Electronically Filed on December 17, 2010

REDACTED VERSION

IN THE UNITED STATES COURT OF FEDERAL CLAIMS
Bid Protest

GOOGLE, INC,	)	
	)	
and	)	
	)	
ONIX NETWORKING CORPORATION,	)	Case No. 10-743C
	)	
Plaintiffs,	)	Judge Susan G. Braden
	)	
v.	)	
	)	
UNITED STATES OF AMERICA,	)	
	)	
Defendant,	)	
	)	
SOFTCHOICE CORPORATION,	)	
	)	
Intervenor.	)	
	)	

SOFTCHOICE CORPORATION'S OPPOSITION TO PLAINTIFFS' MOTION FOR JUDGMENT UPON THE ADMINISTRATIVE RECORD, AND CROSS-MOTION FOR JUDGMENT UPON THE ADMINISTRATIVE RECORD

William A. Shook
SHOOK DORAN KOEHL LLP
643 E Street, N.E.
Washington, D.C. 20002
Tel: (202) 583-0008
Fax: (202) 280-1097
bill.shook@sdklaw.net

Steven J. Rosenbaum
Counsel of Record
Alan A. Pemberton
Sarah L. Wilson
Scott A. Freling
Shelli L. Calland
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
Tel: (202) 662-5568
Fax: (202) 778-5568
srosenbaum@cov.com

Counsel for Softchoice Corporation

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES

Plaintiffs Google, Inc. and Onix Networking Corporation, each of whom lack standing to bring this pre-award protest, improperly seek to substitute their own views and business judgments regarding the optimal security requirements of a cloud computing system for the Department of the Interior's reasoned and well-documented determination.

DOI's analysis and conclusions are supported by a robust administrative record that refutes Plaintiffs' allegations. After nearly three years of extensive market research and analysis, the Department decided to pursue cloud computing, and defined certain minimum security and other requirements for the cloud. These minimum requirements were based on a comprehensive assessment of the Department's information security demands and its tolerance for risk. The Department thoroughly investigated the existing cloud computing marketplace to identify solutions that could meet each of its minimum requirements. Although the Department gave Google and Microsoft a fair opportunity to meet its requirements, Google failed to do so.

Faced with a substantial record supporting DOI's rational and lawful decisions, and a standard of review that is highly deferential to the government, Plaintiffs resort to accusing agency officials of selectively describing facts, misleading higher-level government officials, and conspiring to prevent fair and open competition. None of these accusations withstand scrutiny.

Plaintiffs' position in this case is directly at odds with the Federal Circuit's recent decision in *Savantage Financial Services, Inc.* v. *United States*, 595 F.3d 1282, 1285 (Fed. Cir. 2010), a case that Plaintiffs simply ignore. Consistent with this binding precedent, this Court should reject Plaintiffs' invitation to allow competitors to dictate the Department's minimum needs. The Department has already determined that Plaintiffs' solution is not sufficiently secure to protect DOI's highly sensitive information, and its rational and well-supported decision must be upheld.

I. COUNTER-STATEMENT OF FACTS.

The procurement at issue in this dispute is designed to solve a longstanding and increasingly critical problem for the agency: unifying and streamlining its email and other messaging systems while simultaneously reducing its risk of data security breaches.

DOI's current email infrastructure consists of a "hodgepodge of 13 systems owned and operated by each bureau and office," and is fraught with operational and security problems. AR 765-66. For several years, DOI has recognized that its email structure was failing to meet the Department's needs. AR 751, 844. In 2003, DOI began the Enterprise Messaging System ("EMS") Initiative to consolidate its decentralized email systems into one system for the entire Department. AR 1. The EMS Initiative, which represented the prevailing Government-wide approach at the time, relied on a systems integrator to custom-build an email system for DOI. AR 751, 844. However, the EMS Initiative ultimately failed, in part due to the complexity of creating an enterprise-wide email system. AR 1, 844.

Following the cancellation of the EMS Initiative in September 2006, the Department's Chief Information Officer ("CIO") directed each DOI bureau and office to migrate from their existing email systems to a standard platform, Microsoft Exchange. AR 1. After several months of waiting for each bureau and office to migrate to the standard platform, the CIO initiated the current effort to reassess the Department's email strategy, to be led by Mr. William Corrington, DOI's Chief Technology Officer ("CTO"), along with representatives from each DOI bureau and office. AR 1-2. Mr. Corrington and his review team were directed "to perform an analysis and to make recommendations about email policy direction" for the Department. AR 2.

A. DOI Establishes The Current Unified Messaging Project.

In late 2007, DOI began to assess the viability of a renewed effort to implement a single messaging system for the entire Department. AR 175. During this assessment, which took place over the next three years, DOI conducted extensive market research that was guided by a number of sources, including independent, expert analysis from Gartner, Inc. ("Gartner"), a leading provider of information technology ("IT") research and analysis; guidance from the National Institute of Standards and Technology ("NIST"), the Cloud Security Alliance ("CSA"), and the Government Accountability Office ("GAO"); and meetings with potential vendors. AR 175-85.

In 2007 and 2008, [redacted] advised that DOI should pursue a consolidated email system for all DOI bureaus and offices, and recommended that a cloud-based system be considered as an alternative to an on-premises implementation, such as the one that DOI previously and unsuccessfully pursued during the EMS Initiative. AR 175-76 (summarizing conversations from November 29, 2007, April 7, 2008, and July 28, 2008).

Cloud computing is a relatively new, and evolving, method for organizations to obtain email and other office automation solutions. AR 436, 752, 847. Rather than purchasing, assembling, and then maintaining its own computer infrastructure (*e.g.*, servers, hard drives, software), an organization can now purchase the desired solution from a vendor who is responsible for all aspects of the system. AR 752. The solution provider then maintains the computer infrastructure (often off-site) and delivers the solution to the organization through the Internet. *Id*. Cloud computing can be deployed in a variety of different models, ranging from a private cloud that is dedicated exclusively to an organization, to a public cloud that is open to all sorts of different customers. AR 162.[1]

In April 2009, DOI formally decided to implement a single, enterprise-wide email system, termed the "Unified Messaging" project. AR 753. DOI again consulted with [redacted] for expert assistance in April and May 2009 to select the appropriate unified email system for DOI to pursue, and in particular to assess the viability of using cloud computing. AR 176-77 (summarizing conversations from April 15, April 27, May 14, and May 28, 2009). [redacted] continued to advocate that DOI consider using a cloud-based email solution, and explained that a principal benefit of cloud computing is the elimination of capital expenditures for hardware and software, and the establishment of a predictable cost model for ongoing operations. AR 176. In addition, [redacted] recommended that the Department's Chief Information Security Officer be engaged in the conversations regarding the possible use of a cloud computing solution, to ensure that any security concerns were addressed as soon as possible. *Id.*

During a conversation on April 27, 2009, [redacted] recommended that DOI only consider Microsoft's single-tenant model for cloud computing, meaning a cloud model with physical infrastructure that is dedicated to a single organization. *Id.* During a subsequent conversation on May 28, 2009, DOI and [redacted] further discussed differences between the single-tenant and multi-tenant models for cloud computing. While [redacted] explained on May 28

[1] The Federal government recently adopted a "Cloud First" policy that will now require agencies to make cloud-based solutions the first choice in any new IT acquisition. In a report issued last week, the U.S. Chief Information Officer explained: "When evaluating options for new IT deployments, OMB will require that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists." Vivek Kundra, *25 Point Implementation Plan to Reform Federal Information Technology Management*, at 7 (Dec. 9, 2010) ("U.S. CIO 25 Point Implementation"), *available at* http://cio.gov/.

that the multi-tenant model, under which an organization shares physical cloud infrastructure with other organizations, may provide better economies of scale, *see* AR 176-77, many of the research reports on cloud computing that [redacted] submitted to DOI for its review identified a number of risks associated with shared infrastructure in a multi-tenant cloud, *see*, *e.g.*, AR Tab 14M ("[redacted]"); AR Tab 14U ("[redacted]"); AR Tab 14R ("[redacted]").

B. DOI's Market Research To Define Its Cloud Computing Requirements, And To Identify Available Solutions.

By the end of May 2009, DOI was seriously considering the implementation of a cloud-based email system, and was exploring the appropriate model for such a cloud. AR 176-177. In June 2009, Mr. Corrington began to develop a "Project Plan" for the Unified Messaging project, to account for the market research that had been conducted to date. AR 180, 753. Mr. Corrington updated this document on numerous occasions between June 2009 and May 2010, *see* AR 1580; it became an evolving document that reflected the progression and development of the market research and analysis conducted by Mr. Corrington. In September 2009, the working Project Plan reflected Mr. Corrington's initial inclination that if the Department were to move to a cloud computing environment, it could only do so with a dedicated computing infrastructure. AR Tab 33.

In the summer of 2009, during his development of the draft Project Plan, Mr. Corrington met with both Google and Microsoft to discuss the Unified Messaging project, and to understand the capabilities of the companies' respective cloud offerings. AR 150, 184. At the time, Microsoft offered two different models of the Business Productivity Online Suite ("BPOS") – BPOS-Standard, a multi-tenant, public cloud, and BPOS-Dedicated, a single-tenant cloud with infrastructure that is dedicated solely to one organization.[2] In contrast, Google only offered Google Apps, a multi-tenant, public cloud with infrastructure that is shared among various cloud users. During DOI's meeting with Microsoft in August 2009, Microsoft confirmed that it could provide a cloud with infrastructure dedicated solely to DOI. AR 184. The record establishes that Google did not, and would not, provide DOI with this same assurance during their meeting with DOI in the summer of 2009. AR 150.

Consistent with DOI's initial market research, the September 28, 2009 version of the draft Project Plan proposed that DOI utilize Microsoft's dedicated cloud offering to deliver a single email system to all DOI users. AR 1098. The Department's research at that point in time had revealed that BPOS-Dedicated was the only available cloud solution that met this requirement.

DOI subsequently requested that [redacted] review the draft Project Plan and provide an independent perspective. AR 180. On October 19, 2009, [redacted] responded to DOI with written feedback on the draft Project Plan, both in the form of general observations (AR 181) and specific comments and suggestions within the document (*see*, *e.g.*, AR 1098). [redacted] advised DOI that [redacted] AR 181.

Also in October 2009, DOI contracted with [redacted] to secure acquisition support for its Unified Messaging project, including eventual

[2] AR 912 [redacted]

market research "to identify and document vendors capable of supporting DOI requirements." AR 1152, 1173. DOI understood that with the complexity and scope of a migration to a consolidated email system and the critical nature of email to the Department's mission, the employees in the DOI program office would require additional support. AR 1172-73.

In addition, DOI officials continued with their own market research, and in particular sought to learn more about the available cloud computing models. Over the ensuing months, DOI officials held several meetings with Microsoft and Google, giving each company the opportunity to offer a cloud computing solution that could satisfy DOI's requirements and in particular its tolerance for information security risk. AR 184. Throughout this research, Mr. Corrington also continued to revise his draft Project Plan. AR 1580.

