U.S. GOVERNMENT ACCOUNTABILITY OFFICE

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

Comptroller General
of the United States

Decision

Matter of: Dentrust Dental International, Inc. d/b/a DOCS Health

File: B-423938; B-423938.2

Date: February 6, 2026

Eric W. Leonard, Esq., Matthew Howell, Esq., and Rachel Schwartz, Esq., Cozen O'Connor, for the protester.
Adam K. Lasky, Esq., Ken M Kanzawa, Esq., and Zohra Tejani, Esq., Seyfarth Shaw LLP, for Acuity International, LLC, the intervenor.
Michael H. Noyes, Esq., and Jessica Chen, Esq., Department of Homeland Security, for the agency.
Paula A. Williams, Esq., and Evan D. Wesser, 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, adequately documented, and in accordance with the terms of the solicitation; to the extent any errors were made, such errors were not competitively prejudicial to the protester.

2. Protest that the agency engaged in disparate treatment in evaluating proposals is denied where the record shows that the agency's evaluation was reasonable and the differences in ratings were based on differences in the proposals.

DECISION

Dentrust Dental International, Inc. (Dentrust) d/b/a DOCS Health, of Pipersville, Pennsylvania, protests the award of a contract to Acuity International, LLC (Acuity), of Reston, Virginia, under request for proposals (RFP) No. 70US0925R70092450, issued by the Department of Homeland Security (DHS), United States Secret Service (Secret Service) for medical examination services. The protester primarily argues that the agency unreasonably evaluated the protester's and the awardee's proposals.

We deny the protest.

BACKGROUND

The RFP was issued on June 23, 2025, and contemplated the award of a fixed-price contract with a 1-year base period and three 1-year option periods. Agency Report (AR), Exh. 2, RFP at 156.[1] Secret Service law enforcement personnel are required to meet certain medical and fitness standards and the RFP sought proposals for a contractor to provide medical examination services for all employees and pre-employment applicants in the agency's mandatory medical examination program. *See generally*, RFP Performance Work Statement (PWS) at 157-191. These medical examination services will be provided at designated locations nationwide including in Puerto Rico, Alaska, and Hawaii. *Id.* at 157, 162. The PWS identified specific services the selected contractor must provide, including performing complete physical examinations for all employees and pre-employment applicants to determine their ability to perform strenuous physical exertion and to identify any physical defects or abnormalities that would restrict or prohibit the employee's participation in required physical fitness testing, defensive tactics, training, or dangerous assignments that may require the use of firearms or physical force. *Id.* at 162-163.

As is relevant, the contractor is required to upload all medical information for the agency's employees and pre-employment applicants to a government-provided staff/employee-patient portal (if available). *Id.* at 162. However, the solicitation informed offerors that the government-provided staff/employee portal was not yet available, *see* RFP at 116, 117, but the agency will acquire an electronic medical record (EMR) system under a separate contract and the awardee under this medical examination services contract will be required to work with the EMR contractor to transfer all medical examination documents into the new EMR system. RFP at 182.

Additionally, the RFP provided cybersecurity guidance to offerors whose proposed approach might include the use of an automated medical data management tracking system to upload medical information. RFP at 136-137. Specifically, the solicitation provided that the storage and transfer of agency employees' and pre-employment applicants' medical records using a cloud-based environment must meet the Federal Risk and Authorization Management Program (FedRAMP)[2] authorization requirements. *Id.* at 137. With regard to the requirement for FedRAMP compliance, the solicitation provided as follows:

> If the Contractor uses cloud technologies to provide services to the Government under this solicitation, the Contactor and proposed

[1] References to page numbers for agency report exhibits are to the Bates numbering provided by the agency. References to page numbers for exhibits submitted by the protester and intervenor are to the electronic pagination.

[2] FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. *See* https://cloud.cio.gov/ (last visited Jan. 31, 2026).

> [automated] system must already be designated as FedRAMP Authorized (Moderate) upon contract award. The Contractor shall continue to comply with the FedRAMP authorization process for cloud-based systems throughout the contract period of performance. The Contractor is responsible for all costs associated with achieving and maintaining their FedRAMP authorization.

