U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

Comptroller General
of the United States

Decision

Matter of: IPKeys Technologies, LLC

File: B-414890; B-414890.2

Date: October 4, 2017

John E. Jensen, Esq., Alexander B. Ginsberg, Esq., Travis L. Mullaney, Esq., and Megahn D. Doherty, Esq., Pillsbury Winthrop Shaw Pittman LLP, for the protester.
E. Sanderson Hoe, Esq., and Evan R. Sherwood, Esq., Covington & Burling, LLP, for By Light Professional IT Services, LLC, an intervenor.
Laura J. Barke, Esq., and Colleen A. Eagan, Esq., Defense Information Systems Agency, for the agency.
Evan D. Wesser, Esq., and Edward Goldstein, Esq., Office of the General Counsel, GAO, participated in the preparation of the decision.

DIGEST

1. Protest challenging the agency's evaluation of proposals is denied where the agency's evaluation was reasonable and consistent with the terms of the solicitation.

2. Protest alleging that the agency engaged in disparate treatment in the evaluation of proposals is denied where the different evaluation results were reasonably based on substantive differences between the proposals.

DECISION

IPKeys Technologies, LLC, a small business, of Stafford, Virginia, protests the issuance of a task order to By Light Professional IT Services, Inc., a small business, of Arlington, Virginia, under request for proposals (RFP) No. GSMETI00031, which was issued by the Defense Information Systems Agency (DISA), for engineering, transition, implementation, and sustainment support for video services.[1] IPKeys primarily challenges the agency's evaluation of technical proposals.

[1] The RFP was issued as a small business set-aside under DISA's Global Information Grid Services Management, Engineering, Transition, and Implementation (GSM-ETI) multiple-award indefinite-delivery, indefinite-quantity (IDIQ) contract. RFP at 1.

We deny the protest.

BACKGROUND

The RFP, which was issued to small business contractors under DISA's GSM-ETI multiple-award IDIQ contract, contemplated the award, on a "best-value" basis, of a cost-plus-fixed-fee task order for a base year and up to two 1-year option periods and one 5-month option period. RFP at 2.[2] The RFP sought proposals for the provision of engineering, transition, implementation, sustainment, and cybersecurity monitoring support services for DISA's Global Video Service (GVS). RFP, Performance Work Statement (PWS), at 2.[3]

For the purposes of conducting the best-value tradeoff evaluation, DISA was to consider two evaluation factors: (1) technical/management approach; and (2) cost. RFP at 4. The technical/management approach factor was to be more important than cost. Id. With respect to cost, the agency was to evaluate offerors' total proposed costs for completeness, reasonableness, and realism. Id. at 5. With respect to the technical/management factor, DISA was to evaluate four equally weighted subfactors (3 technical subfactors and a management subfactor). Id. at 4-5.

Under technical subfactor 1, offerors were to demonstrate (i) that their proposed architectures and designs incorporate support for current and emerging standards for video compression and call signaling associated with videoconferencing, and (ii) their knowledge of and aptitude with the unified capabilities requirements pertaining to architectures and designs, including the integration of video with the unified capabilities voice and multimedia collaboration services. Id. at 4. Under technical subfactor 2, offerors were to demonstrate their ability to provide (i) continuing security engineering support for any required video cross-domain interfacing with GVS to evaluate system patches and upgrades, and (ii) engineering support to investigate problems and identify solutions, comply with security procedures, specify configurations for system components, and evaluate proposed system enhancements to support systems services. Id. Under technical subfactor 3, offerors were to demonstrate their ability to analyze problems related to the videoconferencing infrastructure, determine problem

[2] The RFP was amended four times. References herein are to the conformed version of the RFP that is inclusive of the four amendments.