C. Google Fails To Offer DOI A Dedicated Cloud.

In early February 2010, Mr. Corrington registered to attend a "Federal CIO Briefing" on Google Apps to gain a better understanding of the Google cloud solution. AR 86-87. The Briefing, which was scheduled to take place on February 10, 2010, was cancelled due to winter weather. AR 86. On February 12, 2010, Mr. Corrington contacted Google to express his disappointment that the program had to be cancelled, and suggested that, rather than waiting for the event to be re-scheduled, DOI and Google meet the following week. *Id.*

On February 18, 2010, Mr. Corrington, along with Mr. Bernard Mazer, DOI's Chief Information Officer (who at the time was the CIO for the U.S. Fish and Wildlife Service), and Mr. Andrew Jackson, DOI's Deputy Assistant Secretary for Technology, Information and Business Services, met with Google officials, including the company's Vice President of North America, regarding the planned Unified Messaging project. AR 85, 150. During the meeting, Google advised DOI that Google would not offer a single-tenant cloud. AR 150 ("no single tenant offering would be available").

On April 28, 2010, Mr. Corrington and Mr. Mazer attended a Google Apps Summit for government IT leaders to learn more about the cloud offering that Google could offer to DOI. AR 97-98, 150. After the presentation, Mr. Mazer and Mr. Corrington shared certain security concerns that DOI believed required the Department to implement a cloud solution with a dedicated infrastructure. The Google officials responded by objecting to the premise that DOI required a dedicated cloud, and again refused to offer DOI a dedicated cloud. AR 150.

On May 17, 2010, Google sent a letter to DOI explaining how the Google Apps cloud could meet DOI's needs (as defined by Google), and informing DOI that Google was currently in the process of developing a new cloud solution that would be available to all federal, state, and local government customers in the United States. AR Tab 2.

In response, on May 27, 2010, DOI sent a letter to Google inviting the company to make a presentation to enhance prior market research discussions between DOI and Google. AR Tab 4; *see also* AR 151. The May 27 letter presented Google with a lengthy list of requirements that DOI had identified for the Unified Messaging project, and asked Google to address how the Google Apps solution could meet each of those requirements. AR 47-48. Among the many requirements was the "[a]bility to provide an underlying infrastructure that is operated solely for DOI." AR 47.

On June 9, 2010, Google made a detailed presentation to several DOI officials, including Mr. Jackson, Mr. Mazer, and Mr. Corrington,[3] on the Google Apps solution, describing

[3] Mr. Jackson, Mr. Mazer, and Mr. Corrington were joined at the meeting by DOI contracting officials. AR 151.

at a high level how Google believed that its cloud offering met all of DOI's requirements. AR 151. However, when DOI specifically asked Google about whether the company was able to provide the service on a dedicated infrastructure, Google again replied that it was "incapable of supporting a dedicated solution and proceeded to argue against the merits of a dedicated infrastructure." *Id.* Google further explained that [redacted] *Id.*

After the meeting, on June 17, 2010, Google sent another letter to DOI that argued that the Department was defining its requirements too narrowly and continued specifically to object to DOI's expressed preference for a dedicated cloud with a physically isolated computing infrastructure. AR Tab 5.

D. DOI Initiates A Proof Of Concept Study For The Unified Messaging Project.

In contrast to Google, Microsoft repeatedly assured DOI that Microsoft could provide a cloud computing solution with infrastructure that is dedicated solely to DOI. *See*, *e.g.*, AR 184 (noting that in August 2009, Microsoft confirmed that it could offer "email services that were deployed on computing infrastructure that was dedicated to DOI"). As was the case with Google, DOI officials met with Microsoft on a number of occasions in late 2009 and early 2010 to understand the company's cloud offerings, and to assess whether these offerings could meet each of DOI's minimum requirements. *See*, *e.g.*, AR 1039-41, 1069.

In February 2010, Microsoft publicly announced plans to offer BPOS-Federal, a cloud computing solution specifically for the Federal government. BPOS-Federal is a modified version of Microsoft's existing BPOS-Dedicated cloud, with additional enhancements to meet the privacy and security requirements of the Federal government. Like BPOS-Dedicated, BPOS-Federal offers a dedicated cloud infrastructure that is not shared with other organizations.[4]

On June 14, 2010, [redacted] DOI initiated a Proof of Concept study to confirm that migrating to a cloud-based email system was indeed a viable approach for DOI. AR 176, 859. Under the Proof of Concept study, DOI contracted with Dell to migrate 5,000 email users in the Bureau of Indian Affairs to a BPOS-Federal cloud. AR Tab 31. DOI conditioned its moving forward with an enterprise-wide cloud procurement upon the "successful completion" of the Proof of Concept study. AR 1003.1.

E. DOI Finalizes Its Market Research And Risk Assessment.

On June 25, 2010, Mr. Corrington again consulted with [redacted] to discuss the levels of risk associated with the various cloud models. [redacted] advised that a multi-tenant cloud structure is [redacted] AR 177. [redacted] further explained that there is [redacted] *Id.*

On June 28, 2010, Mr. Corrington and DOI's Chief Information Security Officer, Lawrence Ruffin, completed a risk assessment of cloud deployment models. AR Tab 11. During this risk assessment, DOI examined the different cloud computing models, explaining:

[redacted]

[4] *See* Microsoft Press Release, *Microsoft Unveils New Government Cloud Offerings at Eighth Annual Public Sector CIO Summit*, Feb. 24, 2010, *available at* http://www.microsoft.com/Presspass/ press/2010/feb10/02-24CIOSummitPR.mspx.

AR 162.[5] DOI considered [redacted] AR 163-64. DOI then examined [redacted] AR 164-66. As a result, DOI [redacted] AR 166-68.

F. DOI Concludes That BPOS-Federal Is The Only Cloud Solution That Meets Its Requirements, And Proceeds To Implement The Unified Messaging Project.

On June 29, 2010, [redacted] completed a market research analysis for DOI. During its research, [redacted] considered thirteen firms that provide messaging systems, including Microsoft and Google, to determine if each firm was capable of meeting the Department's requirements, including the requirement for either a DOI-only or a Federal-only cloud. AR 169-72. [redacted] concluded that only Microsoft's BPOS-Federal met all of DOI's requirements. AR 171. In particular, [redacted] determined that Google was unable to meet DOI's requirement for an external, private cloud. *Id.* This independent research confirmed internal research conducted by DOI.

On July 15, 2010, DOI's Assistant Secretary for Policy, Management and Budget approved a standardization decision to establish BPOS-Federal as the Department-wide standard

[5] DOI also considered [redacted] AR 162.

for messaging services. AR 748-56. The standardization decision considered the research and analysis conducted by DOI, [redacted], and [redacted] over the prior three years, including the risk assessment performed by Mr. Corrington and Mr. Ruffin on the cloud computing models and their identification of the Department's risk tolerance. AR 752-56. The standardization decision confirmed that DOI "requires the use of an external private cloud deployment model to meet security and risk tolerance requirements," and concluded that "BPOS-Federal is the only available standard service offering that meets all of DOI's requirements." AR 756.

On August 30, 2010, DOI issued a Limited Source Justification in accordance with Federal Acquisition Regulation ("FAR") Subpart 8.4 to limit competition to resellers of BPOS-Federal. The Limited Source Justification, which was approved by the Contracting Officer, the Competition Advocate, the Head of the Contracting Activity, and the Senior Procurement Executive, explained that through its market research, DOI had determined that "although many companies can provide messaging services in general, they either cannot provide services that address the complexity of messaging requirements within DOI, or they could not meet the degree of security required by DOI." AR 848. The Limited Source Justification also made clear that "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." AR 849.[6]

Shortly after DOI's standardization decision, Google publicly announced the availability of its planned government-wide cloud (consisting of infrastructure that is shared

[6] In other words, DOI has not adopted a "once Microsoft, forever Microsoft" attitude as alleged by Plaintiffs, (Pls. Br. at 32), but rather has committed to continuing to evaluate viable alternatives as they become available.

among federal, state, and local government customers), and also publicly announced that this cloud had received certification from the General Services Administration ("GSA") pursuant to the Federal Information Security Management Act ("FISMA"). *See*, *e.g.*, AR 783 (referencing Google's website announcement of the availability of Google Apps for Government); *see also* Attach. 1 hereto, *cited in* AR 783 ("Google Apps for Government, now with FISMA certification."). In response to this Google announcement – [redacted] [redacted],[7] DOI conducted supplemental market research to assess the impact of these two announcements on the Department's prior decision to implement a unified messaging system using BPOS-Federal. AR Tab 21. On August 20, 2010, Mr. Corrington and Mr. Mazer completed this supplemental market research and concluded that Google's recent announcements did not warrant a change in the July 15, 2010 standardization decision because Google's government-wide cloud continued to present an unacceptable risk to DOI. AR 784. This supplemental market research was then presented to Mr. Jackson and Ms. Debra Glass, Chief of DOI's Acquisition Management Division IV. AR 783.

On August 30, 2010, utilizing GSA's public E-Buy system, DOI issued Request for Quotations No. 503786 (the "RFQ") to solicit quotes for the acquisition of hosted messaging and collaboration services using a BPOS-Federal solution to support approximately 88,000 users across all DOI bureaus and offices. AR 786, 799. The RFQ was issued pursuant to FAR Subpart 8.4 and the August 30, 2010 Limited Source Justification, and contemplated the

[7] As the Government has pointed out in its cross-motion for judgment upon the administrative record, [redacted] (Gov't Cross-Mot. at p. 13 n.3, p. 38 n.13, Attachs. 1-5.)

competitive award of a single, firm-fixed-price Blanket Purchase Agreement to a Schedule 70 contract holder. AR 804. The RFQ required that offerors submit their quotes to DOI on or before September 13, 2010. AR 854.

On October 29, 2010, Plaintiffs filed this pre-award protest of the Department's decision to limit competition for its requirements to resellers of BPOS-Federal, alleging that DOI established requirements that exceed its own minimum needs in order to justify a decision to standardize on a BPOS-Federal solution and exclude other cloud computing services from consideration.

II. STANDARD OF REVIEW.

DOI's Limited Source Justification may not be set aside unless it is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law. *See Savantage Fin. Servs., Inc.* v. *United States*, 595 F.3d 1282, 1285 (Fed. Cir. 2010); *see also* 28 U.S.C. § 1491(b)(4); 5 U.S.C. §§ 702 & 706(2)(A). Under this standard, DOI's decision "is entitled to a presumption of regularity, and the agency's action must be upheld as long as a rational basis is articulated and relevant factors are considered." *Emery Worldwide Airlines, Inc.* v. *United States*, 264 F.3d 1071, 1085 (Fed. Cir. 2001) (citations and internal quotation marks omitted). Contracting officers may "exercise discretion upon a broad range of issues confronting them" in the procurement process. *Impresa Construzioni Geom. Domenico Garufi* v. *United States*, 238 F.3d 1324, 1332 (Fed. Cir. 2001) (citations & internal quotation marks omitted).

Accordingly, procurement decisions such as this one "invoke[] 'highly deferential' rational basis review." *CHE Consulting, Inc.* v. *United States*, 552 F.3d 1351, 1354 (Fed. Cir. 2008) (citations omitted). "This standard requires a reviewing court to sustain an agency action evincing rational reasoning and consideration of relevant factors." *Advanced Data Concepts, Inc.* v. *United States*, 216 F.3d 1054, 1058 (Fed. Cir. 2000). This deferential standard also "recognizes the possibility of 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 decisionmaking.'" *Wit Assocs., Inc.* v. *United States*, 62 Fed. Cl. 657, 660 (2004) (quoting *Baltimore Gas & Elec. Co.* v. *Natural Res. Def. Council, Inc.*, 462 U.S. 87, 105 (1983)).