Id.[3]

The RFP included questions and answers (Q&A) that reiterated the above FedRAMP compliance requirements in which the agency stated: "FedRAMP certification is mandatory for all executive agency cloud deployments and service models at the Low, Moderate, and High risk impact levels." RFP Q&A at 118. Pertinent here, in response to another question:

> Q: It is our assumption that a proposed solution in a private cloud environment, which would meet the [authority to operate (ATO)] standards and achieve the same compliance level, does not require FedRAMP certification. Is this assumption correct? If [not] please clarify.

The agency responded:

> A: Correct, a non-cloud solution will not require FedRAMP certification; however, the [c]ontractor's solution must comply and adhere to the information technology security requirements and management principles as outlined in the [PWS].

Id.

With regard to an offeror's proposed automated non-cloud based solution, the RFP provided in relevant part: "[i]f the [contractor] plans to utilize a non-cloud-based system it is required that upon contract award, the proposed system must be operating under a current ATO at DHS or one of its subordinate components in order to leverage the DHS allowance for ATO reciprocity." *Id.* at 137.

The RFP provided for a two-phase, best-value tradeoff source selection process, considering the following evaluation factors, which are listed in descending order of importance: (1) oral presentations; (2) technical capability; (3) management approach; (4) experience/qualification; (5) past performance; and (6) price. *Id.* at 153. The RFP advised that the technical capability, management approach, experience/qualification

---

[3] The RFP provided that government information security guidelines do not distinguish between government-owned or contractor-owned hosting systems. All contractor-owned hosting systems that contain government data must achieve and maintain the same level of cybersecurity and protection required for government-owned hosting systems. RFP at 137.

and past performance factors (factors 2-5), when combined were more important than the oral presentations factor (factor 1); and the five nonprice evaluation factors, when combined, were significantly more important than price. *Id.*

In phase one, the agency would evaluate only oral presentations (factor 1). *Id.* at 153. During the oral presentation, the offeror would provide answers to questions set forth in the solicitation and any on-the-spot questions posed by the agency during the presentation. *Id.* at 153-154. The solicitation stated that, after each oral presentation concluded, the evaluation team would do a consensus evaluation of the presentation to determine a confidence rating of high, some, or low confidence and would document the evaluation decision in real time. *Id.* at 155-156. As specifically relevant here, the solicitation defined a rating of high confidence as "[t]he Government has high confidence that the Offeror understands the requirement, proposes a sound approach, and will be successful in performing the contract with little or no Government intervention." *Id.* at 155. The solicitation defined a rating of some confidence as "[t]he Government has some confidence that the Offeror understands the requirement, proposes a sound approach, and will be successful in performing the contract with some Government intervention." *Id.*

After the phase one evaluation, the agency would issue an advisory notice to each offeror identifying whether the agency viewed the offeror as a viable competitor; all offerors would have the option to submit a phase two proposal.[4] *Id.* at 154; COS at 604.

In phase two, offerors would submit written proposals addressing evaluation factors 2-6. As with the phase one evaluation, phase two proposals would be evaluated under the technical capability, management approach, and experience/qualification factors (factors 2-4), by assigning a confidence rating of high, some, or low confidence, reflecting the agency's level of confidence that the offeror understands the requirements and will be successful in performing the contract. *Id.* at 155. Past performance (factor 5) also would be assigned a confidence rating of high, some, or low confidence, reflecting the agency's confidence that the offeror can successfully perform the requirements of the contract. A past performance rating of neutral would be assigned for lack of relevant past performance. *Id.* at 154-155. Price (factor 6) would be evaluated to determine whether the proposed prices were fair and reasonable. *Id.* at 155.