[3] GVS provides global unclassified and classified videoconferencing services as one of the unified capabilities for customers in Department of Defense (DOD or DoD) and other government departments and agencies and for DOD sponsored sites. RFP, PWS, at 2. Pursuant to DOD policy, the term "unified capabilities" is defined as "[t]he integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities." DOD Instruction No. 8100.04, DOD Unified Capabilities (UC) (Dec. 9, 2010), at 26.

root causes, and develop methods to resolve and eliminate the identified problems, including interim work-arounds for time-critical problems. Id. Under the management subfactor, offerors were to demonstrate a comprehensive management approach including an acceptable mix of labor categories, labor hours, and other direct costs to meet the PWS's requirements, as well as providing generic resumes for key personnel. Id. at 5.

The agency received three proposals in response to the RFP, including from the protester and intervenor. AR, Tab 10, Price Negotiation Memorandum, at 5. After receiving the three initial proposals, the agency conducted discussions with the offerors and requested final proposal revisions. Agency Report (AR) at 14. Relevant here, the agency evaluated IPKeys' and By Light's final proposals accordingly:

	By Light	IPKeys
Technical/Management		
Subfactor 1	**Green**	**Green**
Subfactor 2	**Purple**	**Green**
Subfactor 3	**Green**	**Green**
Management Subfactor	**Purple**	**Green**
Price/Cost		
Total Proposed Cost	**$59,487,541.33**	**$56,677,105.66**
Most Probable Cost/ Total Evaluated Cost	**$59,487,541.33**	**$56,677,105.66**

AR, Tab 10, Price Negotiation Memorandum, at 5.[4]

In the tradeoff analysis, the contracting officer began by recognizing that By Light's total evaluated cost ranked second, and was 5 percent higher than IPKeys' evaluated cost. Id. at 7. The contracting officer, however, then analyzed the two unique strengths awarded to By Light's proposal.[5] As discussed in greater detail below, the contracting

[4] Pursuant to the RFP, a "green" rating equated to a rating of "acceptable," meaning the "[p]roposal meets requirements and indicates an adequate approach and understanding of the requirements, and risk of unsuccessful performance is no worse than moderate." RFP, attach. No. 6, Evaluation Table. A "purple" rating equated to a rating of "good," meaning the "[p]roposal indicates a thorough approach and understanding of the requirements and contains at least one strength, and risk of unsuccessful performance is low to moderate." Id.

[5] Pursuant to the RFP, a strength was "an aspect of an offeror's proposal/quotation that has merit or exceeds specified performance or capability requirements in a way that will (continued...)

officer first considered the strength awarded to By Light under technical subfactor 2 relating to the awardee's proposed cybersecurity framework; the contracting officer found that the proposed framework would help to manage cybersecurity risks and lead to improved efficiencies. Id. at 7-8. Additionally, the contracting officer considered the strength awarded to By Light under the management subfactor relating to its comprehensive management and staffing approach. Id. at 8-9. The contracting officer concluded that the perceived technical advantages of By Light's proposal provided the best value to the government as compared to the 5 percent cost savings associated with IPKeys' proposal, and therefore selected By Light's proposal for award. Id. at 10. Following the receipt of a debriefing, the protester filed this protest with our Office.[6]

DISCUSSION

IPKeys challenges DISA's evaluation of By Light's proposal; specifically, the assessment of a strength under technical subfactor 2 for By Light's cybersecurity approach, and a strength under the management subfactor for By Light's staffing approach. The protester contends that the evaluated strengths are unreasonable and unsupported. Alternatively, IPKeys alleges that the agency engaged in disparate treatment by failing to reasonably credit the protester's proposal for including similar strengths. For the reasons that follow, we find no basis to sustain IPKeys' protest.[7]

(...continued)
be advantageous to the Government during contract performance." RFP, attach. No. 6, Evaluation Table.

[6] The awarded value of the task order is approximately $59.5 million. Accordingly, this procurement is within our jurisdiction to hear protests related to the issuance of task or delivery orders under multiple-award IDIQ contracts. 10 U.S.C. § 2304c(e)(1)(B).

