In the United States Court of Federal Claims

No. 13-198C

(Filed Under Seal: July 12, 2013)
(Reissued: July 17, 2013)

****

MCAFEE, INC.,	)	Pre-award bid protest; jurisdiction; standing; brand-name, sole-source procurement; Competition in Contracting Act, 41 U.S.C. § 3301; 10 U.S.C. § 2304(a)(1); factors governing equitable relief; interests of national defense and national security; 28 U.S.C. § 1491(b)(3)
Plaintiff,	)	
v.	)	
UNITED STATES,	)	
Defendant.	)	

****

Richard J. Conway, Dickstein Shapiro LLP, Washington, D.C., for plaintiff. With him on the briefs were Charlotte Rothenberg Rosen and Adele H. Lack, Dickstein Shapiro LLP, Washington, D.C.

K. Elizabeth Witwer, United States Department of Justice, Washington, D.C., for defendant. With her on the briefs were Stuart F. Delery, Acting Deputy Assistant Attorney General, Jeanne E. Davidson, Director, and Deborah A. Bynum, Assistant Director, Commercial Litigation Branch, Civil Division, United States Department of Justice, Washington, D.C. Of counsel were Richard Bean, Attorney Advisor, and Frank Yoon, Lt. Col., Trial Attorney, United States Air Force.

OPINION AND ORDER[1]

LETTOW, Judge.

In this pre-award bid protest, plaintiff, McAfee, Inc. ("McAfee") complains of an alleged brand-name, sole-source procurement performed by the United States through United States Department of the Air Force ("Air Force") in violation of the Competition in Contracting Act

[1]Because this opinion and order might have contained confidential or proprietary information within the meaning of Rule 26(c)(1)(G) of the Rules of the Court of Federal Claims ("RCFC") and the protective order entered in this case, it was initially filed under seal. The parties were requested to review this decision and to provide proposed redactions of any confidential or proprietary information. The resulting redactions are shown by brackets enclosing asterisks, *e.g.*, "[***]."

("CICA"), 41 U.S.C. § 3301. McAfee alleges that in a quest to reconfigure and strengthen its network security technology, the Air Force made what amounts to a sole-source selection without the requisite justification. McAfee seeks injunctive relief against the Air Force to prevent the alleged enterprise-wide standardization. Compl. ¶ 5.

FACTS[2]

McAfee is a wholly owned subsidiary of Intel Corporation, AR 15-535 [***],[3] organized under the laws of Delaware and having its principal place of business in Santa Clara, California, Compl. ¶ 7. It is a software developer and manufacturer, focusing on computer and network security software and hardware products. *Id*. ¶¶ 7-8. McAfee software has been used by the Air Force for network security (in concert with software from other companies) over the last fifteen years up to the present day. *Id*. ¶ 7. If the Air Force's present network-security standardization plans go forward, McAfee effectively will be barred from competing for Air Force network-security contracts because it does not manufacture a program compatible with the Air Force's network-security infrastructure that is tied to a particular sole source.

A. *Air Force Cyber Security Architecture*

Air Force network security is managed by the Combat Information Transport System ("CITS"), established in the 1990s "as a ground infrastructure modernization program to support the day-to-day information transport needs at fixed base Air Force installations world-wide." AR 8-329 (AFNet Life Cycle Management Plan). Through CITS, the Air Force implements various discrete programs to achieve satisfactory network security throughout the entirety of its systems. One such program is the Air Force Network Increment 1 program ("AFNet"),[4] which manages system integration, modernization, support, commercial-off-the-shelf equipment purchase, and interim contract support. *Id.* at 328 to -29.

Under the AFNet program, the Air Force periodically redesigns and upgrades its "network management capabilities, network security and defense capabilities." AR 51-2113

---

[2]The recitations that follow constitute findings of fact by the court drawn from the administrative record of the procurement and the parties' evidentiary submissions related to prejudice and equitable relief. *See Bannum, Inc. v. United States*, 404 F.3d 1346, 1356 (Fed. Cir. 2005) (specifying that bid protest proceedings "provide for trial on a paper record, allowing fact-finding by the trial court").

[3]All citations to an administrative record refer to the Amended Administrative Record filed on May 8, 2013. The record in this case is paginated sequentially and also divided into tabs. When citing to the Amended Administrative Record, the court will first designate the tab in which the cited material can be found, followed by the page number. For example, "AR 8-329" refers to page 329, which is located in Tab 8 of the Amended Administrative Record.

[4]AFNet was formerly titled "CITS Block 30 Foundation Spiral and Spiral 1," and as such, any references to the latter will be treated as equivalent to the former in this opinion. *See* AR 8-328 (AFNet Life Cycle Management Plan).

(AFNet Sufficiency Review). As a "key component of reducing [Air Force] vulnerability to cyber threats," AFNet constantly enhances the Air Force's security technology for its unclassified and classified networks. *Id.* at 2121. This security is achieved in large part by focusing on securing various "gateways" in the Air Force network system, each gateway representing a potential point of ingress for cyber threats from outside the Air Force. *See* Def.'s Mot. to Dismiss, or in the Alternative, Mot. for Judgment Upon the Admin. Record ("Def.'s Mot.") at 5 n.2.

During the early 2000s and before, AFNet practiced a "base-centric" form of security, meaning that network security was managed primarily through securing individual base boundaries. *See* AR 51-2114 (AFNet Sufficiency Review). The resulting structure was one where each base had its own network boundary that had to be individually secured, amounting to 104 unique access points to the Air Force network. *See* AR 8-326 (AFNet Life Cycle Management Plan). As time went on and technology shifts occurred, it became apparent that the high number of access points and lack of standardization across bases made the base-centric approach unwieldy, engendering a shift towards an Air Force-centric structure. *See id.* at 344. This new approach was determined to have benefits that included "minimiz[ing] the entry points to the [Air Force] Intranet; provid[ing] central management of policy, control and monitoring of the [Air Force] network; and [feeding] into and complement[ing] the [Department of Defense network] architecture." *Id.* at 343. The shift reduced the number of primary network access points from 104 to sixteen. *Id.* at 326. Now, to reach individual base networks, a threat must first pass through one of the sixteen Air Force gateways. Under the new, less exposed system, "[e]ach squadron has the capability to provide continuity of operations for the other." *Id.* at 344.

When AFNet shifted to Air Force-centric security, it relinquished primary control over the base boundaries. *See* AR 38-1652 to -53 (AFNet Gateway Technical Requirements document ("TRD") (Apr. 4, 2012)). Eventually, another program within CITS entitled the Enclave Non-Classified Internet Protocol Firewall and Automated Security Incident Measurement Sustainment ("ENFAAS")[5] assumed responsibility for shoring up the base boundaries; however, ENFAAS was not fully functional until several years after AFNet shifted to gateway security. *See* AR 45-1758 (Request for Proposal ("RFP") for ENFAAS (Feb. 11, 2013)). Although AFNet now managed a first-wave line of defense against external threats at the gateways, base boundaries still acted as a second line of defense against external assaults, as well as a primary check against threats originating from within the Air Force network (which never have to pass through any of the sixteen Air Force gateways because their points of origin are inside those gateways). *See* Def.'s Mot. at 6-7.

To employ use funds appropriated for "products and services associated with the design, engineering, integration, installation and configuration of Air Force networks and network infrastructure," CITS programs must expend those funds through a standing Indefinite Delivery/Indefinite Quantity ("IDIQ") contract group of system integrators, termed Network Centric Solutions ("NETCENTS"). AR 1-1 (NETCENTS Memorandum (Jan. 27, 2005)). The Department of the Air Force issued a mandatory use policy in January 2005, setting out the

[5]The parties also refer to the base boundary management program as "AFNet 2," but the court will refer to it as ENFAAS going forward.

scope of NETCENTS contracts in a "Mandatory Use Decision Matrix." AR 1; AR 2 (NETCENTS Mandatory Use Decision Matrix). Eight concerns had already been selected in 2004 through a competitive solicitation process for NETCENTS eligibility: General Dynamics Information Technology, Inc., Centech Group, Inc., Harris IT Services Corporation, Northrop Grumman Information Technology, Inc., NCI Information Systems, Inc., Booz Allen Hamilton, Inc., Lockheed Martin Integrated Systems, Inc., and Telos Corporation. *See* Air Force NETCENTS-1 Documents, www.netcents.af.mil/contracts/netcents-1/documents/index.asp (last visited July 8, 2013). Because the NETCENTS group is the mandatory "primary source for acquiring voice, video, and data communications hardware and software," AR 1-1, both AFNet and ENFAAS projects fall under the scope of NETCENTS, and are therefore required to purchase through the NETCENTS IDIQ. McAfee is not, nor apparently has it ever been, a qualified NETCENTS concern. However, it has frequently and successfully participated as a subcontractor to NETCENTS concerns in the past. *See, e.g.*, AR 57-2742 (General Dynamics Response to AFNet RFP (Dec. 8, 2011)).