III. DOI'S DECISION TO LIMIT COMPETITION TO BPOS-FEDERAL WAS RATIONAL AND SHOULD NOT BE DISTURBED.

Plaintiffs' assertion that the Limited Source Justification renders the solicitation an "improper sole-source procurement" (Pls. Br. at 28)[8] is legally unsupported. The FAR expressly provides that a procuring agency may restrict consideration to an "item peculiar to one manufacturer" under certain circumstances. FAR 8.405-6(a)(2). Specifically, a procuring agency placing an order on the Federal Supply Schedule 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." *Id.* This is precisely the situation in this case – DOI determined through extensive and well-documented market research that BPOS-Federal is the only solution that meets its needs, because it is the only solution that provides a unified and consolidated email system hosted in a cloud that is physically and logically dedicated solely to Federal government departments and agencies.

A. DOI Is Entitled To Determine Its Own Minimum Needs.

DOI is best suited to determine its own minimum needs, and the law affords it substantial discretion to do so. As the Federal Circuit made clear in *Savantage* – a decision that

[8] "Pls. Br." refers to Plaintiffs' motion for judgment upon the administrative record.

again is entirely absent from Plaintiffs' brief[9] – "competitors do not dictate an agency's minimum needs, the agency does. And 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." *Savantage*, 595 F.3d at 1286 (citations and internal quotation marks omitted; alteration in original); *see also Coastal Int'l Sec., Inc.* v. *United States*, 93 Fed. Cl. 502, 541 (2010) (although a bid protestor may disagree with the agency's methodology for ascertaining its needs, "this is not a basis for overturning an agency's determination of its own needs") (citing *Savantage*, 595 F.3d at 1286) (Braden, J.).

Given DOI's unique understanding of the highly sensitive nature and value of its data and the events that have led it to be particularly risk-averse, Plaintiffs have no proper basis to ask this Court to substitute its technical judgment for that of DOI. *See Coastal Int'l Sec.*, 93 Fed. Cl. at 544 ("As a matter of law, if the agency's explanation reflects rational reasoning and consideration of relevant [agency] factors, the court is required to defer to the agency's decision, even if it is one the court would have determined differently.") (citations and internal quotation marks omitted; alteration in original) (Braden, J.).

B. DOI Reasonably Concluded That A Federal-Only Cloud Is Necessary To Protect DOI's Uniquely Sensitive And Confidential Data.

DOI's decision to require a Federal-only cloud-based messaging system that excluded state agencies, local agencies, and the public was entirely rational and based on DOI's legitimate interests in safeguarding its highly confidential data.

[9] Plaintiffs have thus far ignored the *Savantage* decision, even though Softchoice and the Government cited to the decision at length in their briefs opposing Plaintiffs' motion for a preliminary injunction, and even though Plaintiffs' counsel represented the (unsuccessful) protestor in that case.

1. It Was Rational For DOI To Focus On Security When It Considered Various Cloud Computing Models.

The record demonstrates that DOI is reasonably concerned about the security of its data and has sought to assess and minimize the risks that transitioning to a new cloud-computing system would pose to these data. *See*, *e.g.*, AR 164-65, 845. As noted in the Limited Source Justification, DOI is responsible for a significant amount of sensitive and confidential data. AR 845. These data include information related to DOI's management of tribal trust funds and Individual Indian Money accounts; procurement and business communications; information relating to DOI's law enforcement, investigative, and resource protection and management authorities; "personally identifiable information"; and other sensitive internal government communications. AR 845, 847; *see also* AR 159.

Given DOI's acute and well-publicized problems with its computer systems in the past, its persistent emphasis on security from the start of this project is entirely reasonable. DOI's IT infrastructure has been the subject of sharp criticism, particularly with regard to security vulnerabilities. For example, a 2008 report by the DOI's Inspector General described recent security breaches of DOI computer systems, and explained that DOI's current strategy of a decentralized IT management structure was not working. AR 1198-99, 1202-05.[10] Indeed, DOI has repeatedly received failing grades from the United States House of Representatives Committee on Oversight and Government Reform ("House Oversight Committee") for its lack of computer security. AR 1344, 1346 (reflecting F grades for 2003, 2005, 2006, and 2007; reflecting a D+ grade for 2004). The security of DOI's IT systems has also been criticized by the

[10] The record reflects that at least since 2005, the Inspector General has authored similar critiques of the Department's IT system, and in particular its security vulnerabilities. *See*, *e.g.*, AR 1379 (Oct. 2005 report); AR 1438 (Sept. 2006 report); AR 1470 (Sept. 2007), AR 1496 (Sept. 2008); AR 1536 (Nov. 2009).

Federal courts. Between 2001 and 2005, a Federal district judge issued multiple orders directing DOI to shut down a significant portion of its Internet connections based on findings that DOI's systems were insufficient to secure against external threats. *See Cobell* v. *Norton*, 394 F. Supp. 2d 164 (D.D.C. 2005), *vacated by Cobell* v. *Kempthorne*, 455 F.3d 301 (D.C. Cir. 2006).[11] These orders left more than 5,000 DOI computer users without the ability to access the Internet or to exchange email with external entities for almost seven years.

On the basis of these incidents, DOI concluded that security failures in the cloud could lead to very serious problems, such as loss of mission-critical data, court-imposed fines, improper direction of DOI resources and personnel, and damage to DOI's reputation. AR 159-61. DOI also determined that it is risk-averse and that its tolerance for risk is low, based in part on its experience in the *Cobell* lawsuit. AR 164-66 ("[T]he specter of a return to a disconnected state influences many of the decisions that are made regarding risk and information technology security."). DOI therefore concentrated on finding a cloud model that was best suited to address these concerns about security and to minimize the risk to DOI's data.

2. DOI's Market Research Supported DOI's Final Determination That The More Tenants A Cloud Has, The Less Secure It Is.

Contrary to Plaintiffs' assertion that DOI misleadingly "cherry-picked certain statements from certain reports" so that it could build a case in favor of some pre-determined end result (Pls. Br. at 35), DOI's analysis reflects the consensus among the experts and reports DOI consulted – that larger clouds are less secure than smaller clouds. Plaintiffs can point to nothing in the record that contradicts this basic conclusion.

[11] *See also* John Files, *For 4th Time, Judge Seeks to Shield Indian Data*, The New York Times, Oct. 25, 2005 (reporting that for the fourth time since 2001, the U.S. District Court for the District of Columbia had ordered DOI to disconnect certain of its computers from the Internet because of data security concerns).

Plaintiffs also do not dispute the necessity or propriety of DOI's focus on security. Instead, Plaintiffs quibble about DOI's mastery of cloud terminology and claim that counsel has "blurred the distinctions among defined cloud models." (Pls. Br. at 37.) Yet the distinctions among defined cloud models are, in fact, blurred. Cloud computing is an emerging and developing technology where definitions are not yet firm and settled. AR 436 ([redacted]). Different groups use different language to describe various types of clouds. Even within a single group's categories, there is substantial room for interpretation. For instance, NIST's definition of a "private" cloud is one that is "operated solely for an organization," but it is unclear what constitutes an "organization." AR 437. The Federal government might well qualify as a single organization under the current NIST definition.

Rather than relying on labels and definitions that may shift or become obsolete, DOI used its June 29, 2010 Risk Assessment to analyze the underlying substance of its extensive market research. AR 167 ([redacted]). That market research clearly supported DOI's conclusion that as clouds grow larger and service more "tenants," they become less secure. Conversely, clouds that are dedicated to one organization or a finite group of related organizations are more secure than clouds open to unlimited numbers of organizations that do not necessarily share the same interests or priorities. AR 163-164.[12]

NIST, for example, has stated that "private clouds may have less threat exposure than community clouds which have less threat exposure than public clouds." AR 163 (quoting NIST, *Effectively and Securely Using the Cloud Computing Paradigm*, Oct. 7, 2009); *see also* AR 182 (same); AR 471. The independent GAO similarly reported that "[m]ultitenancy and use of shared resources can also increase risk. . . . because one customer could intentionally or unintentionally gain access to another customer's data, causing a release of sensitive information." AR 183 (quoting GAO, *Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing*, Report No. GAO-10-513, May 2010); AR 716. [redacted] likewise advised that the inherent complexities associated with admitting additional tenants to a cloud leads to increased risks, and [redacted] concurred with DOI's [redacted]. AR 163, 177, 180, 1148; *see also* AR 31 (NIST: cloud models have "differing tradeoffs between threat exposure and efficiency").

[12] Plaintiffs' only attack on the Risk Assessment is falsely to accuse DOI of "selectively quot[ing] statements, and tak[ing] others out of context." (Pls. Br. at 39-42.) First, Plaintiffs are the ones who are guilty of "selectively quoting statements and taking others out of context" by ignoring three full paragraphs of the Risk Assessment that deal specifically with the perils of introducing additional tenants to a cloud. AR 163. Plaintiffs instead skip to DOI's discussion of the security concerns involved in ceding control of sensitive data to cloud operators, which is a different topic. Second, there is nothing deceptive about DOI choosing to emphasize the portions of market research that are important to it, particularly when the original sources are all cited directly in the Risk Assessment.

3. DOI Reasonably Decided That Only A DOI-Only Cloud Or A Federal-Only Cloud Would Meet Its Needs.

With these security considerations in mind, DOI carefully weighed the relative advantages and disadvantages of various cloud models, and rationally decided that only a cloud dedicated solely to DOI or to DOI and other Federal government customers (*i.e.*, a Federal-only cloud) would provide the level of protection and control necessary to safeguard DOI's sensitive and confidential data. AR 167; *see also* AR 783 ("[O]ne of the major elements supporting the standardization decision was Microsoft BPOS-Federal's ability to provide a dedicated computing infrastructure to support stringent DOI requirements."). In particular, DOI balanced the economies of scale of a public or near-public cloud against the enhanced security of a dedicated cloud, and concluded that only a DOI-dedicated or Federal-only cloud that was physically and logically isolated from the infrastructure of other customers of the cloud provider "represent[ed] an acceptable tradeoff of the benefits, risks and organizational maturity." AR 167. This analysis was a reasonable exercise of the agency's discretion and should not be disturbed. *See Savantage*, 595 F.3d at 1286; *Costal Int'l Sec.*, 93 Fed. Cl. at 544.

This case is virtually identical to *Savantage*, in which the Department of Homeland Security ("DHS") decided to implement a financial management software system that was pre-integrated with other key systems rather than to build a system by beginning with a core financial system and then integrating other systems piece by piece. Even though the Savantage protestor argued that creating a fully integrated system at the outset was more difficult and therefore more likely to fail than integrating peripheral systems one at a time into a core system, the Federal Circuit held that, on a technical question about how best to construct an agency-wide computer system, "an agency's preferences are entitled to great weight." *Savantage*, 595 F.3d at 1286. Just like DHS in *Savantage*, DOI has relied on its past experiences to evaluate how best to consolidate its many fractured and incompatible email systems into one, and DOI's preferences on how to structure its cloud, what is in its cloud, and who else may be physically or electronically connected to its cloud should similarly be "entitled to great weight."