[7] IPKeys raises other collateral arguments. While our decision does not specifically address every argument, we have considered all of the protester's additional assertions and find that none provides any basis on which to sustain the protest. For example, IPKeys' initial protest alleged that DISA failed to evaluate a number of strengths associated with the protester's proposal across all four technical subfactors. See Protest at 17-30. The agency provided detailed responses to these protest allegations in its initial agency report. See AR (July 28, 2017) at 33-46; AR, Tab 16, Decl. of GVS Deputy Program Manager, at 1-16. In its comments, however, IPKeys merely "incorporated [ ] by reference" its previously asserted protest grounds and, with only limited exceptions, generically questioned the agency's "post hoc assessment." IPKeys' Supp. Protest & Comments (Aug. 7, 2017), at 24. On this record, we find that the protester abandoned its originally asserted protest grounds that the agency unreasonably failed to evaluate strengths in its proposal (other than the two specific alleged instances of disparate treatment addressed herein). In this regard, where an agency provides a detailed response to a protester's assertions and the protester fails to rebut or otherwise substantively address the agency's arguments in its comments, the protester provides us with no basis to conclude that the agency's position with
(continued...)

The task order competition here was conducted among DISA GSM-ETI IDIQ contract holders pursuant to Federal Acquisition Regulation subpart 16.5. In reviewing protests of awards in a task order competition, we do not reevaluate proposals but examine the record to determine whether the evaluation and source selection decision are reasonable and consistent with the solicitation's evaluation criteria and applicable procurement laws and regulations. Diamond Info. Sys., LLC, B-410372.2, B-410372.3, Mar. 27, 2015, 2015 CPD ¶ 122 at 7; Harris IT Servs. Corp., B-406067, Jan. 27, 2012, 2012 CPD ¶ 57 at 5.

Technical Subfactor 2

IPKeys contends that the agency unreasonably awarded By Light's proposal a strength under technical subfactor 2 for its proposed cybersecurity approach since the awardee, in essence, only committed to meeting the RFP's minimum cybersecurity requirements. Alternatively, IPKeys alleges that DISA engaged in disparate treatment for failing to credit the protester for its commitment to meeting similar cybersecurity requirements. DISA responds that the awarded strength was reasonable because By Light's proposal in fact exceeded the RFP's minimum requirements, and there was no disparate treatment because IPKeys did not commit to implement the heightened cybersecurity procedures as proposed by By Light. For the reasons that follow, we find IPKeys' challenge is without merit.

Throughout its pleadings, the protester cites the following provision from the agency's evaluation documentation as constituting the strength evaluated by the agency: "[o]ur team utilizes the Risk Management Framework (RMF) and the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, also known as the Cybersecurity Framework, as the foundation for the development and execution of the Security Plan." AR, Tab 10, Price Negotiation Memo., at 7. Based exclusively on this quote, the protester contends that the awarded strength was for By Light's reference to "the RMF and the NIST Framework," which the protester contends is unreasonable because the RMF and cybersecurity framework are synonymous (or the cybersecurity framework is otherwise subsumed within the RMF) and the RMF is a basic requirement of the PWS. See, e.g., IPKeys' Supp. Protest & Comments (Aug. 7, 2017) at 9.

The record reflects that the strength the agency awarded By Light's proposal was based on more than the limited language referenced by the protester and reflected the

(...continued)
respect to the issue in question is unreasonable or improper. Bannum, Inc., B-411586.2, Jan. 6, 2016, 2016 CPD ¶ 13 at 3-4; Straughan Envtl., Inc., B-411650 et al., Sept. 18, 2015, 2015 CPD ¶ 287 at 9-10; IntegriGuard, LLC d/b/a HMS Fed.--Protest & Recon., B-407691.3, B-407691.4, Sept. 30, 2013, 2013 CPD ¶ 241 at 5; Israel Aircraft Indus., Ltd.--TAMAM Div., B-297691, Mar. 13, 2006, 2006 CPD ¶ 62 at 6-7.

agency's determination that By Light's implementation of NIST's cybersecurity framework provided independent benefits to the agency. Specifically, the strength was evaluated as follows:

> The NIST Framework for Improving Critical Infrastructure Cybersecurity enables organizations to support and improve cybersecurity practices based on their individual business needs, tolerance for risk, and available resources. It is not designed to replace existing processes and has not been mandated for use within the DoD or DISA. However, it supports using a set of industry standards and best practices to help manage cybersecurity risks that offer tangible benefits that include improved efficiencies. . . . Using this Framework as a management tool will support identifying activities that are most important to critical service delivery and allow for prioritization expenditures to maximize the impact of investment.