[4] The agency's two-phase evaluation utilized an "advisory down-select" process. RFP at 154. The agency would issue each phase one offeror an advisory notice and those offerors whose presentations were rated low confidence would be advised of the likelihood of receiving the award. Contracting Officer's Statement (COS) at 604. The notice was a recommendation only and offerors were permitted to choose whether to participate in phase two of the competition regardless of the nature of the agency's advisory notice. *Id.*

During the week of July 14, six offerors, including Dentrust and Acuity, participated in oral presentations and oral questions and answers exchanges (factor 1). COS at 603; AR, Exh. 7, Decl. of Technical Evaluation Team (TET) Evaluator A at 609; *see also* RFP at 113. Dentrust's oral presentation was held on July 17. Among other things, Dentrust described its proposed automated medical data management tracking system, called the [DELETED]. The [DELETED] system is a cloud-based data storage system that will be used to schedule medical appointments, administer medical questionnaires, and to receive, store, review, and transmit employee examination documents and laboratory results.[5] AR, Exh. 7, Decl. of TET Evaluator A at 609. During the oral question and answer exchange, Dentrust was asked if its [DELETED] system was FedRAMP authorized, and the offeror responded that the [DELETED] system was hosted "on the [DELETED] FedRAMP Platform."[6] *Id.* The evaluator reports that he "verbally advised Dentrust that both the platform [DELETED] and the solution [DELETED] had to be *separately* FedRAMP Authorized to store [the agency's] data." *Id.* (emphasis in original).

Three offerors' oral presentations, Dentrust, Acuity and a third offeror, were among the most highly rated and were invited to participate in phase two of the procurement.[7] *See* Protest, exh., 7, Advisory Downselect Notice at 1 (July 18, 2025); *see also*, AR, Exh. 3, Source Selection Decision (SSD) at 245. The agency received phase two proposals from all three offerors by the August 8 submission deadline.[8] MOL at 3; AR Exh. 3, SSD at 245.

---

[5] The agency reports that this type of employee data is deemed sensitive personally identifiable information (SPII) and is subject to specific handling restrictions on cloud-based automated systems. Memorandum of Law (MOL) at 3 *citing* AR, Exh. 7, Decl. of TET Evaluator A at 609. In other words, the storage and transfer of SPII data in a cloud environment must gain FedRAMP authorization. *Id.*

[6] The protester contends that the evaluator's declaration responding to the protest is a *post hoc* statement "that attempts to rewrite the [a]gency's evaluation and understanding of [its] proposal to cover the obvious gaps and inconsistencies in the [a]gency's evaluation[.]" Comments & Supp. Protest at 3. We note that an agency is not required to document every single aspect of its evaluation or explain why a proposal did not receive a higher confidence rating for a particular aspect of a protester's proposal. *Sterling Med. Assocs., Inc.*, B-418674, B-418674.2, July 23, 2020, 2020 CPD ¶ 255 at 8; *ICON Gov't and Public Health Solutions, Inc.*, B-419751, July 2, 2021, 2021 CPD ¶ 238 at 8. As discussed herein, we find the evaluator's post-protest explanations to be credible and consistent with the contemporaneous evaluation record.

[7] The agency reports that the offerors rated low confidence elected not to proceed to phase two of the competition. MOL at 3.

[8] The phase two proposal submitted by the third offeror is not relevant to this protest and is not further discussed.

In its phase two proposal, Dentrust proposed its [DELETED] system that is hosted on [DELETED] FedRAMP authorized [DELETED] platform. The offeror's proposal also described numerous additional applicable utilized security measures. Protest, exh. 4, Dentrust Proposal at 13. In its phase two proposal, Acuity proposed its automated medical data management tracking system, called [DELETED], that is a non-cloud, web based electronic records/reports system. AR, Exh. 5, Acuity Clarification Req. & Resp. 3 at 595.

After an initial evaluation, the agency decided to email request for clarifications to both offerors to confirm the cybersecurity details of their respective proposed automated medical data management tracking systems. Protest, exh. 5, Dentrust Clarification Requests; AR, Exh. 5, Acuity Clarification Requests.