Unable to undermine DOI's sound and well-documented reasoning, Plaintiffs' brief is filled with a series of weak and ineffective efforts to poke holes in DOI's logic. For example, Plaintiffs criticize DOI's use of the five-step analysis recommended by the CSA, a non-profit organization whose mission is to "promote the use of best practices for providing security assurance within Cloud Computing." AR 158-68; *see also* AR 549-51. In fact, DOI used the CSA method in precisely the manner in which it was intended to be used – as a flexible tool to help DOI assess the value of its data, gauge its tolerance for risk, and determine which cloud model would be most appropriate for DOI's specialized needs. There is no reason to think that the CSA method is worthless if it is not applied in a mechanical, rigid, formalistic way. Indeed, the CSA itself states repeatedly that its 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 as securely as possible, on your own terms," AR 547, and that its five-step analysis is merely "a quick method for evaluating your tolerance for moving an asset to various cloud computing models." AR 549.

Furthermore, although Plaintiffs claim that DOI applied the CSA's framework "incorrectly" because DOI did not go through each of its assets one at a time to evaluate DOI's risk tolerance with respect to that particular asset (*see* Pls. Br. at 41), DOI stated quite clearly in the Risk Assessment that it was purposefully zeroing in on its most sensitive data because those were the data that would dictate how restrictive DOI's cloud would have to be. AR 159 [redacted]

[redacted]

[redacted] Moreover, it is absurd to suggest that DOI should have considered obtaining different kinds of clouds for different assets; that kind of fragmentation is precisely what DOI's new consolidated messaging system was intended to avoid.

In reality, it is irrefutable that DOI's market research was rigorous and comprehensive. DOI conducted thorough and wide-ranging research on various cloud models for years and consulted numerous experts, articles, and reports; met with vendors; and hired independent third parties to examine available products.[13] AR 175-85. In particular, DOI studied nearly 600 pages of industry reports discussing cloud computing and enterprise messaging (AR 186-747), spoke to [redacted] on at least eight separate occasions (AR 175-77), communicated extensively with both Google and Microsoft (AR 3-6, 47-49, 50-58, 59-117, 150-52, 1004-90), and created its own summary and evaluation of the information acquired through this market research (AR 175-85). This painstaking work in turn created a very robust administrative record replete with support for DOI's decisions. More importantly, as the Federal Circuit recently held, the administrative record does not need to contain evidence to counter all of a plaintiff's post hoc criticisms. *See Savantage*, 595 F.3d at 1287 ("DHS was not required to synthesize its thinking and its market research into a prelitigation written explanation of the rationale for each of the solicitation requirements.").

[13] Although Plaintiffs also condemn the [redacted] analysis at length, (*see* Pls. Br. at 34-35), [redacted]'s report simply confirmed what Plaintiffs have effectively conceded – that Google failed, and indeed refused, to satisfy DOI's requirements because Google would not create a physically and logically isolated Federal-only cloud in accordance with DOI's specifications. AR 184 (Google reiterated that it was "incapable of supporting a dedicated solution"); *see also* AR 185 (Google insisted that a Federal-only cloud was not necessary, "argu[ing] against the merits of a dedicated infrastructure" and attempting to substitute Google's assessment of how best to meet DOI's needs for the agency's own judgment).

4. DOI Considered And Reasonably Rejected Google's Federal, State, And Local Government-Wide Cloud.

Rather than providing actual evidence that DOI does not require a DOI-only or Federal-only cloud, Plaintiffs expect the Court (and DOI) merely to take their word that Google's government-wide cloud is just as secure as a Federal-only cloud. Moreover, Plaintiffs' contention that DOI never justified its decision to require a cloud limited to the Federal government rather than a cloud open to federal, state, and local governments (*i.e.*, a government-wide cloud), (*see* Pls. Br. at 42-46), is inaccurate.

As an initial matter, it is simply false 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." (*Id.* at 42.) The record demonstrates that DOI examined precisely this issue and rejected Google's government-wide cloud as not sufficiently secure. AR 783-85. This determination is clearly rational for a security-conscious user such as DOI, because other Federal agencies, unlike the state governments and thousands of local governments, are faced with similar security concerns and legal requirements, may suffer the same nationwide consequences of a security breach, and are thus likely to value and comply with security requirements at the same high level as DOI.

Google announced the availability of its government-wide cloud on July 22, 2010. Until then, there was no reason for DOI formally to evaluate Google's government-wide cloud offering, because that cloud offering did not yet exist, or was at best incomplete. AR 185 (June 9, 2010: [redacted] ;

see also AR 5 (May 17, 2010: "Google Apps is currently developing a Government-only cloud environment available only for federal, state, and local U.S. government customers. This Government-only cloud, planned to be operational in time for this procurement, would be hosted completely within the U.S., including the primary and backup sites.") (emphasis added); AR 115 (June 24, 2010: [redacted]) (emphasis added). There is no reason to require agencies such as DOI to consider hypothetical aspirational solutions that may not ever move beyond the conceptual stage, or may not be ready by the time the agency must act.

Nevertheless, even though Google's announcement of its government-wide cloud occurred after DOI had already established BPOS-Federal as the departmental standard for messaging and collaboration services, DOI still conducted supplemental market research, provided Google with an opportunity to explain its position, and comprehensively analyzed whether the existence of Google's government-wide cloud warranted a modification of the decision. AR 47-49, 151, 783-85. In the memorandum summarizing its assessment, DOI concluded that continuing to require a Federal-only cloud was justified, primarily because Google's "announcements [did] not indicate that there was any change to the Google Apps' architecture which is a multi-tenant model." AR 784. The potential inclusion of state and local governments – from the Yuma County Water Authority to the Los Angeles Sanitation Department – in the government-wide cloud "remains an issue," because those "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.* Furthermore, while the universe of

Federal entities that could populate a Federal-only cloud is relatively limited, the number of state or local entities that could participate in a government-wide cloud is virtually infinite.[14]

By restricting the cloud to Federal agencies, DOI has ensured that the other cloud users will be obligated to comply with fundamental Federal security requirements, such as background checks and basic information security training, and are subject to Federal laws governing the disclosure of confidential information. *See*, *e.g.*, the Trade Secrets Act, 18 U.S.C. § 1905 (a criminal statute which prohibits Federal government employees from disclosing confidential commercial and financial information to the public).[15] There is no guarantee that state and local governments have instituted similar requirements.

In addition, DOI understands that other Federal agencies – which, like DOI, protect data of national importance – take security as seriously as does DOI. Among other issues, Federal agencies and not state and local agencies must comply with FISMA, which is intended to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets." 44 U.S.C. § 3541 (emphasis added). State and local agencies do not necessarily place, and do not have the same requirements to place, such a premium on security. DOI's choice to exclude

[14] According to the U.S. Census Bureau, there were 89,476 local governments in the United States in 2007, which was 1,951 more than the number of local governments in 2002. *See* U.S. Census Bureau, *Table 416: Number of Governmental Units by Type: 1962 to 2007*, *available at* http://www.census.gov/compendia/statab/2010/tables/10s0416.pdf.

[15] Whether or not DOI has a "right of action to force another Federal agency to maintain any security controls or to not disclose 'trade secret' information," (Pls. Br. at 43), is irrelevant. Federal employees are subject to the Trade Secrets Act and its criminal penalties, and are therefore much more likely to take precautions and demand security mechanisms – and less likely to "mistakenly send a sensitive e-mail to the wrong person(s)," (*id.* at 44) – than an employee of the Los Angeles Sanitation Department. It is perfectly reasonable for DOI to want to maximize the chances that other members of its cloud care as much about security as DOI does.

state and local agencies from its cloud is hardly irrational, especially given that NIST lists "security requirements" as an attribute that should be shared by the members of a community cloud. AR 755. These are not "retroactive justifications" concocted by counsel, and there is no "yawning gap" in the record. (Pls. Br. at 42.) Rather, these reasons to exclude state and local governments from DOI's cloud are clearly spelled out in the administrative record. AR 783-85.

Furthermore, it was entirely proper for DOI to take into account the difficulties that the City of Los Angeles – a client that Google touted in its June 17, 2010 letter to DOI, AR 53 – was experiencing in July 2010 during its "highly-publicized implementation of Google Apps." AR 784. Many of these difficulties were related to the Los Angeles Police Department's "security concerns about Google Apps," which were "the primary culprit for the delay." *Id.* (quoting David Hubler, *Google's LA Cloud Turns Into a Summer Squall*, Washington Technology, July 26, 2010).[16] In particular, "the law enforcement agency expressed concerns about Google Apps' data encryption, 'segregation of city data from other data maintained by Google,' and background checks for Google employees with access to police department information." *Id.*; *see also* AR 179 ("'Consequently, while Google Apps is now sufficiently secure for less-demanding enterprises, some organizations will not be satisfied – in particular, extremely security-conscious organizations . . . .'") (quoting Matthew W. Cain & Monica Basso,

[16] Contrary to Plaintiffs' suggestion (Pls. Br. at 45-46), there was no requirement that DOI "establish the truth or accuracy" of this published article – which was provided to them by their expert [redacted], *see* AR 763-64 – before considering it. Nonetheless, had DOI done so, it would have discovered a number of other articles describing these security concerns with Google Apps. *See*, *e.g.*, Tom Bradley, *Google Apps Project Delays Highlight Cloud Security Concerns*, PC World, July 26, 2010, *available at* http://www.itworld.com/print/115307; Andrew R. Hickey, *Security Fears Delay Google, CSC Cloud Computing Project in L.A.*, CRN Technology News, July 23, 2010, *available at* http://www.crn.com/news/security/226200161/security-fears-delay-google-csc-cloud-computing-project-in-l-a.htm; John Letzing, *Google Misses Deadline for High-Profile L.A. Contract*, MarketWatch, July 23, 2010, *available at* http://www.marketwatch.com/story/google-misses-deadline-in-high-profile-la-deal-2010-07-23.

Google Bids for Enterprise E-Mail with New Mobile Features, Feb. 5, 2010); AR 627. DOI reasonably worried that these security vulnerabilities would be present in any of Google's non-dedicated clouds, even if such a cloud only served federal, state, and local governments, and noted that these were exactly the considerations that led it to identify its need for a DOI-only or Federal-only cloud. AR 784.

5. DOI Reasonably Treated FISMA As A Security Floor, Not A Security Ceiling.

There is no merit to Plaintiffs' argument that FISMA and its accompanying NIST guidance somehow set a ceiling on security, and that any additional precautions intended to safeguard an agency's data are unnecessary and irrational. (Pls. Br. at 46-48.) Rather, FISMA and the NIST guidance establish a minimum level of security for Federal information systems that may be heightened in accordance with an agency's specific needs. Indeed, the NIST publications expressly permit and even encourage agencies to supplement these minimum security measures to accommodate agencies with especially sensitive documents or especially low tolerances for risk. *See*, *e.g.*, NIST, *Recommended Security Controls for Federal Information Systems*, Special Publication 800-53, at 9, Dec. 2007 ("Since the baseline security controls represent the minimum controls[,] . . . . additional security controls and control enhancements for the information system are available to organizations and can be used in supplementing the tailored baselines to achieve the needed level of protection in accordance with an organizational assessment of risk."); *see also* U.S. CIO 25 Point Implementation, p. 8 (recognizing that agencies may add "additional, agency-specific requirements" for cloud computing to baseline Federal government requirements).