AR, Tab 10, Price Negotiation Memo., at 8.[8]

Turning to the question of whether the RMF and NIST cybersecurity framework are synonymous or otherwise coextensive, we conclude that the agency reasonably found the two standards to be distinct and complementary. As explained by DISA, federal agencies are required to manage information and information systems according to the Federal Information Security Management Act of 2002 (FISMA) and related standards and guidelines. Relevant here is NIST Special Publication (SP) 800-37, titled "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach." NIST SP 800-37 details the NIST RMF, which is a six-step process that provides a method of coordinating the inter-related FISMA standards and guidelines to ensure systems are provisioned, assessed, and managed with appropriate

[8] In its supplemental comments, IPKeys argues for the first time that only federal agencies, not contractors, may implement complementary portions of the NIST cybersecurity framework into their existing RMF implementations. See IPKeys' Supp. Comments (Aug. 18, 2017) at 7. The protester also alleges for the first time in its supplemental comments that By Light's proposal should have been found technically unacceptable if its incorporation of elements of the cybersecurity framework was inconsistent with the mandatory RMF requirements. See id. at 10-11. We decline to consider these arguments because they are untimely, as the initial agency report clearly indicated that the awardee had explicitly proposed to incorporate--and the agency explicitly credited the awardee for its proposed incorporation of--elements of the NIST cybersecurity framework into its proposed cybersecurity approach, and thus the basis for these protest allegations were reasonably knowable to the protester at that time. 4 C.F.R. § 21.2(a)(2) (requiring protest issues to be filed within 10 days after the basis is known or should have been known); see also GS Eng'g, Inc., B-413299.2, Jan. 10, 2017, 2017 CPD ¶ 39 at 5 n.5 (piecemeal presentation of protest grounds, raised for the first time in comments, are untimely); Wall Colmonoy Corp., B-413320, B-413322, Oct. 3, 2016, 2017 CPD ¶ 63 at 6 n. 6 (same).

security. NIST, Cybersecurity Framework FAQs: Relationship Between the Framework and Other Approaches and Initiatives, ¶ 40, available at https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-relationship-between-framework-and-other-approaches-and (last visited Sept. 28, 2017) (hereinafter, "NIST Cybersecurity Framework FAQs"). The DOD specific implementation of the NIST RMF is set forth in DOD Instruction No. 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) (July 28, 2017), ¶ 3.b, c. Both parties agree that compliance with DOD Instruction No. 8510.01 is required by the RFP. See RFP, PWS, at 2.

Another set of NIST cybersecurity guidelines is the Framework for Improving Critical Infrastructure Cybersecurity. The NIST cybersecurity framework, which is voluntary and targeted to the private sector, provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes. See NIST Cybersecurity Framework FAQs, ¶ 40. In describing the relationship between the RMF and cybersecurity framework, NIST explains that while the RMF is mandatory for federal agencies, agencies may also augment RMF-based practices with elements from the cybersecurity framework. Specifically, NIST advises that:

> The [NIST Cybersecurity] Framework is not intended to duplicate the current information security and risk management practices in place within the Federal Government. However, in the course of managing information security risk using the established NIST [RMF] and associated security standards and guidelines required by FISMA, agencies can leverage the Cybersecurity Framework to complement their current information security programs.

Id. (quoting OMB Circular No. A-130, Responsibilities for Protecting Federal Information Resources).