On August 21, the agency issued request for clarifications to Dentrust. Among other things, Dentrust was asked if its automated medical data management tracking system (known as an electronic medical record) was currently designated as FedRAMP Ready, FedRAMP In-Process, or FedRAMP Authorized. Protest, exh. 5, Dentrust Clarification Req. 1 at 2. Dentrust responded, in relevant part, that its [DELETED] "is a [Health Insurance Portability and Accountability Act (HIPAA)]-compliant solution that is hosted in [DELETED] which is FEDRAMP-Authorized as FEDRAMP High" and its [DELETED] system is "NIST [National Institute of Standards and Technology]-Compliant FEDRAMP Hosted Cloud Solution." *Id.*, Clarification Resp. 1 at 2. The agency also asked Dentrust to indicate where its medical examination data resides, for example, in a cloud environment or in an on-premises corporate data center. Protest, exh. 5, Clarification Req. 4 at 3. In response, Dentrust stated, in pertinent part: "[a]ll medical information resides on [DELETED] servers that are FEDRAMP Authorized." *Id.*, Clarification Resp. 4 at 4. Additionally, in response to whether a DHS agency has issued an authority to operate (ATO) or risk acceptance memorandum (RAM) for its automated management/tracking system, Dentrust confirmed that it did receive a RAM from the Federal Emergency Management Agency (FEMA) and that its system is also currently being used by Immigration and Customs Enforcement (ICE) and the Federal Protective Service (FPS). *Id.* at 3.

The agency similarly sent requests for clarification to Acuity. The offeror was similarly asked if its automated medical data management tracking system (known as an electronic medical record) was currently designated as FedRAMP Ready, FedRAMP In-Process, or FedRAMP Authorized. AR, Exh. 5, Acuity Clarification Req. 1 at 595. In its response, Acuity stated: "[the] proposed [DELETED] system is a non-cloud web-based system [and] it is not FedRAMP Ready, FedRAMP In-Process, or FedRAMP Authorized[,]" and that its proposed [DELETED] system "has completed and passed an independent [DELETED] audit." *Id.*, Clarification Resp. 4 at 595. Acuity also was asked to indicate where its medical examination data resides, for example, in a cloud environment or in an on-premises corporate data center; Acuity responded that its medical examination data resides in its on-premises corporate data center located in [DELETED]. *Id.* at 595. Additionally, Acuity confirmed that its system has previously

received an ATO from the Transportation Security Administration (TSA), and a RAM from Customs and Border Protection (CBP). *Id*.

After evaluating proposals and the offeror's responses to the clarification requests, the agency assigned the following overall consensus ratings:

	Dentrust	Acuity
Factor 1 - Oral Presentation	High Confidence	High Confidence
Factor 2 – Technical Capability	Some Confidence	High Confidence
Factor 3 – Management Approach	Some Confidence	High Confidence
Factor 4 – Organizational Experience	Some Confidence	High Confidence
Factor 5 - Past Performance	Some Confidence	High Confidence
Factor 6 - Price	$11,971,456.04	$11,025,057.68

AR, Exh. 3, SSD at 245, 249.

The contracting officer, who was also the source selection authority (SSA), reviewed the consensus evaluation reports and concurred with their findings. *Id.* at 251. The SSA conducted a comparative tradeoff analysis and selected Acuity's proposal for award because it received the highest confidence rating under each non-price evaluation factor and was lower-priced than Dentrust's proposal. *Id*. at 251-252.

The agency awarded the contract to Acuity on September 12. COS at 606. Thereafter, on September 15, the agency notified Dentrust that its proposal was not selected for award and provided a written debriefing. *Id.*; MOL at 2. On September 22, Dentrust filed this protest with our Office.

DISCUSSION

Dentrust challenges various aspects of the agency's evaluation of its proposal under the technical capability and management approach factors. The protester alleges that the agency applied unstated evaluation criteria in its technical capability evaluation, disparately evaluated Dentrust and Acuity's technical capability in some instances, and that these errors rendered the selection decision flawed. Protest at 8-9; Comments & Supp. Protest at 1-3. We have considered all of the protester's arguments including several collateral arguments and, while we do not address them all, we find that none provide any basis on which to sustain the protest.[9]

[9] For example, we do not discuss in detail Dentrust's contention--and the agency's and intervenor's rebuttals thereto--that its proposal should have been evaluated as high confidence under the management approach factor. *See, e.g.*, Protest at 9-10; Comments & Supp. Protest at 3-4; COS at 605; MOL at 12-15; Intervenor's Comments at 8-9. Our review of the record indicates that, similar to Dentrust's challenges to the evaluation of its proposal under the technical capability factor, discussed herein,

(continued...)