Moreover, NIST's current guidance does not address the distinctive security risks generated by the cloud computing solutions in general and multi-tenant clouds in particular. For example, in the same report that Plaintiffs cite on page 46 of their motion for judgment upon the administrative record, GAO stated that NIST's existing guidance is "insufficient" and "is not specific to cloud computing issues," and that NIST "has only begun plans to issue cloud-specific security guidance." AR 183 (quoting GAO, *Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing*, Report No. GAO-10-513, May 2010); AR 718, 726. Gartner has likewise asserted that "the risk associated with multi-tenant approaches is not addressed by existing information security assessment frameworks." AR 163; *see also* AR 177, 784.

NIST itself has recognized that its guidance does not yet cover cloud computing. The Director of the Information Technology Laboratory at NIST recently testified before the House of Representatives Committee on Oversight and Government Reform that NIST was launching a new initiative "'to facilitate the development of cloud computing standards.'" AR 784-85 (quoting the Director's July 1, 2010 testimony); *see also* AR 784-85 ("While FISMA certification is important, the fact that NIST is initiating efforts to create standards for cloud computing may be interpreted as an indication that the security controls defined in NIST Special Publication 800-53 revision 3 do not address the new security issues that are introduced by the multi-tenant cloud computing model.").

Consequently, although DOI is requiring the eventual contract awardee to comply with all applicable NIST guidance once it begins to set up the cloud, *see* AR 817-18, that NIST guidance is not determinative as to the question whether DOI should accept a government-wide cloud rather than a Federal-only cloud. In this uncertain environment, where the Federal government's standards for cloud computing have not yet been fully developed, it was reasonable for DOI to rely on sources other than the NIST minimum guidance and to use its discretion to impose rigorous restrictions on its cloud, such as total physical isolation, that minimize the risk that DOI's data will be compromised.

C. DOI Rationally Concluded That BPOS-Federal Meets Each Of DOI's Needs.

BPOS-Federal meets each of DOI's stated requirements. In particular, BPOS-Federal fulfills the agency's enhanced security requirements with data storage and computing infrastructure that would be solely dedicated to DOI. Plaintiffs' continued attempts to characterize BPOS-Federal as an "unproven" messaging solution that fails to meet DOI's stated needs are simply without merit. (Pls. Br. at 50-52). These arguments continue to reflect a fundamental misunderstanding of DOI's requirements.

Plaintiffs suggest that it was illogical to choose BPOS-Federal cloud over Google's government-wide cloud because Google Apps for Government has already been FISMA-certified and BPOS-Federal has not. (Pls. Br. at 47-49.) As discussed above at page 13, the oft-repeated[17] premise of this argument – that Google Apps for Government has been FISMA-certified – [redacted] Indeed, Google [redacted] (Gov't Cross-Mot. at p. 13 n.3, p. 38 n.13, Attachs. 1-5.) [redacted] With respect to FISMA compliance, there was thus absolutely no reason for DOI to pick Google Apps for Government over BPOS-Federal, [redacted]

[17] *See*, *e.g.*, Pls. Br. at 2-3, 16, 17, 18, 36, 45, 46, 47, 48; Compl. ¶¶ 20, 22; Pls. Mot. for Prelim. Inj. at 3, 9-10, 18, 29, 33, 27; AR 1005, 1007, 1018; Google, *FISMA-certified cloud applications for government - Google Apps*, *at* http://www.google.com/apps/intl/en/government/trust.html (cited in AR 783, and attached hereto as Attachment 1).

Moreover, Plaintiffs' argument presumes that DOI's only priority is, and should be, to obtain a "pre-FISMA-certified" cloud. Instead, based on its analysis of the applicable market research and its prior experiences – including "the systemic security breaches in DOI's IT systems over the years, and the consequent tongue-lashing by Judge Lamberth in his *Cobell* v. *Norton* decisions," (Pls. Br. at 49) – DOI's top priority is to obtain a cloud that is physically and logically dedicated solely to Federal government departments and agencies, and that will comply with FISMA before the cloud goes "live" and is actively used by DOI employees. While DOI requires a messaging solution to have the "[a]bility to comply with" FISMA security requirements, meaning the "[a]bility to successfully complete a Certification and Accreditation (C&A)," it does not mandate the attainment of FISMA certification as an eligibility criterion, nor is there any federal requirement for a pre-certified solution. AR 167 (emphasis added); AR 816.

Indeed, such a mandate would be inconsistent with the reality of the FISMA certification process – an agency can only certify and accredit the security of an information system after testing its controls to ensure they work properly. Because a dedicated cloud, such as BPOS-Federal, must be built for its customer, the cloud cannot possibly obtain FISMA certification or accreditation prior to the customer's decision to purchase the cloud and the physical completion of the cloud environment. Plaintiffs can offer no evidence that calls into question the ability of BPOS-Federal to achieve FISMA compliance.[18]

Plaintiffs also argue that BPOS-Federal was an irrational choice because it uses a separate, non-dedicated data center to archive emails. According to Plaintiffs, the Risk

[18] Furthermore, the actual successful completion of the FISMA certification and accreditation process is a matter of contract administration to be determined after contract award, and is therefore not the proper subject of a bid protest. *See Precision Standard, Inc.* v. *United States*, 69 Fed. Cl. 738, 755 (2006); *Chapman Law Firm* v. *United States*, 63 Fed. Cl. 519, 529-30 (2005).

Assessment's conclusion that DOI requires a DOI-only or Federal-only cloud for sending and receiving active email messages must necessarily mean that DOI also requires a dedicated cloud for archiving those messages. (Pls. Br. at 51-52.) However, Plaintiffs' argument incorrectly assumes that the security concerns present with active (*i.e.*, sent and received) messages are the same as those with archived (*i.e.*, stored) messages. In reality, the security concerns presented by the two types of emails are quite different. Archived emails are stored in an encrypted form, and are only unencrypted when they return to the active, dedicated environment. AR 805-06.

The RFQ reflects this important distinction, identifying DOI's requirements for active messaging and its requirements for archived messaging in completely separate places in the Statement of Work ("SOW"), *compare* AR 816-22 *with* AR 805-06, and establishing separate security measures (including stringent encryption requirements) to protect archived messaging data, AR 805. That DOI determined in the SOW that it required different requirements for these two different types of message does not, as the Plaintiffs contend (Pls. Br. at 51), "undermine[]" DOI's requirement for dedicated infrastructure for its active messaging environment. Plaintiffs ignore the realities of the two different types of messages, focusing instead on the fact that a single email in the active environment may one day be transferred to the archived environment.

IV. PLAINTIFFS CANNOT ESTABLISH PREJUDICE BECAUSE GOOGLE'S CLOUD SOLUTION DOES NOT MEET OTHER DOI MINIMUM REQUIREMENTS.

Plaintiffs concentrate entirely on the issue of whether DOI properly determined that its low tolerance for information security risk meant that it needed a cloud that is dedicated exclusively to the Federal government. However, while information security is essential, it is not the sole criterion for an award. The RFQ sets forth a number of other minimum requirements for its enterprise-wide messaging system that Plaintiffs have completely ignored. This omission is not surprising, because Google Apps cannot satisfy some of those additional critical requirements.

For example, Google Apps does not offer adequate mobile device support. Section 2.3 of the SOW requires the messaging system to support DOI's current base of approximately 8,000 Blackberry wireless devices. Full support of mobile devices was a top priority for DOI, which regards the use of mobile devices to access email as a "fundamental productivity tool that must be provided." AR 801. The RFQ correctly recognizes that "Blackberry services require the deployment of the Blackberry Enterprise Server (BES)," a separate system that connects an enterprise's email servers to its Blackberry devices. *Id.* The SOW seeks to maximize efficiency by transferring responsibility for the BES to the eventual contract awardee, and further requires that the BES be "co-located with" the email servers that reside inside the cloud. *Id.*

While Microsoft offers the BES inside its cloud, Google does not. Rather, Google expects its cloud customers to install and manage the BES outside the Google cloud (*e.g.*, at the customer's own location) and then connect to the cloud through additional software, the Google Apps Connector. Google's own web site states that a customer must "[i]nstall the Google Apps Connector on a server in <u>your environment</u> along with Blackberry Enterprise Server."[19] Google apparently refuses to implement, manage, or secure the BES inside its cloud, and would therefore deprive DOI of the full efficiencies and savings of a cloud-based system. Accordingly,

[19] Google, *Overview of Google Apps Connector - Google Apps Help*, *at* http://www.google.com/support/a/bin/answer.py?hl=en&answer=154346 (emphasis added) (attached hereto as Attachment 2).

Google itself admits that Plaintiffs cannot offer a cloud solution that fulfills Section 2.3 of the SOW.[20]

In addition, Google Apps does not offer several valuable business-productivity features for email, calendaring, and scheduling. Section 2.2 of the SOW requires its messaging system to have "core functionality" based on commonly used business productivity features in Microsoft Outlook, DOI's standard email software. AR 801. Google's cloud does not have this "core functionality" because it is incompatible with Microsoft Outlook in basic respects. For example, Google's website lists a number of "features that Google Apps Sync for Microsoft Outlook® does *not* support in Outlook Mail," including the ability to recall an inadvertently sent message, recover a deleted message, share mailbox folders with other users, access public folders, obtain delivery or read receipts, send executable files as attachments, and mark sent messages with "high importance." (Emphasis in original.) Google explains that "[t]hese features either aren't available in Outlook, or they might not work as you'd expect."[21]

[20] Google's website further acknowledges that the Google Apps Connector that is supposed to connect the customer's Blackberries to the Google cloud has significant compatibility issues that can frustrate users. For example, Google admits that critical fields in Blackberry users' address book, such as names and addresses, "may display incorrectly" on the Blackberry device. Google, *Release Notes - Google Apps Help*, *at* http://www.google.com/support/a/bin/answer.py?hl=en&answer=159400 (attached hereto as Attachment 3). These compatibility issues have the potential significantly to impair a Blackberry's role as a "fundamental productivity tool." AR 801.

[21] Google, *What's not supported in Outlook Mail - Gmail Help*, *at* http://mail.google.com/support/a/google.com/bin/answer.py?hl=en&answer=155553; *see also* Google, *What's not supported in Outlook Calendar - Gmail Help*, *at* http://mail.google.com/support/a/google.com/bin/answer.py?hl=en&answer=156466 (detailing several calendar features in Microsoft Outlook that either are not available or "might not work as you'd expect" when using Google Apps); Google, *Outlook Notes, Tasks, and Journals - Gmail Help*, *at* http://mail.google.com/support/bin/answer.py?hl=en&answer=156588 ("Google Apps doesn't have equivalent features, so notes, tasks, and journal entries you make in Outlook are *not* synchronized with your Google Apps account in the cloud. Instead, they're stored locally on (continued…)

DOI's goal is to establish "a single messaging and collaboration infrastructure," thereby "eliminating interoperability issues from the current disparate internal infrastructure." AR 748 (emphasis added). Plaintiffs' lofty assertions that Google Apps is fully compatible with Microsoft Outlook (*see* Pls. Prelim. Inj. Mem. at 37 & 43), are belied by Google's own public representations. Google Apps would not allow DOI users to take advantage of the full array of features available in the Department's standard email software, and many of the features missing from Google Apps are common functions that a typical email user utilizes on a regular basis. Consequently, in addition to failing to meet the requirements in Section 2.3 of the SOW, Google Apps also fails to meet the core functionality requirements in Section 2.2 of the SOW.