The cybersecurity framework itself explains that the framework "complements, and does not replace, an organization's risk management process and cybersecurity program." NIST, Framework for Improving Critical Infrastructure Cybersecurity (v. 1.0, Feb. 12, 2014), at 4; see also id. at 13 ("The Framework is designed to complement existing business and cybersecurity operations."). Rather, "[b]uilding from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations" to describe their current cybersecurity posture and target state for cybersecurity, identify and prioritize opportunities for improvement within the context of a continuous and repeatable process, assess and progress toward the target state, and communicate among internal and external stakeholders about cybersecurity risk. Id. at 4.

In this regard, the "framework core" provides a set of activities to achieve cybersecurity outcomes to manage cybersecurity risks that are broadly divided into five functions: identify; protect; detect; respond; and recover. Id. at 7. The framework core, and its functions and their constituent categories and subcategories, "is not a checklist of actions to perform." Id. Rather, the core is a methodology for achieving key

cybersecurity outcomes when implementing specific cybersecurity requirements, including, for example, compliance with applicable NIST guidelines and standards. Id.; see also id., appx. A: Framework Core, Table 2 (showing the interaction of specific cybersecurity guidelines or standards, including applicable NIST guidelines and standards, with the overall framework core). Based on the foregoing guidance from NIST--the author of both the RMF and cybersecurity framework--regarding the relationship between the two standards, we find that the agency reasonably concluded that the two NIST standards are separate and complementary.

Furthermore, we are not persuaded that the agency acted unreasonably based on IPKeys' argument that DOD's implementation of the NIST RMF is so robust as to subsume any of the perceived benefits of voluntarily incorporating the NIST cybersecurity framework. The protester fails to elaborate on or explain with any specificity how the DOD implementation of the NIST RMF is coextensive with the specific methodologies laid out in the NIST cybersecurity framework. See IPKeys' Supp. Comments (Aug. 18, 2017) at 9 ("Given how complete the DoD RMF already is, the Cybersecurity Framework may have little to add when it is ultimately incorporated under agency guidance as per Executive Order 13800.") (emphasis in original omitted). In the face of the above-described NIST guidance regarding the distinct and complementary nature of the cybersecurity framework to the underlying NIST RMF requirements, we do not find that the protester's generic assertions regarding the DOD RMF provide a reasonable basis to question the agency's evaluation in this regard.

In an alternative argument, to the extent RMF and the NIST cybersecurity framework are not synonymous or subsumed within the solicitation's existing requirements, IPKeys argues that elements of the cybersecurity framework are expected to become mandatory for all federal agencies. Specifically, the protester represents that both Executive Order 13800, Strengthening The Cybersecurity of Federal Networks and Critical Infrastructure (May 11, 2017), and Draft NISTIR 8170, The Cybersecurity Framework: Implementation Guidance for Federal Agencies (May 2017), will require federal agencies to implement complementary elements of the NIST cybersecurity framework into their applicable governing cybersecurity standards and guidelines. See, e.g., IPKeys' Supp. Comments (Aug. 18, 2017) at 7, 9-10. Based on these developments, IPKeys contends that it was unreasonable to credit By Light for a strength for its voluntary incorporation of elements of the cybersecurity framework when "[i]t is thus clear that any portion of the Cybersecurity Framework deemed complementary by agency authorities will [be] subsumed within the RMF via changes to NIST publications already incorporated therein." IPKeys' Supp. Comments (Sept. 7, 2017) at 9 (emphasis in original omitted). We find no merit to this argument.

The reasonableness of an agency's evaluation is based on the facts available at the time of the evaluation, not speculation of future developments. Here, the current, applicable mandatory cybersecurity requirements do not require incorporation of the cybersecurity framework, and By Light was reasonably assessed a strength for voluntarily agreeing to exceed the requirements. The fact that the NIST cybersecurity framework is seen as a positive addition to existing cybersecurity standards and

guidelines and may ultimately be mandated in whole or in part does not undermine the reasonableness of the evaluated strength for By Light's commitment to voluntarily implementing the framework prior to the framework becoming mandatory. Therefore, we find no basis to sustain IPKeys' protest with regard to the agency's evaluation of proposals under technical subfactor 2.[9]