Technical Capability

Dentrust protests the evaluation of its proposal under the technical capability factor, asserting that it should have received the best possible rating of high confidence. Protest at 8-9. Citing an initial evaluative finding under the oral presentation factor (factor 1) that FedRAMP certification was not a requirement since its [DELETED] is hosted on a FedRAMP certified platform, the protester contests the agency's subsequent critique under the phase two technical capability factor that its [DELETED] system as a cloud-based system required FedRAMP authorization. Protest at 9; Comments & Supp. Protest at 2-3.

When reviewing an agency's evaluation of proposals and source selection decision, it is not our role to reevaluate submissions; rather, we examine the supporting record to determine whether the evaluation and selection decision were reasonable, consistent with the solicitation, and adequately documented. *US&S-Pegasus JV, LLC*, B-421681.8, B-421681.9, Nov. 19, 2024, 2024 CPD ¶ 284 at 4; *Horizon Strategies, LLC*, B-419419.5, B-419419.6, Mar. 15, 2023, 2023 CPD ¶ 71 at 10. A protester's disagreement with the agency's judgments, or with the agency's determination as to relative merits of the competing proposals, does not establish that the evaluation or selection decision were unreasonable. *Id*. We have reviewed the protester's challenges to the agency's evaluation under this factor and conclude that the agency's evaluation was reasonable and consistent with the terms of the solicitation.

Under the technical capability factor, offerors were required to provide a comprehensive and complete technical proposal demonstrating the likelihood of the offeror's successful performance of all contract requirements and conforming to all required terms and conditions. *See* RFP at 156. As noted, the successful contractor is required to upload SPII medical data to the contractor-owned automated medical data management tracking and data storage system. *See id.* at 137. The RFP clearly stated that FedRAMP authorization was required for both the contractor and the proposed system if the contractor proposed a cloud-based automated system. *Id.*

The agency evaluated Dentrust's phase two proposal as warranting a rating of some confidence under the technical capability factor. *See* AR, Exh. 3, TET Consensus Eval. Report at 230. In its evaluation under this factor, the evaluators identified significant concerns with Dentrust's [DELETED] system. First, the evaluators noted that Dentrust's "system is not FedRAMP approved and [the offeror] did not provide evidence to indicate they currently exercise appropriate security controls to safeguard patient SPII data." *Id.*

Dentrust's challenges under the management approach factor at most reflects only the protester's disagreement with the agency's reasonable evaluation judgments. A protester's disagreement with the agency's evaluation and assessment, without more, does not establish that the evaluation was unreasonable. *Arctic Slope Mission Servs. LLC*, B-417244, Apr. 8, 2019, 2019 CPD ¶ 140 at 8; *Serco Inc.*, B-407797.3, B-407797.4, Nov. 8, 2013, 2013 CPD ¶ 264 at 8.

Next, the evaluators reviewed Dentrust's explanation that its [DELETED] system is used at FEMA, ICE, and FPS and complies with various NIST standards, but nevertheless concluded that the assessment of a weakness was warranted because "the [DELETED] system used to process the medical information is not FedRAMP approved, thereby indicating that minimal safeguards are in place for storing SPII in a cloud environment." *Id.* Finally, the evaluators noted that because the protester's [DELETED], a cloud-based data storage system, is not FedRAMP authorized, this "creates a major concern that the [agency] will not be able to readily use the [DELETED] system, which is critical to efficient management of exams and medical documentation." *Id*.; *see also* AR, Exh. 3, SSD at 248.

