is addressed in an entirely different section of the SOW and is wholly distinct from the security requirements for the messaging system. Compare AR805-806 with 816-822. The agency has imposed separate security measures, including stringent encryption requirements, to protect the archiving data. AR805. Accordingly, plaintiffs' arguments are baseless.

IV. Plaintiffs Have Failed To Demonstrate They Will Suffer Irreparable Harm If This Court Does Not Grant Its Motion For A Preliminary Injunction

A plaintiff must demonstrate irreparable injury in order to obtain injunctive relief and to demonstrate an irreparable injury, a plaintiff must show that without a preliminary injunction it will suffer irreparable harm before a decision can be rendered on the merits. *Heritage of Am., LLC v. United States*, 77 Fed. Cl. 66, 78 (2007). See also *Sierra Military Health Services, Inc. v. United States*, 58 Fed. Cl. 573, 582. In this case, plaintiffs have failed to demonstrate that they will suffer any harm in the absence of a preliminary injunction, let alone irreparable harm.

Plaintiffs contend that if the Court fails to issue a preliminary injunction, they will suffer "severe competitive disadvantage" because they will be denied the opportunity to compete for the procurement. Pl. Memo. 37-38. In support of their contention, plaintiffs rely upon PGBA, LLC

[REDACTED]

v. United States, 57 Fed. Cl. 655, 664 (2003) for the proposition that “[t]his court has acknowledged that a lost opportunity to compete may constitute an irreparable harm....”. Pl. Memo. 37. PGBA, LLC is distinguishable from the case at bar, however, for two reasons. First, PGBA, LLC concerned an agency's override of an automatic stay imposed by the Competition in Contracting Act of 1984, and in its override memorandum, as it was permitted to do, the agency indicated that it would continue the contract even if the Government Accountability Office sustained the protest. Id. at 665. Second, in PGBA, LLC, the protestor was the incumbent contractor and the successful bidder had not begun to perform substantially under the contract. Id. Because of these two differences, this Court should not adopt the reasoning of PGBA, LLC.

Plaintiffs also rely upon *Overstreet Elec. Co. v. United States*, 47 Fed. Cl. 728, 744 (2000) to support the proposition that “a lost opportunity to compete in a fair competitive bidding process for a contract ... has been found sufficient to prove irreparable harm.” Pl. Memo. 37. Similar to PGBA, LLC, *Overstreet* is distinguishable from the case at bar because the Court in *Overstreet* was faced with a judgment upon the administrative record and evaluated the case on the merits. Id. at 729. In this case, the Court is considering plaintiffs’ motion for a preliminary injunction, rather than a motion for judgment upon the administrative record and plaintiffs will not suffer any harm prior to the time the Court will decide the case on the merits.

Plaintiffs’ claims of harm are illusory. First, the Department has shown that its requirements are reasonable and available in the market, thus modification of its requirements is not necessary. Plaintiffs were afforded the full opportunity to explain their capability of satisfying the Department’s requirements as part of DOI’s market research , but Google

[REDACTED]

specifically advised DOI on June 9, 2010, that its products would not and could not meet DOI's requirements for a virtual and physically separate email messaging service. AR151-152. Thus, to the extent that plaintiffs now claim they are harmed by an alleged lost opportunity to compete in the procurement, that harm is a result of Google's intentional refusal to meet DOI's requirements or modify their service to meet the requirement.

Second, any alleged harm to the plaintiffs is belied by the fact that if they are successful on the merits of their claims, this Court will consider issuing a permanent injunction enjoining DOI from proceeding with award of the contract. Although lost competitive advantage may constitute a valid injury, it is not an injury that provides, standing alone, a compelling justification for a preliminary injunction. *Protection Strategies, Inc. v. United States*, 76 Fed. Cl. 225, 236 (2007). Accordingly, any alleged harm to plaintiffs may be alleviated and plaintiffs would, presumably, have the chance to compete in DOI's action. By definition, harm cannot be "irreparable" if it can be alleviated at a later time.