Because Plaintiffs do not offer a cloud computing solution that is capable of satisfying all of DOI's requirements, they cannot show prejudice. "To prevail in a bid protest case, the protester must not only show that the government's actions were arbitrary, capricious, or otherwise not in accordance with the law, but the protestor also must show that it was prejudiced by the government's actions." *KSD, Inc.* v. *United States*, 72 Fed. Cl. 236, 254 (2006) (citing 5 U.S.C. § 706); *accord Assessment & Training Solutions Consulting Corp.* v. *United States*, 92 Fed. Cl. 722, 729 (2010); *USfalcon, Inc.* v. *United States*, 92 Fed. Cl. 436, 450 (2010). Here, Plaintiffs have focused on the issue of the Federal-only cloud and have never proffered any actual evidence that Google's cloud could satisfy all of DOI's other requirements or that those requirements are unreasonable in any way. Indeed, Google's own website demonstrates that Google's cloud falls far short of meeting DOI's needs with respect to mobile devices and core functionality. As a result, regardless of how the Court were to resolve the

your computer in a PST file.") (emphasis in original) (collectively, attached hereto as Attachment 4).

rationality of DOI's insistence on a DOI-only or Federal-only server, Plaintiffs are not entitled to relief because they have suffered no prejudice.

V. THE COURT MUST REJECT PLAINTIFFS' UNFOUNDED CONSPIRACY THEORY

In the face of a comprehensive administrative record that demonstrates DOI's considered and rational assessment of its needs and DOI's thorough market research, Plaintiffs have now shifted their focus to unsupported allegations of bad faith and improper conduct by several high-level civil servants. Plaintiffs provide no support for these allegations, and fail even to attempt to meet the high legal standard for proving such claims.

Plaintiffs falsely allege that in September 2009 – in the midst of DOI's ongoing market research efforts for the Unified Messaging project and eleven months before the issuance of the RFQ – DOI selected Microsoft as the company that would provide the cloud computing solution for the Department's new enterprise-wide email system. (Pls. Br. at 27 & 31.) According to Plaintiffs, DOI and Microsoft officials then worked together in a secret partnership for over a year to implement this pre-selection of a Microsoft cloud, defining DOI's cloud computing requirements "to fit the characteristics or limitations of the particular Microsoft product." (*Id.* at 28, 51.) In promoting this wild conspiracy theory, Plaintiffs ask this Court to accept – without *any* proof in the administrative record – that Mr. Corrington and several other DOI officials conspired to create a "paper trail" of supporting documentation to cover-up their September 2009 pre-selection. (*Id.* at 34 & 52.)

The Federal Circuit has long recognized that there is a "strong presumption that government . . . officials exercise their duties in good faith." *Am-Pro Protective Agency, Inc.* v. *United States*, 281 F.3d 1234, 1239 (Fed. Cir. 2002); *accord Savantage*, 595 F.3d at 1288 ("As an initial matter, government officials are presumed to act in good faith."). To prevail on an allegation of bias or misconduct, a plaintiff "bears the burden of overcoming this presumption of good faith by 'almost irrefragable' proof." *Chenega Mgmt., LLC* v. *United States*, No. 10-221C, ___ Fed. Cl. ___, 2010 WL 3632960, at *22 (Fed. Cl. Sept. 14, 2010) (Braden, J.) (citing *Galen Med. Assoc. Inc.* v. *United States*, 369 F.3d 1324, 1337 (Fed. Cir. 2004)). "'[I]rrefragable proof' is to be adjudicated using the clear and convincing evidence standard." *Id.* Establishing that a procurement official acted in bad faith requires a showing "of some specific intent to injure the plaintiff." *Savantage*, 595 F.3d at 1288 (quotations omitted).

Plaintiffs fall well short of meeting this very heavy burden. Notably absent from Plaintiffs' motion for judgment upon the administrative record is any evidence that a DOI official had specific intent to injure Google or Onix. Plaintiffs simply offer a skewed timeline of events and arguments contesting the rationality of DOI's articulation of its own requirements.

Indeed, the central premise of Plaintiffs' allegation of bad faith – an alleged September 2009 decision to select a Microsoft solution – is completely unsupported by the record. The September 2009 draft Project Plan, which Plaintiffs point to as proof that the Department pre-selected Microsoft in September 2009, is nothing more than a working assessment of DOI's market research for the Unified Messaging project. The draft Project Plan was created in June 2009 to account for the research that Mr. Corrington and his team had been conducting since 2007. AR 180. The document was then updated by Mr. Corrington on a semi-regular basis to reflect further advancements in this market research and changes in underlying assumptions concerning the project. AR 1580 (showing that the document was revised in June 2009, September 2009, March 2010, April 2010, and May 2010).

While the draft Project Plan clearly shows that Mr. Corrington's acquisition planning and market research in September 2009 were trending toward a Microsoft cloud, the document by no means establishes that DOI had made a decision to implement a unified messaging system with a Microsoft solution.[22] Plaintiffs simply gloss over the fact that the draft Project Plan, which was last updated in May 2010, was never completed. *See* Pls. Br. at 4 n.1. The draft Project Plan contemplated approval from 14 different DOI officials, whose signatures would collectively signify DOI's agreement "on the scope, desired outcomes, schedule, costs, and resource commitments stated in [the] document." AR 1092-93, 1578-79. Notably, the draft document was never signed by <u>any</u> of these DOI officials. *Id.*[23]

The record unequivocally demonstrates that in the months after DOI's alleged September 2009 pre-selection of Microsoft, DOI continued meticulously to assess its own needs and research the available technology, including non-Microsoft clouds. In particular, during this time, DOI officials held several meetings with Google to learn more about the company's Google Apps cloud computing solution. These agency officials actively sought to understand the Google product, and in particular whether the company could provide a cloud computing solution that would meet the Department's minimum needs. *See*, *e.g.*, AR 150 (describing a February 18, 2010 meeting with Google, attended by Mr. Corrington, Mr. Mazer, and Mr. Jackson); AR 97-98, 150 (describing the Google Apps Summit that Mr. Corrington and Mr. Mazer attended on April 28, 2010); AR Tab 4 (May 27, 2010 letter from DOI to Google, inviting

[22] This focus on a Microsoft solution is not at all surprising – at the time that Mr. Corrington was updating his working Project Plan, Mr. Corrington correctly understood the Microsoft solution to be the only available solution that could offer DOI a dedicated computing infrastructure, physically isolated from other cloud customers. *See supra* p. 6.

[23] In fact, a cursory examination of the latest version of the draft Project Plan reveals that the document remained far from complete. Whole sections of the document had yet to be drafted. For example, § 5.3.5 of the draft Project Plan (at AR 1594) contains a placeholder for a discussion of Operation Processes related to email support – "TIER 2 STUFF GOES HERE." Likewise, § 5.6 of the draft Project Plan (at AR 1598) is blank, except for the words "Billing Etc."

the company to make a presentation on how Google Apps could meet specified DOI requirements).

These DOI officials gave Google every opportunity to explain how it could meet DOI's requirements, and Google consistently refused. *See*, *e.g.*, AR 150 (February 18, 2010: Google advised that "no single tenant offering would be available"); AR 151 (describing a June 9, 2010 meeting with DOI where Google stated that it was "incapable of supporting a dedicated solution"); AR Tab 5 (June 17, 2010 letter from Google to DOI: "Google intends to offer messaging services hosted in a Government-only cloud, rather than a private cloud."). Instead, Google responded to DOI's overtures by arguing to change the agency's requirements. *See*, *e.g.*, AR 151 (noting that on June 9, 2010, Google [redacted]); AR Tab 5 (June 17, 2010 letter from Google to DOI, arguing that a requirement for dedicated infrastructure "is not necessary to satisfy [DOI's] needs").

In order to accept Plaintiffs' allegation that by September 2009 DOI had determined that it would implement a Microsoft cloud, the Court would have to dismiss all of the market research and acquisition planning that Mr. Corrington and other DOI officials undertook from October 2009 to September 2010 as a cover-up. For instance, this Court would have to accept that:

- Mr. Corrington, Mr. Mazer, Mr. Jackson, and the DOI contracting officials, all of whom met with Google on at least one occasion after September 2009 to learn more about the company's cloud offerings, in fact had no intention of considering a Google cloud for the Unified Messaging project, despite having represented to Google that this was the reason for their meetings, *see* AR 47.

- Mr. Corrington and Mr. Ruffin completed a biased Risk Assessment to support the alleged pre-selection of Microsoft,[24] and then presented that Risk Assessment to DOI's

[24] *See* Pls. Br. at 39 (asserting that the Risk Assessment "represents nothing more than a *post hoc* justification for a choice made long before its creation") (italics in original).

CIO as an objective assessment of the Department's tolerance for information security risk and a corresponding articulation of the Department's cloud computing requirements, *see* AR 156-57;

- Mr. Corrington, Mr. Mazer, and other DOI officials tailored their market research to support a pre-ordained result,[25] and then certified to the completeness and accuracy of that research on August 19, 2010 when they signed the Limited Source Justification, *see* AR 850; and
- DOI officials engaged [redacted] to perform meaningless market research in order "to create a paper trail,"[26] and then presented that research to the Assistant Secretary for Policy, Management and Budget as independent, unbiased research, *see* AR 756.

Plaintiffs offer no support in the record for any of these conclusions.

This Court has recognized that mere "[s]peculation and innuendo" are "insufficient to overcome the presumption that procurement officials act in good faith." *Chenega Mgmt.*, 2010 WL 6362960, at *23 (citing *T & M Distribs., Inc.* v. *United States*, 185 F.3d 1279, 1285 (Fed. Cir. 1999); *C.A.C.I., Inc.-Fed.* v. *United States*, 719 F.2d 1567, 1582 (Fed. Cir. 1983); *ARINC Eng'g Servs., LLC* v. *United States*, 77 Fed. Cl. 196, 202 (2007)). This Court should reject Plaintiffs' irresponsible attempt to construct a massive conspiracy on the basis of pure speculation and innuendo. The administrative record makes clear that the Department's market research and assessment of its cloud computing requirements continued well past September 2009, and that DOI did not ultimately decide to standardize on a BPOS-Federal solution until the Assistant Secretary for Policy, Management and Budget approved a standardization decision in July 2010, after having completed extensive and unbiased market

[25] *See* Pls. Br. at 28 (alleging that DOI's market research was "tailored to support the pre-ordained result").

[26] *See* Pls. Br. at 34 (accusing DOI of contracting with [redacted] "to create a paper trail to support the decision already made by DOI to procure the Microsoft solution").

research, and afforded Google multiple opportunities to explain how it could meet the Department's objective requirements.

CONCLUSION

For the foregoing reasons, Softchoice respectfully requests that the Court deny Plaintiffs' motion for judgment upon the administrative record, grant Softchoice Corporation's cross-motion for judgment upon the administrative record, and enter judgment in favor of the United States.