B. *Next Generation Firewall Selection*

Very recently, a new cyber-security technology has appeared on the market, called "next generation firewall" ("nextgen firewall") technology. *See* AR 15-526 ([***]). Nextgen firewalls were pioneered by a company called Palo Alto Networks, and other tech companies have since followed suit. AR 15-536. Whereas classic firewalls are designed to "detect and block . . . attacks" attempting to penetrate network barriers, nextgen firewalls can also "enforce granular security policy at the application (versus port and protocol) level." *Id.* at AR 15-527. Thus, while a classic firewall might detect a threat as it passes through a gateway, a nextgen firewall could also detect a threat after it has breached the gateway, in this instance moving within Air Force network space. Before nextgen firewall technology came onto the market, users looking for this combination of security would have had to install a separate intrusion prevention system in addition to a traditional firewall. After the advent of nextgen firewall technology, users could achieve the same level, or higher, of security by using a single, sole-source nextgen program instead. At no point during the relevant periods does it appear that McAfee offered a fully integrated nextgen firewall product. *See* AR 72-3036 ([***]).

1. *AFNet modifications.*

Prior to the advent of nextgen firewalls, the Air Force employed firewalls and intrusion prevention systems in tandem. This was the case in 2009, when AFNet began an upgrade of the Air Force gateways. In September of 2009, the Air Force awarded General Dynamics Information Technology, Inc. ("General Dynamics") a delivery order for implementation of the AFNet gateway update project. AR 7 ("AFNet Update 1 delivery order"). The AFNet Update 1 delivery order was not competed; the Air Force awarded the delivery order to General Dynamics under one of the fair-opportunity exceptions in 48 C.F.R. [(Federal Acquisition Regulation ("FAR")] § 16.505(b)(2)(i). *See* AR 3-15 to 16 (Fair Opportunity Exception Justification, 2009) ("The current [Air Force] security boundary is inadequate to face the increasingly sophisticated cyber-attacks being detected. . . . The Air Force need for the [AFNet] configuration is so urgent that providing a fair opportunity would result in unacceptable delays. . . . [General Dynamics]

. . . possesses a complete understanding of the current [AFNet] sites and knowledge of site-specific conditions that no other contractor has at the present time.").

As early as 2011, the Air Force had become aware of emerging nextgen technology and was investigating its capabilities. *See* AR 36-1570 (Engineering Change Proposal (Sept. 19, 2012)). In February of 2011, the Air Force put out a Request for Information ("RFI"), soliciting software vendors for information about their most recent cyber security products which could be used on AFNet. *See* AR 52-2240 (2011 RFI). Specifically, that RFI inquired about devices "which provide for the integration of both Firewall and Intrusion Detection/Prevention System (IDPS) capabilities." AR 52-2240. McAfee and Palo Alto both responded to the RFI, among others. *See* AR 53-2335 to -2362 (McAfee's Responses to RFI); AR 70-2989 to -3002 (Merlin/Palo Alto's Response to RFI). In the meantime, Air Force networks continued to run separate firewall and intrusion prevention software.

Somewhat later in 2011, AFNet's systems were once again due for a routine upgrade and modernization. Again, the Air Force determined that General Dynamics should receive the award based upon a fair-opportunity exception. *See* AR 11-446 (Fair Opportunity Exception Justification, 2011) ("Currently, [General Dynamics] is the only firm that possesses a complete understanding of the 'as installed' AFNet Increment 1 System and has in-depth technical knowledge of site-specific conditions necessary for continued support.").

As the Air Force was preparing to issue the delivery order for the second AFNet update (the "AFNet Update 2 delivery order"), it received alarming information from one of its technical advisors, MITRE Corporation: MITRE predicted that due to increased network traffic, AFNet gateway security would experience total failure by April 12, 2012. *See* AR 18-566 (Final Price Negotiation Memorandum Addendum for Modification 2 to General Dynamics's NETCENTS Contract (Jan. 26, 2012)); *see also* AR 55 (MITRE Predicted Failure Timeline (Sept. 1, 2011)). The AFNet Update 2 Delivery Order was modified to reflect an expedited completion date of March 6, 2012, and included a requirement for both an updated firewall and an updated intrusion prevention system. AR 54-2370, 2377 (AFNet Update 2 Delivery Order). The AFNet Update 2 delivery order was awarded in December 2011. *Id.* at 2363. Prior to AFNet Update 2, the sixteen Air Force gateways were using intrusion prevention software from McAfee, namely the [***]. *See* AR 57-2742 (General Dynamics Response to AFNet RFP (Dec. 8, 2011)). The firewall in use at the time was designed by another software company, [***]. *See* AR 24-823 (Modification Proposal, (Mar. 9, 2012)). General Dynamics recommended that in light of the expedited schedule, the fastest and best way to upgrade the Air Force network would be to install the newest version of the same software already in use. AR 57-2742. The Air Force adopted this recommendation and incorporated it as modification of the delivery order that ultimately issued. *See* AR 19 (Modification 02 to Delivery Order No. RSFB (Feb. 9, 2012)).

2. *Trouble at the base level.*

As AFNet was coping with the expedited update schedule on the Air Force gateways in 2011 and 2012, base level network security was experiencing its own difficulties. Because AFNet abandoned direct management of the base boundaries, the Air Force had secured them in part by using a device called the Automated Security Incident Measurement Sensor ("the

sensor"). *See* AR 71-3004 (Modification Proposal (Mar. 9, 2012)). Due to "failing equipment, [sensor] overload and labor intensive management of the current system," the sensor had to be removed from the base boundaries, leaving them unacceptably vulnerable. *See* AR 63-2868 (E-mail between Air Force personnel (Jan. 18, 2012)). The decision to decommission the sensor was set to be implemented in April 2012. AR 36-1570 (Engineering Change Proposal (Sept. 19, 2012)).[6] The Air Force had been using Generic Routing Encapsulations ("GREs") as a band-aid over the failing sensor, but it had concerns over the steep cost of continuing to purchase GREs in light of the sensor's deteriorating condition. *See* AR 12-497 (E-mail between Air Force personnel (Aug. 20, 2011)).

With the impending sensor decommission looming over the base boundaries, the Air Force scrambled to prevent network shut-down by increasing security elsewhere. ENFAAS (then referred to as the Enclave Control Node) was only just coming into being, and would not be ready in time to manage the base boundaries' security gaps by April 2012. *See* AR 24-823 (Modification Proposal (Mar. 9, 2012)). An interim solution was required until ENFAAS could take over administration of the base boundaries. *Id*. In search of a solution, the Air Force's Integrated Product Team held weekly meetings to explore emerging technologies, including nextgen firewalls, which could be implemented at the AFNet gateway to compensate for increased vulnerability at the base level. *See* AR 36-1570 (Engineering Change Proposal (Sept. 19, 2012)). Around August 2011, it appears that some of the internal conversations concerning how to cope with the base boundaries touched on the possibility of a sole-source, brand-name acquisition. *See* AR 12 (E-mail chain between Air Force personnel (Aug. 2011)).[7]

---

[6]The actual date of decommission is not apparent from the administrative record. An Air Force memorandum written on September 19, 2012 dates the sensor decommission to April 2012. *See* AR 36-1570. Similarly, the proposed modification dated March 9, 2012 states that "[the sensor] was decommissioned on 31 March 2012," AR 24-823, even though the reference was to a future, not a past date. In all events, it is evident that the sensor was decommissioned at some point during the spring of 2012, around the same time as AFNet Update 2 was adopted.