V. Plaintiffs Have Not Demonstrated That The Harm To The Government From Granting The Plaintiffs' Motion For A Preliminary Injunction Would Be Less Than The Harm To Plaintiffs If The Court Denied Plaintiffs' Motion

In deciding whether to grant a preliminary injunction, this Court "balances the harm that the plaintiff would suffer without injunctive relief against the harms a preliminary injunction would inflict upon the defendant and intervenors." *Eskridge Research Corp. v. United States*, 92 Fed. Cl. 88, 100 (2010). "Generally, if the balance tips in favor of defendant, a preliminary injunction is not appropriate." *Akal Security*, 87 Fed. Cl. at 320.

As demonstrated in Section IV, above, plaintiffs have not proven that they will suffer any

[REDACTED]

harm if the Court denies its motion for a preliminary injunction. The Government, however, would suffer harm if the Court grants plaintiffs' motion and enjoins DOI from making award of the contract on January 26, 2010. 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." Attch. A. p.6.² 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. Indeed, if permitted to award the contract on January 26, 2011, 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 preliminary injunction is not appropriate in this case.

² Mr. Corrington's declaration is submitted for the sole purpose of showing the harm to DOI if the Court issues a preliminary injunction in this case and is not supplementing the administrative record. This Court has held that, although limited to the administrative record when reviewing the rationality of an agency's decision, it may consider extra-record evidence in deciding injunctive relief. Holloway & Co., PLLC v. United States, 87 Fed. Cl. 381, 392, n.12 (2009)

[REDACTED]
[REDACTED]

VI. Plaintiffs Have Not Demonstrated That It Is In The Public Interest To Grant Plaintiffs' Motion For A Preliminary Injunction

As plaintiffs observed in their motion for a preliminary injunction, the public interest is served when the integrity of the procurement system is maintained. Pl. Memo. 39 (citing PGBA, LLC, 57 Fed. Cl. at 663). We agree. “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). In this case, plaintiffs have failed to show that the integrity of the procurement system has been compromised by DOI’s July 15, 2010 standardization decision or by the limited source justification approach of the RFQ. Accordingly, it would be excessive judicial infringement upon DOI’s discretion to preliminarily enjoin DOI awarding the contract on January 26, 2010. Additionally, there is a strong public interest in DOI securing the information it is charged with handling and protecting, increasing the quality of its ability to accomplish its mission through more efficient communication between the 13 bureaus that fall within its ambit, and in reducing excessive costs and thereby saving taxpayer dollars.

CONCLUSION

For the foregoing reasons, the Court should deny plaintiffs’ motion for a preliminary injunction.

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

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
Tel: (202) 305-0041
Fax: (202) 305-7644

SHERYL RAKESTRAW
Attorney Advisor
Department of the Interior

November 19, 2010

Attorneys for Defendant

ATTACHMENT A

URGENCY OF AWARDING DOI-WIDE MESSAGING CONTRACT

INTRODUCTION

I am the Chief Technology Officer (CTO) for the United States Department of Interior (DOI). I have over 30 years of experience in the Information Technology (IT) industry having worked as a software engineer, systems architect, project manager, management consultant and entrepreneur in the areas of operating system development, factory automation, information publishing and network security. I am also a Certified Information System Security Professional (CISSP) and a certified Project Management Professional (PMP).

I joined DOI in July 2004 as the Deputy Chief Information Officer (CIO) for the Bureau of Land Management where I oversaw IT operations in support of more than 14,000 end users. My role as the DOI CTO began in an acting capacity in July 2007. In April 2009, I was named permanently to the position. As CTO I am responsible for coordinating the development of DOI technology strategy and architecture across DOI's 13 bureaus and offices and approximately 88,000 end users.

In addition to my role supporting DOI, on June 2, 2010, I was asked by Vivek Kundra, the Chief Information Officer for the Federal Government, to serve as the Chair of the Software as a Service (SaaS) Email Working Group in support of the Federal Cloud Computing Initiative (FCCI). This group serves as the source of cloud-based email information, solutions and processes that foster adoption of cloud-based email services within the Federal Government.