Respectfully submitted,

s/ Steven J. Rosenbaum
Steven J. Rosenbaum
Counsel of Record
Alan A. Pemberton
Sarah L. Wilson
Scott A. Freling
Shelli L. Calland
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
Tel: (202) 662-5568
Fax: (202) 778-5568
srosenbaum@cov.com

William A. Shook
SHOOK DORAN KOEHL LLP
643 E Street, N.E.
Washington, D.C. 20002
Tel: (202) 583-0008
Fax: (202) 280-1097
bill.shook@sdklaw.net

December 17, 2010

Counsel for Softchoice Corporation

ATTACHMENT 1

Softchoice Corporation's Opposition to Plaintiffs' Motion for Judgment Upon the Administrative Record, and Cross-Motion for Judgment Upon the Administrative Record

Google

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

> “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

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.

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

Learn more

- FAQ
- Compare editions

Additional resources:

- Email security
- Security and privacy FAQs
- Security whitepaper

Certifications:

FISMA

SAS 70 Type II

CSA cloud security alliance℠

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.

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.

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.

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 Apps for Non-profit

Compare editions

Become a reseller

Google Video

More Google Applications

Apps Marketplace

Chrome browser

Product videos

Chrome notebooks

Email & phone support

Terms of Service Program Policies Help Center

Search this site

ATTACHMENT 2

Softchoice Corporation's Opposition to Plaintiffs' Motion for Judgment Upon the Administrative Record, and Cross-Motion for Judgment Upon the Administrative Record

Google Apps **Google Apps Administrator Help**

Overview of Google Apps Connector

Google Apps Connector integrates the Google Apps messaging suite with BlackBerry Enterprise Server, giving mobile users the ability to use built-in BlackBerry applications to access their Google Apps email, calendar, and contacts. Administrators use the same BlackBerry tools they already know for securing and managing BlackBerry devices.

Install the Google Apps Connector on a server in your environment along with BlackBerry Enterprise Server. The Administration Guide includes all steps needed to install the Google Apps Connector and all required components.

Latest Release

Google Apps Connector for BlackBerry Enterprise Server version 3.0.1 includes support for BlackBerry Enterprise Server 5.0.2 and a dynamic GAL. For more information on the new release, see the Release Notes.

Download

- To download the Google Apps Connector, see the download page for **Google Apps Connector for BlackBerry Enterprise Server**.

Maintenance Release Version

The Google Apps Connector is tested with BlackBerry Enterprise Server version 4.1.7 MR3, BlackBerry Enterprise Server 5.0.2, and BlackBerry Enterprise Server Express 5.0.2.

Documentation and Support

- Installation and Administration Guide [HTML] [PDF]
- User Setup Guide
- User Feature Chart
- Release Notes
- Admin Utilities
- Support Forum

Key benefits:

- Keep enterprise BlackBerry devices synchronized with Google Apps.
- Push email synchronization with less than 60 seconds latency.
- Synchronized reading, deleting and archiving between Google Apps and BlackBerry devices.
- Synchronized Global Address List from Google Apps to your device.
- Support for Labels/Folders in email.
- Two-way contact and calendar synchronization.
- Supports key BlackBerry Enterprise Server features such as remote wipe and IT policy administration.
- Hosting partner support for multiple Google Apps domains on a single BlackBerry Enterprise Server.

System requirements:

For up to 250 users per server:

- *Google Apps*: Google Apps for Business or Education
- *Server*: Dual Intel® Pentium® IV processor (2GHz or greater)
- *Memory*: 4 GB RAM
- *OS*: Microsoft Windows 2003 SP2 or 2008 SP2
- *Disk Space*: 1 GB per user (in addition to Windows requirements)
- *BlackBerry Enterprise Server*: BlackBerry Enterprise Server 4.1.7 MR3 or 5.0.2..
- *Database*: Microsoft SQL Server (optional)

For up to 500 users per server:

- *Google Apps*: Google Apps for Business or Education
- *Server*: Quad Core Intel® Pentium® IV processor (2GHz or greater)
- *Memory*: 8 GB RAM
- *OS*: Microsoft Windows 2003 SP2 or 2008 SP2.
- *Disk Space*: 1 GB per user (in addition to Windows requirements)
- *BlackBerry Enterprise Server*: BlackBerry Enterprise Server 4.1.7 MR3 or 5.0.2.
- *Database*: Microsoft SQL Server (required)

For up to 30 users per server on BlackBerry Professional Software:

- *Google Apps*: Google Apps for Business or Education
- *Server*: Intel® Pentium® IV processor (2GHz or greater)
- *Memory*: 2 GB RAM
- *OS*: Microsoft Windows 2003 SP2 or 2008 SP2
- *Disk Space*: 1 GB per user (in addition to Windows requirements)
- *BlackBerry Professional Software*: BlackBerry Enterprise Server Express.
- *Database*: Microsoft SQL Server (optional)

Was this information helpful? ○ Yes ○ No

Google Apps - Support - Help with other Google products -

ATTACHMENT 3

Softchoice Corporation's Opposition to Plaintiffs' Motion for Judgment Upon the Administrative Record, and Cross-Motion for Judgment Upon the Administrative Record

Google Apps Administrator Help

Release Notes

3.0 Release Information

Last updated 28 October 2010

These release notes describe the Google Apps Connector for BlackBerry Enterprise Server Release 3.0. You can find detailed information on features and installation in the Google Apps Connector for BlackBerry Enterprise Server Help Center article.

New Features

The **Google Apps Connector** integrates the Google Apps messaging suite with BlackBerry Enterprise Server, giving mobile users the ability to use built-in BlackBerry applications to access their Google Apps email, calendar, and contacts. Adminstrators use the same BlackBerry tools they already know for securing and managing BlackBerry devices.

Release 3.0 of the **Google Apps Connector** includes new features that enhance the power of the Google Apps Connector:

- **Support for BlackBerry Enterprise Server 5.0.2**
- **Support for BlackBerry Enterprise Server Express**.
- **Support for Microsoft Windows 2008 SP2**.
- **Dynamic GAL**: Google Apps Connector now supports dynamically Global Access List.
- **Reliable Calendar Sync**: A new calendar helper module with enhanced calendar support.

Admin utilities

Admin scripts to create a MAPI profile for BlackBerry Manager to support BlackBerry server management from a terminal server. For sample scripts, see the Support Tools article.

Fixed Issues

Following below are the issues resolved in the current release.

1. Activation messages classified as Spam for international customers

Issue: For some international customers, the Google Apps Connectors triggered Spam filters are were directed to the Spam folder. This caused delayed activation until the activation email was moved to the Inbox.

Resolution: Activation now proceeds normally with no manual move of email needed.

Known Issues

Following below are the known issues in the current release. Each issue includes a brief description and workaround (if applicable).

1. Contact address fields may display incorrectly on BlackBerry device.

Issue: When editing a contact, Gmail displays the contact address in a single text field, while a BlackBerry displays street, city, postal code, and country in separate address fields. Due to this difference, contact addresses may not be formatted in the correct address fields on a BlackBerry device.

Resolution: This will be resolved in a future release.

Workaround: Edit contacts using the BlackBerry device. This will properly store and display the addresses within BlackBerry devices and Gmail.

2. Contact name fields may display incorrectly on BlackBerry device.

Issue: When editing a contact, Gmail displays the contact full name in a single text field, while a BlackBerry displays name prefix, first name, and last name as separate text fields. Due to this difference, contact names may not be formatted in the correct name fields on BlackBerry devices.

Resolution: This will be resolved in a future release.

Workaround: Edit contacts using the BlackBerry device. This will properly store and display the name within your BlackBerry and Gmail.

3. Address fields may not displayed in Gmail

Issue: If a contact is created in Gmail and any field other than the address field is modified on a BlackBerry, Gmail may not display the address field. Address is correctly displayed on BlackBerry devices.

Resolution: This will be resolved in an upcoming release.

Workaround: To display the address field, modify the address field on your BlackBerry.

Was this information helpful? ○ Yes ○ No

Google Apps - Support - Help with other Google products -

ATTACHMENT 4

Softchoice Corporation's Opposition to Plaintiffs' Motion for Judgment Upon the Administrative Record, and Cross-Motion for Judgment Upon the Administrative Record

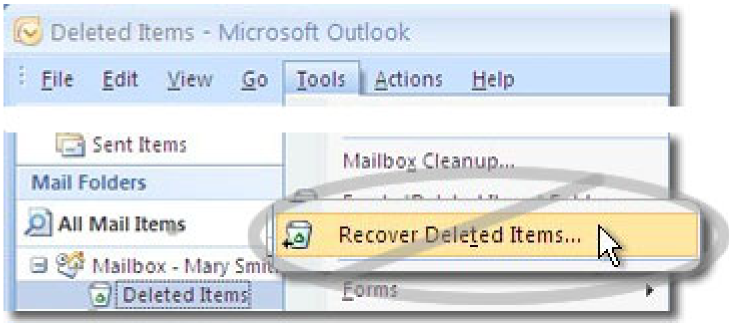
Gmail Help

What's not supported in Outlook Mail

Here are a few features that **Google Apps Sync for Microsoft Outlook®** does *not* support in Outlook Mail. These features either aren't available in Outlook, or they might not work as you'd expect.

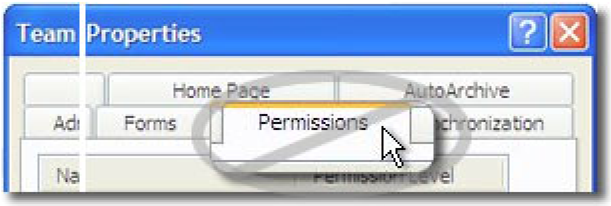
Recovering deleted items

After emptying your Deleted items folder, you can't use "Recover Deleted Items" in Outlook's Tools menu to get the messages back. (This menu item isn't available.)



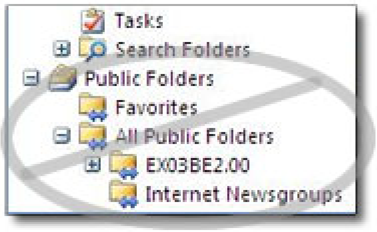
Sharing mailbox folders

You can't share a mailbox folder in Outlook with other users (Permissions settings aren't available in the folder's Properties dialog). This is because folders in Outlook map to *labels* in Gmail, which don't have permission properties.



Public folders

Public folders aren't available with Google Apps Sync (they're missing from Outlook's navigation pane).



Sending executable attachments

Google Apps Sync doesn't allow sending executable file attachments (including executables in compressed attachments) from either Outlook or the Gmail interface.

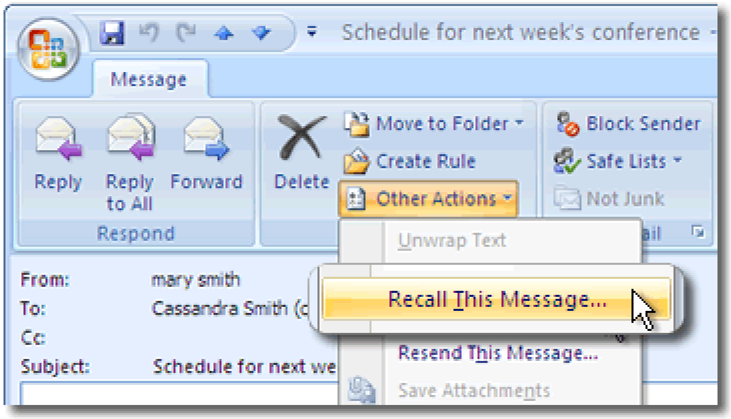
Which file types can I *not* send?

