PROCUREMENT OFFICER'S DETERMINATION
Intergovernmental Cooperative Purchasing
COMAR 21.05.09.04

Department/Procurement Agency: Department of General Services

Contract Term: One Year

Amount: Estimated $270,000

Category: Information Technology

Contract Type: Fixed Price

Name and address of selected Contractor: To be determined by issuing a request for quotation to the NASPO ValuePoint (or ICPA) contract resellers identified by Palo Alto Networks.

Scope Description:

Purchase of the following Palo Alto Networks products/services:

- Palo Alto Networks Expander Platform (PAN-EXP-EXPNDR) – Expander web-based subscription platform, includes 999 AUM (Assets Under Management) and Basic Customer success – Term 12 months
- Palo Alto Networks Expander Network Mapping (PAN-EXP-EXPNDR-DLF-5) – Expander Network Mapping for 150,000-299,999 AUM (Assets Under Management) – Term 12 months
- Palo Alto Networks Premium Success (PAN-EXP-PREM-SUCCESS) – Premium Success Plan includes onboarding assistance, continuous guidance, periodic operational reviews, and access to customer support portal and 24/7 telephone support – Term: 12 months

The Department of IT (DoIT) Office of Security Management (OSM) currently monitors over 220,000 external IP addresses using a variety of manual methods and technologies. Cyber security analysts correlate observations from these disparate processes with known threat intelligence to identify risk to internet-exposed IT assets. This information is used to inform senior leadership and prioritize action taken by the Maryland Security Operations Center (SOC) to reduce risk across the state.

The manual nature of this process is time consuming and error prone; resulting in delayed action by the SOC and reduced confidence in the intelligence gathered.

The DoIT OSM requires an External Attack Surface Management (EASM) platform to provide a comprehensive and continuously updated inventory of the State's global internet-facing assets from the external attacker's perspective.

The purchase of the Palo Alto Network's Expander platform will aid in the identification of both known and potentially unknown internet and attacker-exposed IT assets as well as to monitor them for

unexpected changes and vulnerabilities that increase risk. Having Expander will allow OSM & Maryland Security Operations Center to discover, evaluate, and mitigate cyber-attack surface risks more quickly and with greater confidence.

Since EASM is an emerging technology, DoIT OSM needs flexibility to adapt as the technology and capabilities change by only committing to a one-year contract.

Basis for Selection:

DoIT OSM's evaluation of EASM products focused on those which are leaders in the industry, and which are produced by vendors who supply other products we use within our environment. EASM offerings from two vendors were evaluated. Palo Alto Networks and Recorded Future. With the EASM industry being relatively new, 3rd party evaluations were difficult to rely upon.

This evaluation, between February and May 2022, included independent research, a series of product demonstrations and meetings with each vendor, and limited access to the platforms to evaluate capabilities and ease of use. Evaluation criteria and required features were developed by the OSM based on current and projected future needs of the team and to satisfy the reporting requirements being developed to support the Maryland Chief Information Security Officer.

Palo Alto Network's product, Cortex Xpanse (also known as Expander) is a leader in the EASM space. DoIT uses Palo Alto firewalls for its Managed Firewall service offering. Cortex Xpanse, acquired by Palo Alto Networks in 2020, was originally founded in 2012 and demonstrated the most maturity among the products evaluated. Expander builds an inventory of exposed systems by continuously scouring the entire internet and, using automated processes, associates those systems and services to the State. That asset inventory is leveraged to create risk profiles and actionable intelligence. Expander had the most mature integrations with existing products to include Palo Alto's Cortex line, as well as ServiceNow which is the incident management system used by the Maryland Security Operations Center.

Recorded Future's product, Attack Surface Intelligence, is a new offering resulting from an acquisition of the internet inventory company SecurityTrails in January 2022. The DoIT OSM uses Recorded Future today to collect, structure and analyze threat intelligence information that exists on the internet. Recorded Future's EASM solution is based on current and historical Domain Name System (DNS) record and IP address data collected by SecurityTrails. This solution lacked many of the desired features and functionality being evaluated and did not have integrations into existing tools, including Recorded Future.

As part of the evaluation, DoIT also reviewed all of the products listed in the Gartner report "Innovation Insight for Attack Surface Management" as well as the newly acquired by Recorded Future "Security Trails" attack surface management. Based on our review, only three companies offered a product that met our requirements for system integrations and functionality (Cyberpion, Randori, and Palo Alto) and only two offered all the desired integrations (Cyberpion and Palo Alto). Unfortunately, Cyberpion operates outside of the US and based on the connection to sensitive security data, presents an unacceptable risk. This left us with only one viable product option.

This market is very new, and as such will likely see a significant transformation in the coming years. For this reason, we opted for the one-year contract term over three years.

Regarding the competitiveness of pricing, the pricing through NASPO is approximately 60% off the list price. This price is lower than what the State would expect to see in an open market procurement. We

estimate that this reduces the need for two full-time senior resources, which would provide a cost-saving to the State and will help DoIT modernize the way that we identify risk to the State. Because the product functionality is emerging, it is expected that we will be able to conduct another product comparison in the future.

The use of this procurement method will reduce the time-period between need determination and delivery of the solution; will ensure expeditious transparency to the citizens of Maryland and reduce the administrative burden on DGS. In accordance with COMAR 21.05.09.04, it is determined that this Participating Addendum will provide cost benefits to the State, will promote administration efficiencies, and promote intergovernmental cooperation. The Participation Addendum is in the best interest of the State and is not intended to evade the purpose of Division II of the State Finance Procurement Article.

Determination By:

Susan Howells

Date: June 16, 2022

DoIT, Procurement Officer

Approved by:

Michael Leahy
Michael Leahy (Jun 16, 2022 14:41 EDT)

Date: Jun 16, 2022

DoIT, Secretary (or designee)

Approved by:

Date: Jun 17, 2022

DGS Chief Procurement Officer