CURRENT STATE OF DOI EMAIL SERVICES

In the modern work environment, e-mail is a fundamental communications tool that is relied upon by virtually all DOI employees, contractors, and constituents. Reliance on email occurs in all aspects of DOI's mission and business functions. As a result, emails sent and received by DOI constituents contain a wide range of sensitive information including:

- Suspicious Activity Reports (SAR) describing possible terrorist activities within DOI-managed lands such as national parks and national monuments
- Information regarding DOI assets such as Hoover Dam that have been identified as National Critical Infrastructure (NCI) under the National Infrastructure Protection Plan (NIPP)
- Law Enforcement information shared with DOI partners such as the Department of Homeland Security (DHS)
- Indian Trust Data that is directly related to DOI's fiduciary responsibilities as the Trustee for American Indians
- Information relating to national energy reserves and energy strategies
- Federal Records and policy decisions that related directly to the Public Trust that is DOI's responsibility to uphold.

Accordingly, the breadth and scope of email makes it a mission-critical function for DOI. However, email services at DOI are not provided by a single system. Instead, each of DOI's 13

bureaus and offices operates their own email system. A series of patchwork technical solutions have been implemented over the years in futile attempts to simulate a single system. Unfortunately, these efforts have been in vain, resulting in a level of email service across DOI that is simply unacceptable. The unacceptable level of email service was immediately obvious to Secretary Salazar who, shortly after his confirmation as Secretary of the Interior in January 2009, referred to DOI's email as being in the "dark ages". Secretary Salazar then made the delivery of an acceptable level of email service a priority for the DOI Office of the Chief Information Officer.

In addition to unacceptable levels of service, the level of security associated with the current patchwork environment is also unacceptable. DOI has received a failing grade on the Congressional Scorecard for IT Security every year since 2005. The DOI Inspector General has also repeatedly cited DOI shortcomings in IT security in their annual Federal Information Security Management Act (FISMA) reports that are submitted to the Office of Management and Budget and Congress. The most comprehensive of these reports was delivered in May of 2008 and presented again to the new political leadership in February of 2009. This report cites the fragmented approach to IT management at DOI as the fundamental cause of unacceptable levels of IT security. DOI's patchwork approach to email is a perfect example of how this flawed management structure weakens IT security.

The best example of security weaknesses created by the current approach to email is DOI's inability to respond to security incidents that are reported by the United States Computer Emergency Response Team (US-CERT). US-CERT is responsible for identifying IT security threats and notifying Federal agencies when specific threats have been identified. The most prevalent types of attacks are various "malware"¹ attacks that are perpetrated through the use of email messages sent to Federal agencies. These malicious emails contain software that is designed to compromise the security of systems within the recipient's organization through a variety of means. When notifications are received from US-CERT for these types of attacks, an immediate response is necessary in order to eliminate the risk associated with the attack. With the single email system that will be enabled by the contract award, a single DOI security professional will be able to implement the appropriate response to US-CERT notifications within a matter of seconds or minutes. Under the current amalgamation of systems, notifications must be forwarded to each bureau email administrator for implementation. As a direct result of the wide variety in email systems in place across DOI, the implementation of appropriate responses takes days or even weeks to implement. The result is an unacceptable exposure of DOI information assets to the most common form of malicious software attacks.

¹ Malware, short for *malicious software*, is software designed to secretly access a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Software is considered to be malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, scareware, crimeware, most rootkits, and other malicious and unwanted software or program. Malware's most common pathway from criminals to users is through the Internet: primarily by e-mail and the World Wide Web . See <http://en.wikipedia.org/wiki/Malware>

URGENCY OF AWARD

Solicitation #503786 was issued to allow DOI to implement a strategic initiative to implement a single email system that will support all of DOI's approximately 88,000 end users. The strategy to deploy a single email system was developed as the most efficient way 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. Without the award of this contract, these operational issues will continue to plague DOI on a daily basis.