[7]In August 2011, an Air Force contracting official expressed concern about "hand pick[ing] a contractor" rather than defining capabilities. AR 12-490 (E-mail from Jacqueline Johnson to Air Force personnel (Aug. 23, 2011)). The contracting officer quoted FAR § 11.105:

> Agency requirements shall not be written so as to require a particular brand name, product, or feature of a product, peculiar to one manufacturer, thereby precluding consideration of a product manufactured by another company, unless the particular brand name or feature is essential to the [g]overnment's requirements, and market research indicates that other companies' similar products, or products lacking the particular feature, do not meet, or cannot be modified to meet, the agency's needs.

Id. She concluded that the Air Force officials were "getting out of their swim lane." *Id*.

In September 2011, the Air Force decided to acquire Palo Alto nextgen firewall devices for a proof-of-concept effort. *See* AR 74-3107 (Prototype Event/Test Report). The record does not reflect that proofs of concept were undertaken for other systems. The stated purpose of the proof-of-concept acquisition was to "shorten the overall lead-time" in the event of eventual implementation of the products. *Id.* Contemporaneously, Air Force personnel discussed again the possibility of a sole-source acquisition across the board for gateways and base boundaries, debating whether "commonality with the enterprise" could support a brand-name justification at this juncture. AR 13 (E-mail chain between Air Force personnel (Sept. 2011)).[8]

On December 22, 2011, the Air Force requested a sum of money for the purchase of Palo Alto equipment for use in this proof of concept, termed an "Operational Requirement Assessment." AR 73-3076 (Request for Funding). The funds were authorized on January 12, 2012. *Id.* at 3078 (Fund Cite Authorization). The proof-of-concept assessment spanned several months, extending through March of 2012. *Id.* at 3098 (Modification of Contract (Mar. 30, 2012)). The government represents that, at the end of the proof-of-concept period, the Palo Alto products were uninstalled. Hr'g Tr. 31:21-25 (June 13, 2013).[9]

While the proof-of-concept assessment was still ongoing, Air Force personnel were already discussing ways to integrate the "emerging requirement" of a gateway nextgen firewall project into the current AFNet delivery order as quickly as possible. *See* AR 59 (Feb. 2012 e-mails between Air Force personnel).

On March 9, 2012, the Integrated Product Team issued a set of proposed modifications to the AFNet Upgrade 2 Delivery Order, which included deployment of nextgen firewalls at AFNet gateways, with the caveat that the nextgen system must be "tightly integrated with a full packet capture and forensics system so that security events from the [nextgen firewall] can be used to directly launch queries within the packet capture system." AR 24-824 (Proposal for Modification 06 to Delivery Order No. RSFB (Mar. 9, 2012)). Such a firewall, the team posited, would meet the interim requirement and prevent network shut-down when the sensors went offline at the base boundaries. *See id.* That same day, an Air Force Supervisory Contracting Officer informed General Dynamics that it should "hold off on purchasing all of the equipment for [AFNet Update 2]," indicating that further instructions would be forthcoming. AR 25-827 (E-mail from Debbie Hamilton, Supervisory Contracting Officer, Air Force, to Nathan Keller, General Dynamics).

On March 20, 2012, five courses of action ("COAs") were presented to Air Force management. AR 64-2875 to -2892 (COA Presentation Slides). Each of the five COAs included

[8]In September 2011, a second Air Force contracting official commented that "[b]rand [n]ame justifications cannot be supported due to commonality at initial introduction into the system[;] there needs to be a greater rationale, such as a system is on the network and accredited, etc." AR 13-498 (E-mail from Ed Coyne to Jonathan Kelley, Paul McIntyre, and Peter Jenny (Sept. 30, 2011)).

[9]Further references to the transcript of the hearing on the merits held on June 13, 2013, will omit the date.

a nextgen component, but varied over whether and to what extent additional security software such as McAfee's would also be employed. COA 5, which detailed a combination of nextgen firewall, full-packet-capture software, and McAfee's [***], was the recommended solution at the March 20 meeting. *Id.* at 2888, 2891. It was rated as "[b]est value," "[m]ost cost effective," and "[l]owest security risk" of all the proposed COAs. *Id.* at 2891.

Nonetheless, the Air Force opted not to adopt the recommended COA, and instead chose to proceed with COA 2. *See* Hr'g Tr. 119:20-21. COA 2 incorporated a nextgen firewall and a full-packet-capture system, but [***]. AR 64-2883 (COA Presentation Slides). One of the [***]. *Id.* Furthermore, COA 2 was rated "[t]oo expensive," and predicted to be "[u]nable to meet target date." *Id.* In spite of these drawbacks, the Air Force decided to implement COA 2, effectively moving Air Force networks to a sole-source security configuration and eliminating from any potential competition those software companies which did not offer fully integrated nextgen technology and full-packet capture.[10]

On April 6, 2012, the Air Force moved to implement COA 2 by issuing an informal advance Request for Proposal ("RFP") to General Dynamics, which included an explanation of the technical requirements the new AFNet Update 2 would need to meet. AR 71 (Advance RFP). The advance RFP did not contain specific brand-name preferences, but reflected detailed program requirements comporting with and expanding on those in the March 9, 2012 proposed modifications to the AFNet Upgrade 2 Delivery Order. *Id.*

On April 12, 2012, General Dynamics responded to the requirements posited informally by the Air Force. *See* AR 27 (Response to TRD). In its response to the informal RFP, General Dynamics recommended the Palo Alto [***] nextgen firewall, citing to market research performed in 2011, as well as to particular program features, as the basis for this recommendation. *Id.* at 880. General Dynamics referred to the "2011 Magic Quadrant for Enterprise Network Firewalls," noting that Palo Alto had been recognized as a leader in the upper-right quadrant. *Id.*[11] According to General Dynamics, Palo Alto's software and devices "me[t] or exceed[ed]" all requirements provided in the RFP. *Id.* Neither General Dynamics nor the Air Force held a competitive solicitation for a nextgen firewall provider.

The Magic Quadrant identifies at least one other software company, Check Point Software Technologies, as a leader in firewall technology with nextgen firewall products. *See* AR 72-3021 ([***]). The accompanying [***] McAfee did not have a fully integrated nextgen product in 2011. *See* AR 15-535 ([***]).

[10]The requirements as issued state that the firewall and full packet capture program must be "tightly integrated so that security events from the [nextgen firewall] can be used to directly launch queries within the [full packet capture program]." AR 27-882 (Response to Technical Requirements Document ("TRD")). This edict essentially amounts to a requirement that the two programs be manufactured by the same company, or sole source.

[11]The "Magic Quadrant" is a graphic representation of software providers and their current capabilities, generated annually by Gartner, Inc., a technology research group.

On April 16, 2012, the Air Force authorized General Dynamics to proceed with AFNet Update 2 with the changes as recommended in COA 2, replacing McAfee and [***] software with the Palo Alto nextgen firewall program. *See* AR 28 (E-mail from Debbie Hamilton to General Dynamics). The official RFP was issued on May 3, 2012, incorporating the earlier TRD, at which point formalities were observed to make the modification to AFNet Update 2 official. *See* AR 29 (RFP). The parties refer to this step as "modification 6," and the court will use this shorthand going forward. The portion of the TRD related to nextgen firewalls does not contain a specific brand-name requirement. AR 29-934 to -938. It does require that the nextgen firewall be configured "to perform [sensor] functionality of base [and] . . . to replace [intrusion prevention software] and [classic firewall] functionality." AR 29-936. It goes on to specify that the nextgen firewall must perform "[a]pplication identification," "content filtering" and "[t]hreat detection." AR 29-937. By the time the sensor went offline at the base boundaries, the Air Force had in place its nextgen firewall contingency plan at the gateway level, and no network shutdown was required.

