



Cheryl R. Bailey, Ph.D.
Acting Executive Officer

DISTRICT OF COLUMBIA COURTS
Administrative Services Division
Office: Gallery Place
616 H Street NW, 6th Floor
Washington, DC 20001
Mailing Address: 500 Indiana Avenue NW
Washington, DC 20001-2131



Louis W. Parker, MBA
Administrative Officer

Herbert Rouson, Jr., J.D.
Acting Deputy Executive Officer

AMENDMENT NO. 4

TO: ALL PROSPECTIVE OFFERORS

AMENDMENT

ISSUE DATE: July 12, 2021

OFFER/BID FOR: DCSC-21-FSS-87 - Security Information & Event Management (SIEM)

SUBMISSION

DATE: July 21, 2021, by 1:00 p.m., Eastern Standard Time.

Responses to written question(s) received from prospective offeror(s) are included as Attachment A to this amendment.

ALL OTHER TERMS AND CONDITIONS REMAIN UNCHANGED

One (1) copy of this amendment is being sent to only those offerors who received a copy the solicitation. Offerors shall sign below and attach a signed copy of this amendment to each offer to be submitted to the Courts in response to the subject solicitation. Offers shall be delivered in accordance with the instructions provided in the original solicitation documents. This amendment, together with your offer must be received by the District of Columbia Courts no later than the date and time specified for offer submission. Revisions or price changes occasioned by this amendment must be received by the Courts no later than the date and time set for offer submission. Failure to acknowledge receipt of this amendment may be cause for rejection of any offers submitted in response to the subject solicitation. Offerors who have already submitted their responses may revise their technical and/or price proposals.

Darlene D. Reynolds

Darlene D. Reynolds
Contracting Officer

This amendment is acknowledged and is considered a part of the subject solicitation.

Signature of Authorized Representative

Date

Name of Firm

Title of Authorized Representative

DCSC-21-FSS-87 - Security Information & Event Management (SIEM)

ATTACHMENT A Response(s) to Question(s)

Question #1:

Specifically, if DC Courts is expecting your Managed Services provider to monitor, alert, and potentially remediate potential alerts that are generated from your SIEM, does their SOC need to be FedRAMP certified? Typically, if a team is monitoring and responding to alerts, all of this data is forwarded to a service provider's location that is off site or it is stored locally on site and then forwarded to the MSSP that is off site.

In reading your RFP, it appears that if FedRAMP is a requirement, both the location of the SIEM and the MSSP's facility must be FedRAMP certified, is this correct? or can the MSSP SOC be non FedRamp certified and in either case, what type of connection between the location of the SIEM and the location of the MSSP's SOC is acceptable to DC Courts?

RESPONSE # 1:

Incorrect, **SIEM LOCATION**. The location that is hosting the SIEM must be FedRamp certified or show proof that it is in the process. **SOC LOCATION IF NOT SAME AS SIEM LOCATION**: If the vendors (SOC) facility if not hosting the SIEM it only has to have a FISMA ATO or show proof that it is in the process.

RESPONSE #2:

CONNECTION: The connection between is at the discretion of the Vendor but must meet these basic requirements. NO delays in the transmittal of data and reporting (example if the SIEM reports a high or critical Alert) we don't want the response to be delays and be a detriment to the DC Courts security. The Vendor must know their products and know what an acceptable connection is. Also, the installation must meet FISMA accreditation requirements.