Each of the issue areas, Information Security, Mission Performance and Excessive Costs, are described in more detail below.

Information Security

Information security is a fundamental requirement for all Federal agencies, including DOI. The Federal Information Security Management Act (FISMA) establishes baseline standards for information security that must be met by all Federal agencies. DOI has a history of being risk averse when it comes to information technology and security that has led the agency to go beyond these required baselines in order to achieve an acceptable level of risk.

The single email system enabled by the contract award will dramatically improve DOI's security posture. Every day that the contract award is delayed is another day that DOI is not able to benefit from the following information security enhancements:

- **Implementation of a consistent email security architecture:** Currently, DOI's email services are a complex hodgepodge of 13 different systems. The complexity of this environment carries with it a corresponding increase in the complexity of security controls that must be implemented. This increased complexity brings with it an inherent increase in the security risks associated with the amalgamation of the 13 systems. This complexity includes the use of different email products, the use of different versions of these products and inconsistent application of the security updates provided by the vendors of these products. Establishment of a single email system will reduce the overall security risk associated with email by implementing a single, consistent security architecture. Further, the contract calls for around-the-clock security monitoring of the single email system. DOI is not currently able to provide that level of security monitoring for the amalgamated system.
- **Implementation of consistent security policies for mobile devices:** Mobile devices such as Blackberry smartphones bring additional risks to the email environment. The portability that makes these devices so useful also makes them susceptible to loss and theft. Because these devices often contain sensitive information in the form of email messages and attachments, their security is of utmost concern. As noted above, DOI currently operates 13 separate email systems which means there are 13 separate sets of mobile device security policies. Establishing a single email system through this contract award will allow DOI to establish common, consistent security policies for

these devices that include the ability to remotely wipe all data on devices that are reported as lost or stolen.

- **Moving anti-spam and anti-malware filtering off DOI networks:** DOI currently blocks over [REDACTED] email messages per year because they are suspected to contain spam or malware such as computer viruses. This number represents approximately [REDACTED] of all email that is directed to DOI email addresses. As noted above, there is little consistency in the products and technologies that have been used to implement anti-spam and anti-malware capabilities. What is consistent is the implementation of these capabilities on DOI equipment that is directly connected to the DOI network. The single DOI email system will include the implementation of a single anti-spam and anti-malware solution that is not part of the DOI network, but is provided by the vendor instead. The first benefit of this approach is that the inbound flow of email that flows over the DOI network will be reduced by 85%. The second and more important benefit is that more than [REDACTED] email messages that contain spam or malware will never touch DOI networks or systems, which improves the overall security posture for DOI.
- **Faster response to incidents reported by US-CERT:** The United States Computer Emergency Response Team (US-CERT) routinely issues warnings to Federal agencies regarding malware and phishing attacks. When these warnings are received, DOI must forward the warning to the 13 security operations teams that are responsible for each of the 13 email systems that operate within DOI. Each of these teams must then implement appropriate blocks on specific email addresses or attachment types in order to address the reported threat. This greatly reduces response time and increases the risk associated with any one of these incidents. Award of this contract will provide for the establishment of a single interface to the vendor-operated anti-spam and anti-malware system. As a result, a single person will be able to respond to warnings issued by US-CERT by using the vendor's system to implement the appropriate message or sender blocking for all of DOI's users. This will provide for much faster response time and a single, consistent application of the required security response, which greatly improves DOI's security posture in this area.