3. *Bringing the base boundaries up to par.*

Although the installation of nextgen firewalls at the Air Force gateways staved off network failure, the Air Force nevertheless needed to improve security at the base boundaries after the sensor went offline. To that end, on October 11, 2012, the Air Force requested that ENFAAS develop a request for proposals "that includes a Next Generation Firewall . . . to secure the base boundary." AR 39-1662 (ENFAAS Procurement Directive (Oct. 11, 2012)).

In November 2012, MITRE investigated the possibility of installing non-Palo Alto nextgen firewalls at the base boundaries, which it assumed would require replacement of the gateway firewalls as well.[12] Specifically, MITRE attempted to calculate the cost of such a replacement. MITRE determined that the removal of Palo Alto from the gateways and replacement with a non-Palo Alto software (referred to as the "rip and replace") would cost roughly $[***]. AR 41-1685 (E-mail from Jeff D'Amelia, MITRE, to Amy Smith, Air Force (Nov. 26, 2012)). If the Air Force proceeded with its plan of implementing a common management component between the gateways and the base boundaries, the rip and replace would become necessary only if a vendor other than Palo Alto was selected for the base boundaries. Notably, the court cannot find in the administrative record any indication that either the Air Force or MITRE seriously considered whether it would be possible to install a second management platform to run a non-integrated component of the network security system, at least after the Air Force's choice of COA 2 in March 2012. Correlatively, other than the MITRE assessment, the Air Force does not appear to have contemplated any use of a fully integrated common management platform other than that provided by Palo Alto.

[12]MITRE considered that replacement of the gateway Palo Alto firewalls would be required if a non-Palo Alto system was installed at the boundaries, so that the gateways and base boundaries could run on the same management platform. AR 41-1683 (E-mail from Jeff D'Amelia, MITRE, to Amy Smith, Air Force (Nov. 26, 2012)) (indicating that the Air Force was looking for a "common management component").

In January 2013, ENFAAS issued a Brand Name Justification, stating that it intended to use a Palo Alto nextgen firewall at the base boundaries. *See* AR 44-1707 to 1711 (Brand Name Justification (Jan. 2013)). Under FAR § 16.505(a)(4), procurements may be performed on a brand-name basis if certain requirements are met, namely that "[t]he contracting officer must justify restricting consideration to an item peculiar to one manufacturer." FAR § 16.505(a)(4)(i). The justification offered by ENFAAS hinged on the fact that "Palo Alto [nextgen firewalls] are the only devices that can integrate with the existing [AFNet] management system. . . . Without Palo Alto [nextgen firewalls at the base level,] enterprise management of the [nextgen firewalls] deployed as part of ENFAAS would not be achievable." AR 44-1709. The Brand Name Justification indicates that the Air Force desires "to deploy identical policy configurations, identical software/firmware updates, identical hot fixes, identical patches, identical application signature updates, identical threat signature updates and identical custom signatures to all systems at the [AFNet gateways] and [ENFAAS base boundaries]." *Id*. To accomplish these goals, the systems at the gateways and the base boundaries must be controlled by the same management system. *Id*. Because the gateways were already operating on a Palo Alto management system, the base boundaries had to run Palo Alto software to integrate with the existing infrastructure. *Id*.

On February 11, 2013, the Air Force issued a Request for Proposal ("RFP") under NETCENTS requesting a solution for ENFAAS security comprised of a nextgen firewall which would be compatible with the system installed by AFNet through modification 6. *See* AR 45 (ENFAAS RFP).[13] This RFP contained a brand-name requirement for Palo Alto nextgen firewall products. *Id.* at 1715 ("These brand name items are required, no substitutions are authorized.").

The ENFAAS task order has not yet been awarded. McAfee filed suit in this court on March 19, 2013, alleging that the Air Force's decision to convert to a sole-source system improperly denies it the opportunity to compete as a subcontractor for such NETCENTS projects as the pending ENFAAS contract. Compl. ¶ 1. On May 3, 2013, McAfee filed a motion for judgment on the administrative record, *see* Pl.'s Mot. for Judgment on the Admin. Record ("Pl.'s Mot."), ECF No. 20, and the government concurrently filed a motion to dismiss pursuant to Rule 12(b)(1) of the Rules of the Court of Federal Claims ("RCFC"), or in the alternative, for judgment on the administrative record, *see* Def.'s Mot. A hearing was held on June 13, 2013.

JURISDICTION

McAfee predicates the court's jurisdiction upon the Tucker Act as amended by the Administrative Dispute Resolution Act, Pub. L. No. 104-320, § 12, 110 Stat. 3870, 3874 (Oct. 19, 1996) (codified at 28 U.S.C. § 1491(b)(1)). Compl. ¶ 6. In pertinent part, that statutory

[13]While the accompanying memorandum is dated February 11, 2013, the RFP itself is dated January 31, 2012. AR 45-1713 to 14. Given the facts that in January 2012, the proof of concept had not even been completed and that Palo Alto's system had not yet been implemented in the AFNet gateways, the court regards the January 31, 2012 date as a typographical error where January 31, 2013 was meant. The Air Force could not possibly have requested base boundary security "that can integrate with the existing Air Force . . . [g]ateways management system," AR 45-1715, before the gateway management system existed.

provision grants the court juridical power

> to render judgment on an action by an interested party objecting to a solicitation by a [f]ederal agency for bids or proposals for a proposed contract or to a proposed award or the award of a contract or any alleged violation of a statute or regulation in connection with a procurement or a proposed procurement.

28 U.S.C. § 1491(b)(1). The government contests jurisdiction on two grounds: first, that this court cannot review an in-scope modification of a pre-existing delivery order issued in accord with an IDIQ contract, such as modification 6, and second that McAfee lacks standing as an interested party to bring this suit in relation to the ENFAAS solicitation. Def.'s Mot. at 24-33.

When considering a motion to dismiss for lack of jurisdiction, the court will construe alleged facts in the light most favorable to the pleader. *Reynolds v. Army & Air Force Exch. Serv.*, 846 F.2d 746, 747 (Fed. Cir. 1988)). Nevertheless, the plaintiff bears the burden of establishing subject matter jurisdiction by a preponderance of the evidence. *McNutt v. General Motors Acceptance Corp. of Ind.*, 298 U.S. 178, 189 (1936); *Reynolds*, 846 F.2d at 748 (citing *Zunamon v. Brown*, 418 F.2d 883, 886 (8th Cir. 1969)).

A. *Modification 6 of the AFNet Update 2 Delivery Order*

The government points out, correctly, that this court has no jurisdiction to review an in-scope modification of a delivery order issued under a contract that was competitively awarded. Def.'s Mot. at 25; *see AT&T Commc'ns, Inc. v. Wiltel, Inc.*, 1 F.3d 1201, 1205 (Fed. Cir. 1993) ("[O]nly modifications outside the scope of the original competed contract fall under the statutory competition requirement."). Modification 6 technically is a modification of the AFNet Update 2 delivery order issued to General Dynamics under the firm's NETCENTS IDIQ Contract. *See supra* pp. 7-9. If McAfee sought the court's review of modification 6, it would face the daunting task of demonstrating that modification 6 did more than merely "add[] work to an existing contract that is clearly within the scope of the contract." *Distributed Solutions, Inc. v. United States*, 539 F.3d 1340, 1346 (Fed. Cir. 2008); *see also* 41 U.S.C. § 3105(b)(1) ("[A] contract is a new contract unless the work provided for in the contract is a continuation of the work performed by the specified entity under a prior contract."). Furthermore, the government argues, McAfee cannot challenge the original award of the delivery order because this court does not have jurisdiction to review such orders, unless the court is presented with "a protest on the ground that the order increases the scope, period, or maximum value of the contract under which the order is issued." Def.'s Mot. at 26 (quoting 10 U.S.C. § 2304c(e)(1)).