Finally, we find no merit to IPKeys' allegation that the agency engaged in any disparate treatment with respect to the evaluation of the offerors' proposed cybersecurity approaches. Where a protester alleges unequal treatment in a technical evaluation, it must show that the differences in ratings did not stem from differences in the proposals. ASRC Comms., Ltd., B-414319.2 et al., May 9, 2017, 2017 CPD ¶ 167 at 7; Northrop Grumman Sys. Corp., B-406411, B-406411.2, May 25, 2012, 2012 CPD ¶ 164 at 8. Here, IPKeys has not established that the different ratings were not based on differences between the offerors' proposals. As set forth above, only By Light proposed to incorporate the voluntary NIST cybersecurity framework on top of its compliance with the baseline cybersecurity requirements, which was the basis of the unique strength awarded to its proposal.

Management Subfactor

IPKeys argues that DISA unreasonably assessed a strength based on anticipated cost savings of $1.6 million associated with By Light's proposal to utilize [DELETED] in performance of the order's [DELETED] requirements.[10] The protester contends that the agency irrationally concluded that the use of the proposed [DELETED] for the [DELETED] requirements would obviate the need to exercise any of the optional [DELETED] tasks, and challenges the methodology used to calculate the anticipated cost savings. IPKeys further contends that DISA engaged in disparate treatment by failing to consider the potential for cost savings associated with certain features of the protester's proposal. The agency, in addition to defending the methodology for its calculation of the potential costs savings, argues that the protester unreasonably focuses on only one limited aspect of the overall strength assessed for By Light's

[9] NIST's express recognition of its intent to amend its underlying cybersecurity standards and guidelines, including the RMF specifically, to incorporate elements of the cybersecurity framework further bolsters our conclusion that the agency reasonably gave By Light credit for its voluntary commitment to utilize the framework as a complement to its compliance with the mandatory DOD RMF requirements. See Draft NISTIR 8170, The Cybersecurity Framework: Implementation Guidance for Federal Agencies (May 2017) at v-vi.

[10] IPKeys initially also challenged DISA's basis for finding that By Light had proposed [DELETED] for the pertinent PWS tasks. See IPKeys' Supp. Protest & Comments (Aug. 7, 2017) at 20-22. In response to DISA's detailed response, the protester did not provide any substantive response and effectively conceded the basis for the agency's finding in this regard. See, e.g., Straughan Envtl., Inc., supra.

proposed management and staffing approach. In this regard, DISA contends that the potential for cost savings was only an additional consideration beyond the strength awarded for the awardee's proposed labor mix, was not material to the source selection, and therefore any error in the consideration of or methodology for deriving the potential cost savings was non-prejudicial. As addressed below, we find no basis to sustain IPKeys' protest on this basis.

As an initial matter, we agree with the agency that the protester does not reasonably consider the evaluation of By Light's management and staffing approach in its totality. Rather, IPKeys fixates exclusively on the portion of the awarded strength pertaining to the potential cost savings associated with By Light's proposed use of [DELETED] in performance of the [DELETED] requirements. See IPKeys' Supp. Protest & Comments (Aug. 7, 2017) at 22-23; IPKeys' Supp. Comments (Aug. 18, 2017) at 14-16. The protester, however, does not challenge the other bases identified for awarding By Light a strength for its proposed use of [DELETED] or the other bases identified for supporting By Light's overall good or "purple" rating.

Specifically, DISA awarded By Light's proposed utilization of [DELETED] a strength because:

> By including [DELETED] with an appropriate mix of [DELETED], rather than [DELETED], this proposal exceeds the level of knowledge and experience required to adequately complete the requirements included in the PWS, and further indicates a strong chance of successful integration with other DISA and DoD Unified Capabilities programs. This represents a strength and significant advantage to the government by exceeding the current and future requirements for a standalone GVS, and also providing significant opportunity to engineer a technical way forward within the Unified Capabilities Portfolio for both integration efforts and follow-on efforts. This significantly increases the agility and responsiveness of not only the specific task order, but also the agency's Unified Capabilities Portfolio [DELETED] with the ability to complete complex and comprehensive efforts [DELETED].