Delivery receipts

Delivery receipts aren't generated in Outlook when using Google Apps Sync. If you request a delivery receipt for a message you send from Outlook, you won't receive a response when the message is delivered. However, you can select a read receipt (see below).

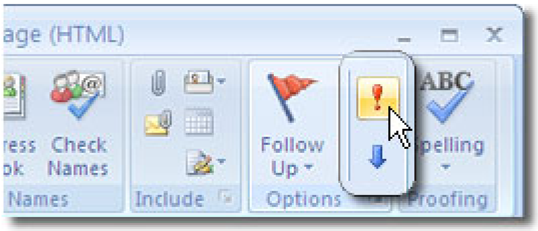
⚠ **Read receipts**
Read receipts are generated in Outlook with Google Apps Sync. However, your recipient must be using Outlook and must enable read receipts for their profile. In that case, you'll get a response when your message is read.

⚠ **Recalling a sent message**
In Outlook, you can choose Recall Message from a sent message's Other Actions menu, to try to recall a message you just sent. However, unlike Microsoft® Exchange, Gmail can't recall messages. Instead, the recipient receives both the original message, along with a follow-up message saying you wanted to recall the message.



From: mary smith
To: Cassandra Smith (c
Cc:
Subject: Schedule for next we

⚠ **Setting importance levels for recipients**
In Outlook, you can send mail marked as “Important” or Low Priority.” But these values aren’t synchronized with your Google Apps account in the cloud and therefore don’t show up for other users.



[Back to help for Outlook Mail (Google Apps Sync)]

updated 10/11/2010

Gmail - Contacting Us - Help with other Google products -

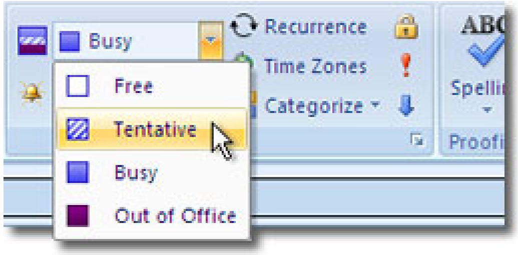
Gmail Help

What's not supported in Outlook Calendar

Here are features that **Google Apps Sync for Microsoft Outlook®** doesn't fully support in Outlook Calendar. These features either aren't available in Outlook, or they might not work as you'd expect.

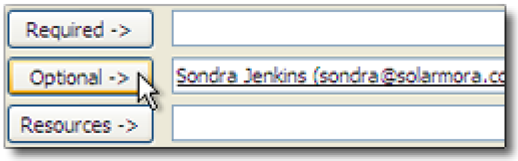
⚠ Tentative or Out of Office status

Choosing Tentative or Out of Office status for a calendar event appears as Busy to other users viewing your status. This is because Google Calendar supports only Free or Busy status, not these other alternatives.



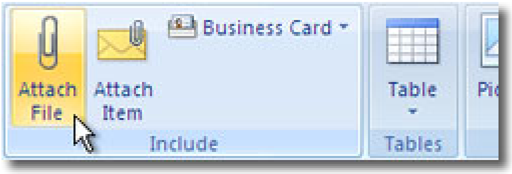
⚠ Optional attendees

If you mark an attendee as Optional when inviting them to a meeting, they appear as Required to everyone else. This is because Google Calendar doesn't differentiate between Optional and Required attendees.



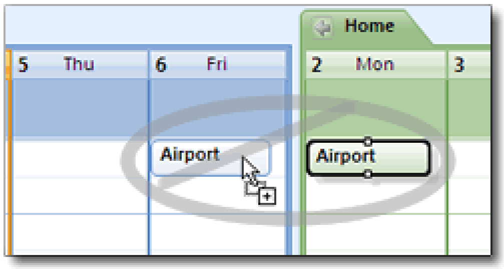
⚠ Calendar attachments

If you attach a document, contact, or other item to a calendar event in Outlook, you see the attachment in your own calendar but other attendees don't see it in theirs. This is because attachments aren't synchronized with other people's calendars.



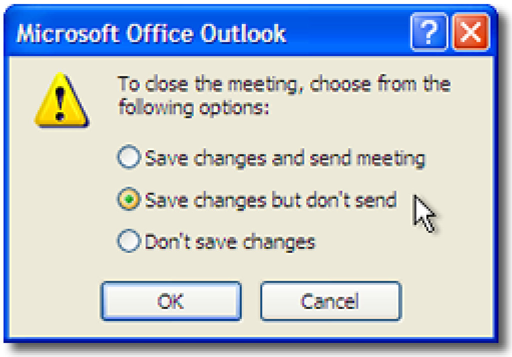
✖ Moving or copying events between calendars

You can't drag an event from one calendar to another in Outllook, as you can when using Outlook with Microsoft® Exchange.



⚠ Saving event updates without sending

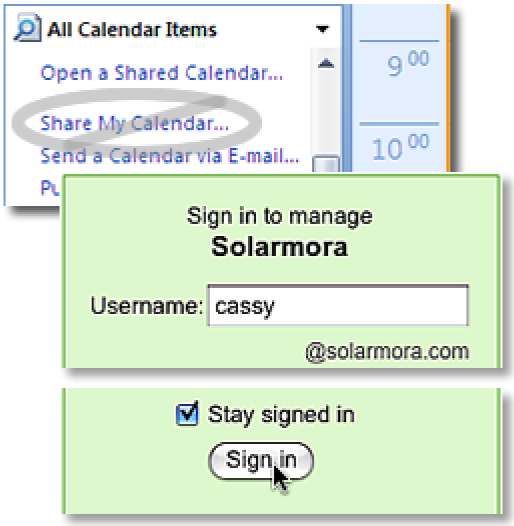
If you create or update an event in Outlook and choose *not* to send the change to attendees (by closing the event window and choosing not to send), attendee calendars update anyway. This is because event data always synchronizes with other people's calendars whether or not you send updates from Outlook.



To close the meeting, choose from the following options:

○ Save changes and send meeting
● Save changes but don't send
○ Don't save changes

⚠ **"Share my Calendar" link**
You can share calendars from Google Apps Sync, but you don't use the "Share my Calendar" link (which isn't available). Instead, set up sharing by signing in to your Google Calendar account in a web browser. For details, see Sharing and delegation.



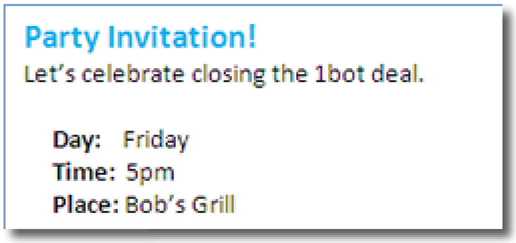
Sign in to manage
Solarmora

Username: cassy
@solarmora.com

☑ Stay signed in

⚠ **"Deleting" calendar folders**
You can delete a calendar folder from Outlook to remove it from your Calendar Navigation Pane. But the calendar isn't deleted from your account. It's just no longer synchronized with Outlook. To delete the calendar completely, you must sign in to your Google Calendar account and delete it there. For details, see Delete a calendar.

⚠ **Rich content in calendar events**
You can add rich content such as links and formatted text to a calendar description in Outlook. But the formatting doesn't synchronize with other users' calendars so everyone else sees only plain text.



Party Invitation!
Let's celebrate closing the 1bot deal.

Day: Friday
Time: 5pm
Place: Bob's Grill

✖ **Calendar invitations sent to a POP or IMAP account**
If you create a POP or IMAP account in your Outlook profile, calendar invitations sent to that account will not appear on your primary Outlook calendar (as they would with Exchange). Google Apps Sync can only update your calendar with invitations sent to your Google Apps account.

Back to help for Outlook Calendar (Google Apps Sync)

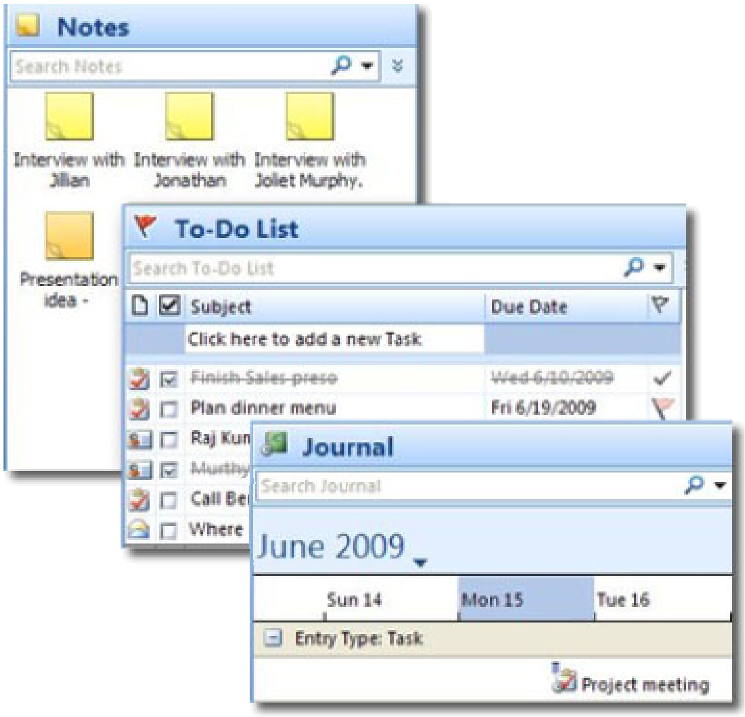
updated 10/11/2010

Gmail - Contacting Us - Help with other Google products -

Gmail Help

Outlook Notes, Tasks, and Journal

With **Google Apps Sync for Microsoft Outlook®**, you can import Notes, Tasks, and Journal entries from your old Outlook profile to your Google Apps profile, then continue using these features in Outlook much as before. You can import this data either when you first install Google Apps Sync (learn more), or later on (learn more).



✓ Notes, Tasks, and Journal entries...

Are available in Outlook, with Google Apps Sync: Track to-do items on your task list, jot down ideas on colored sticky Notes, and record journal entries, just as you have with your old Outlook profile.

✗ However they...

***Aren't* available from Google Apps**: Google Apps doesn't have equivalent features, so notes, tasks, and journal entries you make in Outlook are *not* synchronized with your Google Apps account in the cloud. Instead, they're stored locally on your computer in a PST file. They remain available in Outlook, but there's no way to see them when you sign in to your Google Apps account from a web browser. Learn more about working in the cloud.

Don't support multi-user interactions For example, you can't assign a task to someone or share your Notes. Instead, use these features for personal work.

Don't synchronize with other computers where you use Outlook: If you use Outlook with Google Apps Sync on two computers (say, a desktop at work and a laptop at home), Notes, Tasks, and Journal entries you create on one computer won't be available in Outlook when you open your Google Apps profile on the other computer.

Back to Google Apps Sync help

updated 10/11/2010

Gmail - Contacting Us - Help with other Google products -