Nonetheless, the jurisdictional analysis pertinent here is much less complex than that postulated by the government. The predicate for McAfee's claim is not modification 6 of the AFNet Update 2 delivery order issued to General Dynamics. Rather, what McAfee actually challenges is the underlying decision by the Air Force to standardize its network security structure using a sole-source nextgen scheme. *See* Compl. ¶ 1 ("This action protests *the decision* of the [Air Force] to acquire by brand name and without proper competition [Palo Alto

products].") (emphasis added). This decision is not tied to any single solicitation or delivery order, but encompasses the whole of the Air Force's procurement of a new network security structure. McAfee alleges that the Air Force violated 41 U.S.C. § 3301 and 10 U.S.C. § 2304(a) when it determined, without competition, to move from multiple-source security to sole-source security, effectively cutting out McAfee and all security providers other than Palo Alto. Pl.'s Mem. in Support of Mot. for Judgment on the Admin. Record ("Pl.'s Mem."), ECF No. 21, at 19. As such, McAfee's complaint falls under the third prong of Section 1491(b)(1), concerning an alleged "violation of statute or regulation in connection with a procurement or a proposed procurement." 28 U.S.C. § 1491(b)(1); *see also Rothe Dev., Inc. v. United States Dep't of Def.*, 666 F.3d 336, 338 (5th Cir. 2011) ("[T]he Court of Federal Claims now retains exclusive jurisdiction over 'action[s] by an interested party' 'objecting to . . . any alleged violation of statute or regulation in connection with a procurement or a proposed procurement.'" (citing 28 U.S.C. § 1491(b)(1))).

The third prong of Section 1491(b)(1) is "very sweeping in scope." *Angelica Textile Servs., Inc. v. United States*, 95 Fed. Cl. 208, 215 (2010) (citing *RAMCOR Servs. Group, Inc. v. United States*, 185 F.3d 1286, 1289 (Fed. Cir. 1999)). "[A] procurement 'includes all stages of the process of acquiring property or services, beginning with the process for determining a need for property or services and ending with the contract completion and closeout.'" *Id.* (quoting 41 U.S.C. § 403(2), now codified at 41 U.S.C. § 111); *see also Distributed Solutions*, 539 F.3d at 1346 ("[For jurisdiction, a 'procurement'] involves a connection with any stage of the federal contracting acquisition process, including the process for determining a need for property or services.") (internal quotations omitted); *OTI America, Inc. v. United States*, 68 Fed. Cl. 108, 117 (2005) (holding that the "broad language" of Subsection 1491(b) demonstrated "Congress's expressed intent that the Subsection encompass the entire procurement process").

The Air Force began the process of determining its need for a new generation of network security services long before it issued the delivery order for AFNet Update 2, let alone modified it. The original AFNet Update 2 delivery order to General Dynamics, structured in a non-sole-source manner, was issued on December 9, 2011. *See* AR 54 (AFNet Update 2 delivery order). Considerably earlier than that, in February 2011, ten months prior to the original AFNet Update 2 order, the Air Force had begun to inform its eventual decision to switch to nextgen technology by issuing the Request for Information. *See* AR 52 (2011 RFI). By the time modification 6 occurred, the Air Force was far along in the decision-making process, indeed, nearly finished with it. Modification 6 was but one further step in a series of moves that had already been taken by the Air Force to implement its decision to shift the entire network to sole-source security. As such, McAfee's complaint does not turn on modification 6, and, to establish jurisdiction, McAfee need not demonstrate any change in scope from the original AFNet Update 2 delivery order to the modified delivery order. *See RAMCOR*, 185 F.3d at 1289 ("§ 1491(b) . . . does not require an objection to the actual contract procurement. . . . As long as a statute has a connection to a procurement proposal, an alleged violation suffices to supply jurisdiction.").[14]

[14]The government also makes the argument that McAfee as a subcontractor lacks privity of contract with the Air Force and thus may not sue the government directly. Def.'s Mot. at 30. As explained above, McAfee does not premise jurisdiction either on the AFNet Update 2 delivery order or on the NETCENTS IDIQ contracts, so privity of contract is not at issue.

B. *The ENFAAS Solicitation*

The government challenges this court's jurisdiction over the brand-name restriction in the ENFAAS task order (which has not yet been awarded) on the same statutory grounds as it challenges jurisdiction over modification 6 to the AFNet Update 2 delivery order. Specifically, the government argues that this court does not have jurisdiction over the delivery order itself and thus cannot consider McAfee's arguments here. Def.'s Mot. at 31. For the same reasons as those described above in relation to modification 6, this objection is unavailing. McAfee does not challenge the delivery order in and of itself, but rather the decision made by the Air Force to standardize its entire network security scheme. The ENFAAS solicitation is but another stepping stone in the culmination of this challenged decision.

The government additionally attacks McAfee's standing to raise a sole-source challenge. McAfee, the government argues, is not an "interested party" to the ENFAAS solicitation, and consequently cannot protest the bidding or lack thereof on that solicitation. Def.'s Mot. at 31 (citing 28 U.S.C. § 1491(b)(1)). It argues that because McAfee is not a NETCENTS contractor, it could not possibly have submitted a bid on the ENFAAS solicitation. *Id*. at 32.

To qualify as an interested party to a bid protest under section 1491(b)(1), a party must be an "actual or prospective bidder[] or offeror[] whose direct economic interest would be affected by the award of the contract or by the failure to award the contract." *American Federation of Gov't Emps., AFL-CIO v. United States*, 258 F.3d 1294, 1302 (Fed. Cir. 2001), *modified in another respect by Weeks Marine Inc. v. United States*, 575 F.3d 1352, 1359-62 (Fed. Cir. 2009); *see also Rex Serv. Corp. v. United States*, 448 F.3d 1305, 1307 (Fed. Cir. 2006) (noting that the term "interested party" has the same meaning in both Section 1491(b)(1) and in CICA). McAfee is neither an actual nor a prospective bidder on the ENFAAS contract. Even if there had been no brand-name requirement for the ENFAAS solicitation, McAfee could not have competed directly for the award due to its lack of NETCENTS qualification. At best, McAfee could have been a subcontractor to a NETCENTS awardee, which NETCENTS concern would have been the primary contractor with the government. As a mere subcontractor, McAfee would not possess standing to challenge the terms of the solicitation. *See Distributed Solutions*, 539 F.3d at 1344 (noting that mere "disappointed subcontractors" do not have standing in a bid protest).

Again, however, the government misses the thrust of McAfee's complaint with this standing argument. McAfee objects to the fact that the entire Air Force network scheme is premised on a sole source of fully integrated nextgen technology. Pl.'s Mem. at 1-2. The ENFAAS solicitation, much like modification 6 of the AFNet Update 2 delivery order, represents one incremental step towards the Air Force's ultimate goal: complete control over the entirety of network security via a single management system. The affirmative decision to standardize the entire network system was made when the Air Force adopted COA 2 rather than COA 5. *See supra* p. 8. Had the Air Force pursued COA 5 (or any of the non-standardized COAs), McAfee would have been eligible to compete, as would a number of other network-security providers, some with fully integrated systems and some with add-ons. COA 2, however, precluded all manufacturers who did not offer a specific type of fully integrated single-source nextgen solution, *i.e.*, any system other than that produced by Palo Alto, from competing for Air

Force network-security procurements. But for the decision to standardize with Palo Alto, McAfee would have had a substantial chance of continuing in its role as a security services provider for the Air Force.

The court's reasoning in *Savantage Fin. Servs., Inc. v. United States*, 81 Fed. Cl. 300 (2008), is instructive on the question of standing. In *Savantage*, the Department of Homeland Security determined to standardize its financial systems application software by selecting a particular program without competition, issuing a Brand Name Justification, and then conducting a solicitation for implementation services only. 81 Fed. Cl. at 302-03. The implementation task order was open to prospective offerors from a specific IDIQ only. *Id.* The plaintiff was not a member of the IDIQ, and furthermore could not offer the services requested by the solicitation; however, it did provide a financial software at the time which could have served the government's needs. *Id*. at 306.