Dentrust disagrees with the agency's assessments, arguing that the evaluators' findings under the technical capability factor are "diametrically opposed" to the agency's statements under the oral presentation factor that is, FedRAMP certification is not a requirement for its [DELETED] system hosted on a FedRAMP approved platform result. Comments & Supp. Protest at 2. The protester also contends that the agency's conclusions ignore the fact that in response to the agency's clarification requests, Dentrust confirmed that its [DELETED] system is nested on a FedRAMP authorized platform, and that all medical data will reside in a FedRAMP environment. *Id.* at 2-3. Dentrust argues that, to the extent the agency applied the requirement that its [DELETED] system had to be separately FedRAMP compliant in the evaluation of its technical capability, the agency improperly applied unstated evaluation criteria. *Id.* at 3.

The agency defends its evaluation of Dentrust's phase two proposal under the technical evaluation factor as reasonable and consistent with the terms of the solicitation. In doing so, the agency refers to and quotes the evaluators' documented concerns that Dentrust's [DELETED] system was not FedRAMP authorized, as required by the plain language of the RFP and that served as the basis for the rating of some confidence. *See* COS at 605; MOL at 8-12; *see also* Intervenor's Comments at 5-8.

Moreover, the agency refutes the protester's claims that the agency applied unstated FedRAMP criteria and inconsistently applied those criteria in evaluating Dentrust's [DELETED] system positively during the oral presentation but negatively during the technical capability evaluation. *See* MOL at 10. The agency points out, and the record confirms, that any cloud-based solution needed FedRAMP authorization regardless of its hosting platform's FedRAMP status. Stated differently, the FedRAMP authorization requirement was clearly stated in the solicitation, in the Q&As included in the solicitation, and during Dentrust's oral presentation when an evaluator made clear that the [DELETED] system needed to be separately FedRAMP authorized. *See* MOL at 8. The record confirms, and the protester does not dispute, that its [DELETED], a cloud-based data storage system, was not FedRAMP authorized. Therefore, the agency's evaluation of Dentrust's [DELETED] under the technical capability factor was reasonable and consistent with the stated terms of the solicitation.

Based on this record, we do not find--as Dentrust argues--that the Secret Service applied unstated evaluation criteria when, consistent with the plain language of the solicitation, the agency reasonably considered the protester's non-compliance with the FedRAMP requirements as part of its confidence assessment of Dentrust's proposal under the technical capability evaluation factor. In this regard, the RFP required that "[i]f the Contractor uses cloud technologies to provide services to the Government under this solicitation, the Contractor and proposed system must already be designated as FedRAMP Authorized (Moderate) upon contract award." RFP at 137. Importantly, the solicitation requires the proposed system--not just any hosting environment on which the system rests--to be FedRAMP authorized. The agency subsequently clarified in its Q&A that "FedRAMP certification is mandatory for all executive agency cloud deployments and service models. . . ." RFP Q&A at 118. Here again, the agency emphasized that all service models--including proposed systems, not just hosting environments--had to be FedRAMP authorized. And, finally, the agency affirmed its interpretation during the oral presentation that both the system itself as well as the hosting environment would require authorization. *See* AR, Exh. 7, Decl. of TET Evaluator A at 609. Consequently, the agency's consideration of the [DELETED] noncompliance as part of its assessment of Dentrust's technical capability is neither unreasonable nor is it the application of an unstated evaluation criterion. This basis of protest is denied.

We also reject the protester's claims that any alleged inconsistency between the presentation and the technical capability factor evaluations undermines the reasonableness of the agency's ultimate evaluation conclusions. *See* Comments & Supp. Protest at 2-3. As an initial matter, we do not agree that the evaluation findings made in phase one were binding on the agency and could not be revised upon the receipt of additional clarifying information in phase two. Specifically, in phase one, the agency in connection with Dentrust's experience with recent and relevant contracts, noted that:

- The vendor's electronic medical record and scheduling system, patient portal, and records management system may satisfy some of the [agency's] needs and meet [agency]. They demonstrated to have a platform that is FedRAMP (Moderate) certified and that they operate under an ATO with FEMA and ICE. . . .

- The [vendor] demonstrated their online data management tool [DELETED] which they are hosting on a FedRAMP approved platform. . . .