AR, Tab 10, Price Negotiation Memo., at 8-9.

After this detailed justification for the basis of the awarded strength--which is not meaningfully challenged by IPKeys--the agency's selection decision memorandum highlights examples of potential cost saving efficiencies arising from By Light's proposed utilization of [DELETED]. Specifically, the agency indicates that the strength may lead to initiatives to better integrate the GVS into DOD's unified capabilities portfolio, potentially saving the government engineering, equipment, and labor costs. As an additional potential area of cost savings, the agency notes that the strength had the potential to obviate the need to exercise the optional task for [DELETED]. Id. Aside from these potential areas of cost savings, DISA also discussed other aspects of By Light's management and staffing approach. The agency found that it "show[ed] a

greater understating and granularity of detail in the programmatic, engineering, developmental and operational support that exceeds the requirements for this task order," including, for example, the awardee's proposed utilization of project management, configuration management, logistics support, and communications personnel. Id. at 9.

As noted above, IPKeys challenges the agency's evaluation of By Light's staffing approach only with respect to one of the bases for potential cost savings--the potential to avoid exercise of the solicitation's optional task for [DELETED]. Even assuming for the sake of argument that the agency's conclusion in this regard was unreasonable, we cannot discern any harm arising from the alleged error. Given the numerous uncontested bases for the strength that were independent of the challenged cost savings rationale, removal of this one basis for the strength would not reasonably lead to elimination of the strength or in a downgrade of By Light's purple rating under the management subfactor. In this regard, competitive prejudice is an essential element of every viable protest, and where none is shown or otherwise evident, we will not sustain a protest, even where a protester may have shown that an agency's actions arguably were improper. REG Prods., LLC, B-414638, July 3, 2017, 2017 CPD ¶ 213 at 3.

In addition, and perhaps most importantly, the record reflects that the source selection tradeoff did not turn on the cost savings aspect of the strength. The record reflects that the selection decision was made using the evaluated most probable costs, which did not consider any of the potential cost savings challenged by the protester. AR, Tab 10, Price Negotiation Memorandum, at 5, 7, 9, 10. Specifically, the contracting officer, independent of the challenged potential cost savings, found that "[t]he 5% difference in price between By Light's evaluated [cost] and [IPKeys'] total evaluated [cost] is minimal, and By Light's strengths are well worth the additional benefit to the Government for paying a slightly higher price for their proposal." Id. at 9. The contracting officer determined that the efficiencies associated with the evaluated strengths would "provide enhanced services and security to the warfighter [that were] adjudged as highly valuable to the Government." Id. The detailed record of the contracting officer's rationale makes plain that the potential cost savings was simply an additional consideration, which was not necessary to support the award determination. Thus, as the propriety of this additional consideration would not undermine the primary basis for the agency's evaluation and tradeoff, we have no basis to sustain this aspect of the protest.[11] See ASRC Comms., Ltd., supra, at 6-7 (denying a protest challenging the

[11] In light of our determination that the strength awarded to By Light was not dependent on the potential cost savings, we find no basis to conclude that the agency engaged in any disparate treatment in the evaluation of IPKeys' and By Light's proposals under the management subfactor. In any event, based on our review of the record, DISA did not engage in disparate treatment by failing to credit the protester for potential cost savings. Rather, the different evaluation determinations were the result of substantive differences in the offerors' proposed management and staffing approaches. Northrop Grumman Sys. Corp., supra.

reasonableness of the award of a strength for potential cost savings where the strength was actually based on the awardee's proposed innovative approach, as opposed to the potential cost savings specifically); Wilcox Elec., Inc., B-270097, Jan. 11, 1996, 96-1 CPD ¶ 82 at 6-7 (similarly denying challenge to presumed cost savings where they were only an additional consideration).

The protest is denied.

Susan A. Poling
General Counsel