The court in *Savantage* determined that the government's standardization decision qualified as a "procurement" through which the plaintiff could establish jurisdiction. 81 Fed. Cl. at 305 ("[D]efendant has not identified any competitive process through which [the government] decided to standardize to Oracle and SAP financial systems application software. The failure to make that determination through a competitive process is exactly what [plaintiff] is protesting."). The court held that the plaintiff had standing, even though it was not eligible to receive the only actual task order issued in relation to the matter: "Because plaintiff currently supplies a competitive . . . software system to [the government], it clearly could have competed for the contract if [the government] had bid it out. Furthermore, defendant has failed to point to any reason why plaintiff would not have been a qualified bidder to supply such a system. Therefore, plaintiff has standing to protest [the government's] decision." *Id*. at 306; *see also Myers Investigative & Sec. Servs., Inc. v. United States*, 275 F.3d 1366, 1370 (Fed. Cir. 2002) ("To have standing, the plaintiff need only establish that it 'could compete for the contract' if the bid process were made competitive." (quoting *Impresa Construzioni Geom. Domenico Garufi v. United States*, 238 F.3d 1324, 1334 (Fed. Cir. 2001)).

The government argues that McAfee is in a position similar to that of the plaintiff in *DataMill, Inc. v. United States*, 91 Fed. Cl. 740 (2010). Def.'s Mot. at 27-30. In *DataMill*, an incumbent contractor objected to the award of a delivery order to a competitor under an already-existing Navy contract held by the competitor. 91 Fed. Cl. at 751. The court determined that there was no jurisdiction, even though the incumbent contractor attempted to characterize its suit as a protest of the decision not to conduct a competition and instead to issue the delivery order. *Id*. at 755. Because the *DataMill* plaintiff had "not alleged that the delivery order in this case exceeded the scope, period, or maximum value of the [c]ontract," its objection to the delivery order itself could not be salvaged by framing it in terms of the decision to proceed without competition. *Id*. at 762.

The present case is distinguishable from *DataMill*. As the court noted in *Bayfirst Solutions, LLC v. United States*, 104 Fed. Cl. 493 (2012), "it may be that each protest requires a fact-intensive inquiry as to the agency's decision-making process, and a careful analysis of the connectedness of each challenged procurement decision to the issuance or proposed issuance of a task order." *Id*. at 503. In the instant case, the protested decision is not directly connected to the

award of any particular delivery order. McAfee protests a decision made by the Air Force to standardize an entire system — a decision connected to the procurement process, but not to a specific delivery order. Both modification 6 and the ENFAAS solicitation are simply natural consequences of the decision, but neither comprises the jurisdictional basis of this protest.

McAfee is in a position comparable to that of the *Savantage* plaintiff. Although it may have been a subcontractor at best to any NETCENTS contractor, the government cannot escape its obligation to conduct competition by delegating the task of source selection to a competitively selected primary contractor. *See Distributed Solutions*, 539 F.3d at 1346 ("While the government ultimately decided not to procure software itself from the vendors, but rather to add that work to its existing contract with [a primary contractor], the statute does not require an actual procurement."). McAfee complains of the decision to pursue a sole-source course of action, which the Air Force considered as an alternative to at least four other courses of action which involved a variety of potential software vendors, including McAfee. *See* AR 64 (COA Presentation Slides). The Air Force made the decision to implement COA 2, and General Dynamics as the designated NETCENTS contractor was implementing the Air Force's decision through modification 6 of the AFNet Update 2 delivery order and the ENFAAS solicitation. Thus, McAfee has demonstrated that it is an interested party to the procurement decisions made by the Air Force in relation to its cyber security needs.

The court has jurisdiction to consider McAfee's suit under 28 U.S.C. § 1491(b)(1).

DISCUSSION

A. *Standard for Decision*

The primary standard for decision in a bid protest is specified in 28 U.S.C. § 1491(b)(4) ("In any action under this [S]ubsection, the courts shall review the agency's decision pursuant to the standards set forth in [S]ection 706 of title 5."). Under the Administrative Procedure Act ("APA"), the court may set aside an agency's procurement decision if it is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law," 5 U.S.C. § 706, subject to satisfying the criteria for equitable relief, *see PGBA, LLC v. United States*, 389 F.3d 1219, 1224-28 (Fed. Cir. 2004). In other words, to rescind a procurement decision, the court must find that the "decision lacked a rational basis; or . . . the procurement procedure involved a violation of regulation or procedure." *Impresa Construzioni Geom. Domenico Garufi*, 238 F.3d at 1332; *see also Superior Helicopter, LLC v. United States*, 78 Fed. Cl. 181, 187 (2007). The court may not "substitute its judgment for that of the agency" during its analysis. *Keeton Corrs., Inc. v. United States*, 59 Fed. Cl. 753, 755 (2004) (quoting *Citizens to Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 402, 416 (1971), *abrogated in part by Califano v. Sanders*, 430 U.S. 99, 105 (1977) (abrogating *Overton Park* to the extent it reorganized the APA as an independent grant of subject matter jurisdiction). To afford relief, it must find a that the procurement decision was not "based on a consideration of the relevant factors," or that there has been a "clear error of judgment." *Overton Park*, 401 U.S. at 416. The plaintiff must show this clear error or violation of relevant statute or regulation by a preponderance of the evidence. *Gentex Corp. v. United States*, 58 Fed. Cl. 634, 648 (2003) (citing *Information Tech. & Applications Corp. v. United States*, 51 Fed. Cl. 340 (2001), *aff'd* 316 F.3d 1312 (Fed. Cir. 2003)).

B. *Analysis*

McAfee alleges that the Air Force violated CICA, 41 U.S.C. § 3301, as well as 10 U.S.C. § 2304(a), and certain provisions of the FAR, when it failed to conduct a competition or provide appropriate justification prior to its decision to shift to a sole-source network security scheme. Compl. ¶¶ 22-25; Pl.'s Mem. at 19. McAfee also characterizes the Air Force's exclusive selection of Palo Alto products as arbitrary and capricious. Compl. ¶¶ 26-27.

1. Improper procurement.

The statutory underpinnings of the governmental procurement process require competition in almost every conceivable scenario. CICA states that for public contracts, with only narrow, specific exceptions,

> an executive agency in conducting a procurement for property or services shall—
> (1) Obtain full and open competition through the use of competitive procedures in accordance with the requirements of this division and the [FAR]; and
> (2) Use the competitive procedure or combination of competitive procedures that is best suited under the circumstances of the procurement.

41 U.S.C. § 3301(a). Almost identical language is reiterated in specific reference to procurements conducted by the Armed Forces in 10 U.S.C. § 2304(a). Both statutes indicate that procurements must be conducted "in accordance with the [FAR]." 41 U.S.C. § 3301(a); 10 U.S.C. § 2304(a).

The administrative record manifestly demonstrates that the Air Force did not conduct an open competition for its network security needs prior to selecting COA 2. It did not issue a direct solicitation, nor did it instruct any of its NETCENTS contractors to hold one. Yet, with the selection of COA 2 in 2012, the entirety of the Air Force's network security infrastructure was directed towards a sole-source standardization.

The enumerated exceptions to the statutory directives for competition are narrow and do not apply here. The first such exception is whether "the property or services needed by the agency are available from only one responsible source or only from a limited number of responsible sources and no other type of property or services will satisfy the needs of the agency." 10 U.S.C. § 2304(c)(1). At the point in time when the Air Force decided to pursue sole-source network security software, it was fully aware of other sources or combinations of sources which could have provided network security. *See* AR 64-2875 to -2892 (COA Presentation Slides). However, even before the COA presentation in March 2012, the Air Force had expressed its preference for a sole-source plan. *See* AR 64-2883 (noting as the only "pro" for COA 2 that it "[m]eets [the Air Force's] original request"). The Air Force cannot claim that there were no other options available but to pursue the sole-source procurement, and cannot justify its failure to evaluate other options competitively. *See Savantage*, 81 Fed. Cl. at 308 ("[S]o long as there is more than one source competent to perform the contract, [the government] must evaluate the merit of each offeror's product through the competitive lens.").

The second enumerated exception to competitive procurement arises where "the agency's need for the property or services is of such an unusual and compelling urgency that the United States would be seriously injured unless the agency is permitted to limit the number of sources from which it solicits bids or proposals." 10 U.S.C. § 2304(c)(2). Yet COA 2, the sole-source option, was not the fastest course of action presented to the Air Force in 2012. In fact, COA 1 is listed as the "[f]astest COA," belying any possible assertion that a compelling urgency mandated the selection of COA 2 instead. AR 64-2882 (COA Presentation Slides).