AR, Exh. 3, Consensus Tech. Eval. Worksheets at 221; *see also* Exh. 3, SSD at 245 (noting in connection with the second finding that "[w]hile FedRAMP certification was not a requirement, this represents a significant strength for the Government by ensuring robust security measures, such as encryption, continuous monitoring, and incident response protocols, which help mitigate the risk of cyber-attacks").

The agency explains that its phase one evaluation was limited in scope only to the oral presentations, and that its phase two evaluation was a more thorough review and consideration of the offerors' technical capabilities as reflected in the offerors' technical proposals. In this regard, the agency contends that the oral presentations did not provide adequate information regarding the actual certification status of the protester's [DELETED] system and that it was only "[a]fter the evaluators received Dentrust's Phase [two] proposal and its answers to the August 21, 2025, clarification email [that] it became clear that [DELETED] was not, and would not become, FedRAMP Authorized before the award." MOL at 10. This argument is credible in light of the agency's consistent interpretation of the FedRAMP authorization requirements reflected in the RFP, the Q&A responses, and as communicated to the protester during the oral presentation, as well as the supplemental requests for clarification provided to the offerors during phase two. On this record, we think the agency has reasonably explained the apparent disconnect between the phase one and phase two evaluations.

Furthermore, we agree with the agency's and intervenor's alternative arguments that the protester cannot establish any competitive prejudice as a result of the inconsistency. 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. *Interfor US, Inc.*, B-410622, Dec. 30, 2014, 2015 CPD ¶ 19 at 7. First, in light of the agency's consistent interpretation of the FedRAMP authorization requirements, including as expressed to the protester during the oral presentation, to the extent that the agency erred in assigning a strength to the protester's phase one proposal, such error inured to the protester's benefit as it resulted in a higher assessment than otherwise was warranted. Second, the agency did not convey the assessed strength to the protester when it received its advisory notice following phase one, but, rather, only first learned of the phase one strength post-award. *Compare* Protest, exh. 7, Phase 1 Advisory Notice *with* exh. 6, Notice to Unsuccessful Offeror at 5-7. Finally, Dentrust advances no argument that had it learned of the inconsistency sooner it could or would have substituted its proposed [DELETED] for a different system that otherwise satisfied the RFP's requirements. Therefore, even assuming the agency's phase one evaluation was in error, we can discern no basis to find that the protester was competitively prejudiced by such error, and as such, the allegation does not provide a basis for us to sustain the protest.

Acuity's Technical Proposal

In its supplemental protest, Dentrust challenges the agency's evaluation of Acuity's proposal as warranting a rating of high confidence under the technical capability factor. The protester alleges that the agency improperly determined that a web based system with no FedRAMP authorization or connection to a FedRAMP authorized platform such as Acuity's [DELETED] system, merited an assessment of high confidence than Dentrust's cloud-based [DELETED] system which is "nested on a FedRAMP authorized system." Comments & Supp. Protest at 5; *see also* Supp. Comments at 2-4. Dentrust contends that this represents disparate treatment because the agency's rating of high

confidence does not represent a reasonable or fair evaluative comparison of both offerors' technical approaches. *Id.* The agency asserts that it properly considered both offerors' proposed data storage systems consistent with the terms of the solicitation. Supp. AR at 5-7.

It is a fundamental principle of federal procurement law that a contracting agency must even-handedly evaluate proposals against common requirements and evaluation criteria. *Battelle Memorial Inst.*, B-418047.5, B-418047.6, Nov. 18, 2020, 2020 CPD ¶ 369 at 6; *UltiSat, Inc.*, B-416809 *et al.*, Dec. 18, 2018, 2019 CPD ¶ 6 at 9. To prevail on an allegation of disparate treatment, a protester must show that the agency unreasonably evaluated its proposal in a different manner than another proposal that was substantively indistinguishable or nearly identical. *Sys. Implementers, Inc. et al.*, B-418963.5 *et al.*, June 1, 2022, 2022 CPD ¶ 138 at 17. In this case, the protester's disparate treatment argument fails because the different evaluation findings were based on material differences between the competing proposals.