Mission Performance

In addition to increased security risks, the complex email environment currently in place at DOI is extremely fragile and subject to a variety of operational issues that reduce system availability and performance. Because email is a mission-critical system, operational issues directly impact the ability of DOI to meet its mission requirements. The single email system enabled by the contract award will dramatically improve DOI's mission performance. Every day that the contract award is delayed is another day that DOI is not able to benefit from the following mission performance enhancements:

- **Consistent delivery of email messages:** Each of the 13 email systems that are operated within DOI also represent a single directory or address book of email users. As a result, there is no authoritative directory of email users at DOI. There are also

very complex email routing rules that must be put in place to allow routing of messages from one bureau email system to another. The result of this complex environment is that it is routinely subject to issues such as undelivered email, inability to locate individuals in directories and the delivery of multiple copies of email messages. All of these issues can impact the DOI mission. However, these issues have been most common when attempting to communicate between individual DOI bureaus and the executive leadership within the DOI Office of the Secretary. The result is that the email service outages tend to impact the most senior members of the DOI team which has an increased impact on the ability to achieve the DOI mission.

- **Creation of a single directory of email users:** The contract award will allow the creation of a single email system that leverages the DOI-wide user directory that is currently in place. This will allow that DOI-wide user directory to also serve as the single email directory and eliminate issues with finding users in the directory.
- **Ability to send all-employee messages:** The Secretary of the Interior currently does not have a simple way to send messages to all DOI employees. This directly impacts his ability to communicate with DOI employees and to keep them informed regarding a variety of high-visibility issues, such as the recent Deepwater Horizon Oil Spill. Creation of the single directory of email users described in the previous bullet will also enable the Secretary to send e-mail to all DOI users.
- **System availability:** DOI's current amalgamation of 13 email systems does not have an established performance standard for system uptime. The contract award will establish a system uptime requirement of 99.95%, which equates to less than 25 minutes of system downtime per month.
- **Support for E-Discovery:** DOI's current implementation of email across 13 different systems only includes support for archiving of email to support legal requirements such as E-Discovery for less than half of DOI's user population. As a result, requests for discovery of email documents, implementation of legal holds, etc. are very labor intensive. The single email system that will be enabled by the contract award will include archive of email for legal purposes for all DOI users. This will greatly improve DOI's ability to meet legal requirements for E-Discovery that have been established by the US Department of Justice.

Excessive Costs

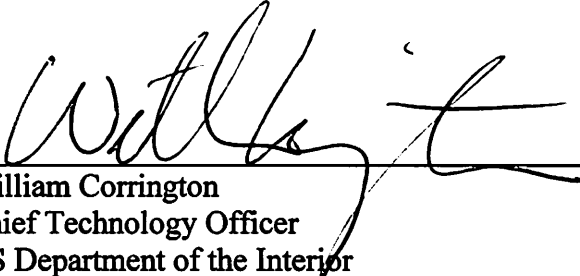
Finally, like all civilian agencies, DOI is facing strict budget cuts, particularly in the area of Information Technology. Implementation of the single email system enabled by the contract award will save DOI \$15M per year or \$1.25M per month over the operational costs associated with the existing amalgamation of 13 email systems. DOI expects to begin realizing these cost savings within three months of contract award. If that award is subsequently terminated for convenience, the cost for termination is estimated at \$1.8M - \$2.1M for three months. As a result, every month the contract award is delayed will cost DOI an additional \$1.25M in excessive operational costs. Achieving the cost savings that will be provided by the single email

system is a critical component of DOI's strategy to meet budget constraints with minimal impact on the DOI mission.

SUMMARY

Solicitation #503786 is 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. Without the award of this contract, these operational issues will continue to plague DOI on a daily basis in the following areas:

- **Information Security:** continuation of increased exposure to information security risks that are created by the existing implementation of 13 emails systems across DOI.
- **Mission Performance:** continued impact on the DOI mission caused by poor system performance that is symptomatic of the existing implementation of 13 emails systems across DOI.
- **Excessive Costs:** ongoing expenditures for email operations that cost DOI \$1.25M per month to operate the existing implementation of 13 emails systems across DOI.


William Corrington
Chief Technology Officer
US Department of the Interior

11/18/2010
Date

CERTIFICATE OF FILING

I hereby certify that on this 19th day of November, 2010, a copy of the foregoing “DEFENDANT'S OPPOSITION TO PLAINTIFFS’ MOTION FOR A PRELIMINARY INJUNCTION” 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/Christopher L. Krafchek