The remaining exceptions to competitive procurement are no less availing for the government. The third allows non-competitive procurements if needed to maintain suppliers during a national emergency, if a nonprofit or federally funded research center must be established or maintained, or if services are required for litigation. 10 U.S.C. § 2304(c)(3). The fourth and fifth exceptions concern situations where international treaties or express statutes mandate other than competitive procedures. *Id.* § 2304(c)(4)-(5). The sixth exception allows an agency to dispense with competition if disclosing the needs in an open solicitation would compromise national security. *Id.* § 2304(c)(6). Finally, the seventh exception to competitive procurements requires simply that it be "necessary in the public interest" to use non-competitive procedures; however, in such a case, the head of the agency must notify Congress in writing of such a determination "no less than 30 days before the award of the contract." *Id.* § 2304(c)(7). None of these situations apply here.

The government contends that its discrete procurement actions (modification 6 and the ENFAAS solicitation) violate neither CICA nor the FAR. Def.'s Mot. at 34-44. The government emphasizes that in-scope modifications are insulated from significant oversight and that the ENFAAS solicitation was accompanied by a Brand Name Justification. However, these particular actions cannot be considered in isolation. The cited actions are but steps taken to implement a broader scheme of standardization and sole-source procurement. The fact that the government may have taken ostensibly insulated steps to accomplish an improper goal does not redeem the government's actions. Rather, the court looks to the predicate decision to adopt a sole-source infrastructure. In that respect, the government's arguments are severely undercut by the commentaries of two Air Force contracting officials in August and September 2011 expressing concern about moving to a sole-source system without demonstrated justification. *See supra* nn.7-8. Given that there were known, additional, responsible, multiple-source options available to the Air Force at the time the key decision was made, its decision to use a sole-source security system without competition does not accord with CICA and its counterpart for the Department of Defense, 10 U.S.C. § 3204. *See Savantage*, 81 Fed. Cl. at 308; *ATA Def. Indus., Inc. v. United States*, 38 Fed. Cl. 489, 502 (1997) ("[T]he contracting officer reasonably was on notice that . . . certain of the products and services purchased under the contract on a sole source basis [were] available competitively. . . . The contracting officer's decision to purchase on a sole source basis $193,060 worth of goods and services that could have been purchased on the open market was an abuse of his discretion and not in accordance with law."), *abrogated on other*

grounds as recognized by Baltimore Gas and Elec. Co. v. United States, 290 F.3d 734 (4th Cir. 2002).[15]

2. *Prejudice.*

Relief in a bid protest is contingent not only upon the finding of an error in the procurement process, but also upon a showing that the error prejudiced the protestor. *See Data Gen. Corp. v. Johnson*, 78 F.3d 1556, 1562 (Fed. Cir. 1996). To establish that it has been prejudiced by the Air Force's improper procurement, McAfee must demonstrate a "substantial chance it would have received the [or a] contract award, but for the alleged error in the procurement process." *Gentex*, 58 Fed. Cl. at 653 (citing *Information Tech. & Applications*, 316 F.3d at 1319); *see also Alfa Laval Separation, Inc. v. United States*, 175 F.3d 1365, 1367 (Fed. Cir. 1999); *Data Gen.*, 78 F.3d at 1562.

McAfee has demonstrated that it was prejudiced by the Air Force's inappropriate procurement selection. Had the Air Force competed a solution to its network security needs, McAfee could have offered its products as discrete pieces of a bundle or composite compiled by a primary NETCENTS contractor precisely as it had done in the past. Furthermore, McAfee's [***] program, already in use on the network, was an integral part of the recommended COA 5 considered by the Air Force. *See* AR 64-2888. Given these circumstances, McAfee has shown that it had "greater than an insubstantial chance of securing [a] contract" once it succeeded on the merits of its protest. *Information Tech.*, 316 F.3d at 1319.

C. *Relief*

McAfee requests injunctive relief which would prohibit the Air Force from moving forward with any sole-source network security procurement. Pl.'s Mem. at 39. To grant permanent injunctive relief, the court must consider "whether (1) the plaintiff has succeeded on the merits, (2) the plaintiff will suffer irreparable harm if the court withholds injunctive relief, (3) the balance of hardships to the respective parties favors the grant of injunctive relief, and (4) the public interest is served by a grant of injunctive relief." *Centech Grp., Inc. v. United States*, 554 F.3d 1029, 1037 (Fed. Cir. 2009) (citing *PGBA, LLC v. United States*, 389 F.3d at 1228-29.

1. *Success on the merits.*

McAfee has succeeded on the merits of its case by showing that the Air Force improperly, and without competition, selected a sole-source network security framework. Accordingly, the first factor weighs in favor of the plaintiff.

[15]Although McAfee does not appear to have had a comparable nextgen firewall *product* at the time of these determinations, *see* AR 72.1-3036 ([***]); AR 15-535 ([***]), it represents that it had available a combination of programs capable of providing the same *service*, *see* AR 53-2279 (McAfee's Response to RFI). It may be that this combination approach would have ultimately proved less effective than a unified nextgen system; however, the court does not have that information before it, as the Air Force never competed the two solutions against one another. Other vendors were also potential competitors because they did have fully integrated systems.

2. *Irreparable harm.*

McAfee argues that it will suffer irreparable harm in the form of an "organizational lock-in" on the Air Force's network security needs, citing *Google, Inc. v. United States*, 95 Fed. Cl. 661 (2011). Pl.'s Opp'n to Def.'s Mot. for Judgment on the Admin. Record and Mot. to Dismiss ("Pl.'s Opp'n") at 25-27, ECF No. 32. In *Google*, the Department of the Interior attempted to acquire, without competition, Microsoft software to run e-mail and collaboration services. 95 Fed. Cl. at 662-63. The court held that Google had suffered irreparable harm because the acquisition of such e-mail services created organizational lock-in such that Google could not conceivably compete to provide that service then or in the future. *Id.* at 679. By standardizing network security, McAfee argues, the Air Force has similarly precluded McAfee and all other potential competitors from not only the opportunity to provide network security now, but also "the opportunity to compete to provide future versions and upgrades of its products." Pl.'s Opp'n at 26.

The government counters that no such organizational lock will result from the present procurement strategy. Instead, the Air Force represents that it intends to conduct a "refresh" three years after implementation of Palo Alto nextgen products at the base boundaries. Def.'s Mot. at 46. The government argues that, unlike the messaging software at issue in *Google*, cybersecurity solutions by their very nature must change, at times drastically, from one implementation to the next. *See* Hr'g Tr. 133:6 to 134:10.

On its facts, *Google* is instructive for this case but it does not mandate a particular result insofar as equitable relief is concerned. The court in *Google* noted that organizational lock-in would occur upon implementation of a Microsoft Office program as an across-the-board e-mail service at the Department of the Interior. 95 Fed. Cl. at 678. That lock-in was held to constitute immediate and irreparable harm to the plaintiff, which would lose any prospect of present or future competition once migration of the agency's e-mail system had been completed. *Id.* at 679. While McAfee may be in a similar position respecting immediate harm,[16] future competition may not be foreclosed.

Network security by its very nature is susceptible to drastic changes from one year to the next. *See* Hr'g Tr. 133:18 to 134:4. While Palo Alto's nextgen software may be the Air Force's preferred program this year, by the time the "refresh" occurs, advances in "hacking" and other offensive means may likely require a defensive move towards a completely different type of security program. Where e-mail programs serve finite, relatively predictable functions, cyber-security programs must adapt to a host of unique and unpredictable situations.

[16]McAfee will undoubtedly suffer an immediate harm in the form of lost contracts and orders which it might have been received in the near future had the Air Force chosen a option other than a sole-source provider for its current network security needs. Because a bid protest plaintiff cannot recover lost profits, this court has held that such losses constitute irreparable harm in the context of a bid protest. *See KWV, Inc. v. United States*, 108 Fed. Cl. 448, 457 (2013); *Hospital Klean of Tex, Inc. v. United States*, 65 Fed. Cl. 618, 624 (2005).