Here, as noted, the RFP permitted offerors to propose either cloud-based or non-cloud based systems and outlined different requirements for supporting security-related information for each type of system. *See* RFP at 137. The RFP stated that cloud-based systems, such as Dentrust's [DELETED] system, were required to meet FedRAMP authorization requirements; non-cloud based systems, such as Acuity's [DELETED], were not required to obtain FedRAMP authorization. *Id.* Instead, the RFP required that non-cloud based systems must be operating under a current ATO at DHS or one of its subordinate components in order to leverage the DHS allowance for ATO reciprocity. *Id.*

The record shows that the agency evaluated Acuity's proposed system and determined that it was an on-premises solution and that "data is housed in a data center," not in the cloud. *See* AR, Exh. 8, TET Consensus Eval. Report at 616; *see also id.*, SSD at 621. The evaluators also noted that Acuity's system was not required to be FedRAMP certified, and that the system had the proper security documentation required for non-cloud based systems, including an active ATO with TSA and a RAM with CBP. *Id.* Based on these findings, the evaluators concluded that Acuity has the capability to meet all technical requirements to support the agency's outreaches and the health unit located at the agency's headquarters. *Id.*

Dentrust disagrees with the agency's evaluative conclusions, alleging that the agency was required to, but did not, evaluate any potential security concerns with Acuity's web-based system nor how these concerns may impact Acuity's technical capabilities. Comment & Supp. Protest at 5. According to the protester, the agency's review of the technical security of Acuity's proposed system was conclusory and failed to consider "how Acuity plans to maintain a secure environment for patient data, or the way in which Acuity's non-cloud based system will inevitably interact with non-FedRAMP certified cloud-based data storage[.]" Protester's Supp. Comments at 3.

The agency responds that contrary to Dentrust's assertions otherwise, the security merits of Acuity's web-based solution are well supported by credible documents from other federal agencies that were provided by Acuity. For example, the agency reports that Acuity provided detailed information concerning its ongoing approvals from TSA and CBP. Agency Addn. Statement at 3 *citing* AR, Exh. 5, Acuity Clarification Req. and Resp. 5 at 595; Intervenor's Supp. Comments at 2-6. While Dentrust complains that the agency should have conducted a more in-depth evaluation of Acuity's [DELETED] system, the protester points to no such requirement in the RFP for a more in-depth evaluation of a non-cloud based system.

We similarly find no basis to conclude that the agency's evaluation was disparate. Here, because Dentrust proposed a cloud-based solution, the RFP made clear that the protester's system would be assessed based on whether the proposed system was FedRAMP authorized. In contrast, because Acuity proposed a non-cloud based system, the RFP established that it would be assessed based on whether the proposed system was currently operating under an ATO approved by DHS or one of its components. Thus, it is immaterial that Dentrust's system is also currently being used by other DHS subagencies because it is a cloud-based solution that needed to possess FedRAMP authorization according to the solicitation's requirements, and, therefore, we find no basis to conclude that offerors were treated disparately.[10]

On this record, we have no basis to question the reasonableness of the agency's evaluation and assessment that Acuity's technical approach merited a rating of high confidence under the technical capability factor. Ultimately, we find that Acuity's higher confidence rating stemmed from differences between its own non-cloud based system and Dentrust's cloud-based system and does not represent disparate treatment. *See Sys. Implementers, Inc. et al.*, B-418963.5 *et al.*, B-418986 *et al.*, *supra*.

The protest is denied.

Edda Emmanuelli Perez
General Counsel

[10] To the extent that the protester believes the solicitation's requirements for cloud-based systems were unreasonable or that the solicitation should have placed more onerous security requirements on non-cloud-based systems, such objections to the solicitation's ground rules are untimely raised post-award. *See* 4 C.F.R. § 21.2(a)(1) (requiring protests based upon alleged improprieties in a solicitation which are apparent prior to bid opening, or the time set for receipt of initial proposals to be filed prior to bid opening, or the time set for receipt of initial proposals).