Any consideration of relief in this case necessarily focuses on an injunction. Because McAfee was never provided any opportunity to prepare a bid here, it cannot recover bid and proposal preparation costs — the only monetary recovery available to a bid protest plaintiff. *See* 28 U.S.C. § 1491(b)(2). In effect, if injunctive relief does not issue, McAfee will suffer an irreparable economic harm, and in fact will be unable to recover economic losses of any sort, such that this factor weighs in favor of the plaintiff.[17]

3. *Balance of hardships and public interest.*

The court must balance the potential harm to the plaintiff against the potential harm to the Air Force and to the awardee when considering injunctive relief. *Gentex*, 58 Fed. Cl. at 654. Although modification 6 applies to a General Dynamics contract and the ENFAAS solicitation has yet to be awarded, the court will treat Palo Alto as the sole-source provider of the products and services being procured. The potential harm to Palo Alto at this juncture is minimal to non-existent; Palo Alto products have already been purchased through modification 6, and injunctive relief unwinding that step of the standardization would drastically affect the Air Force's network security. Furthermore, every proposed COA included a nextgen firewall component. *See* AR 64 (COA Presentation Slides). As to the present solicitation for the ENFAAS update, removal of the brand-name justification would not realistically change Palo Alto's posture because the Air Force would still be running its management system.

The most pressing weight in this balancing equation is the potential harm to the Air Force and, by extension, the American public. The court is required to "give due regard to the interests of national defense and national security." 28 U.S.C. § 1491(b)(3). The government argues that "an injunction would adversely affect national security and would directly impact military operations worldwide." Def.'s Mot. at 47. The government and McAfee have submitted several affidavits which speak to the severity of this impact.[18] Air Force officials aver that any delay in

[17]The government has argued that such lost profits must rise to a level which "would significantly damage [plaintiff's] business above and beyond a simple diminution in profits." Def.'s Mot. at 46 (quoting *Air Transport Ass'n of Am., Inc. v. Export-Import Bank of the United States*, 840 F. Supp. 2d 327, 336 (D.D.C. 2012)). This argument rests upon decisions that are not binding on this court, which, as explained above, allows for the classification of general lost profits as irreparable harm in the bid-protest context. This court does not require that the plaintiff demonstrate a particular degree of severity in relation to its lost profits.

[18]In a bid protest, the parties build a factual record respecting equitable relief that largely exits independently from the administrative record of the procurement. *See Holloway & Co., PLLC v. United States*, 87 Fed. Cl. 381, 391 n.12 (2009) ("It is the responsibility of th[e] [c]ourt, not the administrative agency [conducting the procurement], to provide for factual proceedings directed toward, and to find facts relevant to, irreparability of harms or prejudice to any party or to the public interest through grant or denial of injunctive [or declaratory] relief.") (quoting *PGBA, LLC v. United States*, 60 Fed. Cl. 567 (2004), *aff'd*, 389 F.3d 1219 (Fed. Cir. 2004)); *see also AshBritt, Inc. v. United States*, 87 Fed. Cl. 344, 366-67 (2009) ("In general, it is appropriate to add evidence pertaining to . . . the factors governing injunctive relief to the record in a bid

obtaining and installing nextgen firewalls would put the network "at severely diminished capabilities and disadvantage against the average hacker and at a highly vulnerable posture to defend against any state-sponsored professionals it cannot see." Decl. of Richard J. DeLeon, Technical Advisor, 26th Network Operations Group, 67th Network Warfare Wing, U.S. Air Force ("DeLeon Decl."), ECF No. 22-1, ¶ 5. The government represents that these diminished capabilities make the networks susceptible to complete shutdown or infiltration by hostile forces. DeLeon Decl. ¶ 6. The current classic firewall and intrusion-prevention systems in place at the base boundaries "render [the] base network defenses obsolete and virtually blind to the new attack methods" of modern cyber enemies. *Id.* ¶ 5.

McAfee counters the government's arguments by averring that they are premised on use of [***] of McAfee's older firewall software that is currently installed by the Air Force. Pl.'s Opp'n at 27. If, McAfee argues, the Air Force upgraded to [***], the firewall's capabilities would be on par with those of the Palo Alto products which the Air Force currently intends to install, and at no additional licensing cost to the Air Force. *Id.* at 27-28 (citing the declaration of Scott Montgomery, Vice President of Public Sector Solutions, McAfee ("Montgomery Decl."), ECF No. 32-2, ¶¶ 5-7. The Air Force could, in theory, avoid the dire consequences of failure to install the fully integrated Palo Alto system by instead upgrading to McAfee's [***]. Montgomery Decl. ¶ 13. However, in making this argument, McAfee overlooks the nature of the relief it requests. If the court issued an injunction against the Air Force, prohibiting it from moving forward with its sole-source procurement, the Air Force would be faced with selecting McAfee's or another provider's products once again without competition, albeit on an interim basis. This likely prospect would frustrate the very process which McAfee has been thus far fighting to preserve: competitive selection of network security products. *See Al Ghanim Combined Grp. Co. v. United* States, 56 Fed. Cl. 502, 521 (2003) ("Plaintiff cannot direct the court to a vehicle for contracting that could be used to satisfy, during a period of resolicitation, the [government's] needs for the . . . services covered under the instant solicitation.").

Realistically, the court could instruct the Air Force to conduct a competitive procurement for its network security products and systems according to CICA and the FAR. Enforcing a competitive procurement process would unavoidably create delay in implementing updated technology at the base boundaries. The court has no information that any system other than that provided by Palo Alto has been applied on a proof-of-concept basis. *See supra* p. 7. Under the most concordant and harmonious circumstances, the procurement process would take considerable time to complete.

Bearing in mind that "allegations involving national security must be evaluated with the same analytical rigor as other allegations of potential harm to parties or to the public," *Gentex Corp.*, 58 Fed. Cl. at 655, the court finds that the national security interests at stake here are overpowering. The court cannot conclude that the government's attestations of urgent and

---

protest — not as a supplement to the [administrative record], but as part of this [c]ourt's record.").

The court accordingly admits into the record of the case those declarations that pertain to prejudice and injunctive relief.

present danger in the event of an injunction are without foundation. One need not look very hard to find very recent examples of cyber espionage.

McAfee has not controverted the government's assertions that an under-protected network would leave the Air Force unacceptably vulnerable, nor has McAfee suggested any methods for conducting a competitive solicitation without negatively affecting network security, at least for a time. In the absence of evidence to the contrary, the court finds that delay would damage national security as the government claims. *See Al Ghanim*, 56 Fed. Cl. at 522 ("In light of the parties' inability to provide the court with specific information regarding the impact of delay, the court must defer to the claim that national security concerns counsel against a grant of injunctive relief."). The resulting balance of hardships weighs in favor of the government and against the issuance of an injunction. *See Protection Strategies, Inc. v. United States*, 76 Fed. Cl. 225, 236-37 (2007) (weighing national security interests bearing on a shut-down of security systems at the Nevada Test Site). In this instance, the public's interest in maintaining national security outweighs adherence to the competitive procurement mandate in CICA, 41 U.S.C. § 3301, 10 U.S.C. § 2304, and the FAR, insofar as injunctive relief is concerned. *Id.*

CONCLUSION

For the foregoing reasons, McAfee's motion for judgment on the administrative record is GRANTED. The government's decision to procure and implement Palo Alto's network security system as a sole-source without competition contravenes CICA, 41 U.S.C. § 3301, 10 U.S.C. § 2304(a)(1), and the FAR. The government's motion to dismiss, or in the alternative, judgment on the administrative record is accordingly DENIED. Nonetheless, in light of the balancing of factors pertaining to the issuance of equitable relief, McAfee's request that the court enjoin the Air Force from moving forward with its procurement of Palo Alto software is DENIED. Moreover, because McAfee submitted no bid in the procurement at issue, the court may not award bid preparation and proposal costs under 28 U.S.C. § 1491(b)(2). In effect, this is a situation in which McAfee has demonstrated a violation by the Air Force of statutes and the FAR, but no viable remedy is at hand.

The clerk will enter judgment in accord with this disposition.

McAfee is awarded its costs of suit pursuant to RCFC 54(d).

It is so **ORDERED.**

s/ Charles F. Lettow
Charles F. Lettow
Judge