



Wes Moore, Governor · Aruna Miller, Lt. Governor · Atif Chaudhry, Secretary

**Intergovernmental Cooperative Purchasing Agreement
Procurement Officer Determination**
COMAR 21.05.09.04

Per COMAR 21.05.09.02, as a Primary Procurement Unit, the DGS Office of State Procurement (OSP) may initially sponsor or participate in, renew, modify, or administer an Intergovernmental Cooperative Purchasing Agreement (ICPA) on its own behalf or on behalf of another agency when a determination is made under SFP §13-110 and COMAR 21.05.09.04.

Based upon the analysis and market research conducted as identified in the attached Procurement Officer's Determination, from the Department of Information Technology, Office of Security Management (OSM) for Proofpoint (PSAT - Enterprise Vr.2) Contract, I have conducted an independent analysis and determined that it is in the best interest of the State to participate in this intergovernmental cooperative purchasing agreement, that doing so will provide cost benefits to the State, promote administrative efficiencies, or promote intergovernmental cooperation, and is not intended as a means to evade the purposes set forth under COMAR 21.01.01.03.

Cheryl Howard-Bond

Jan 17, 2024

Cheryl Howard-Bond, Procurement Officer, DGS OSP / Date

Jamie Tomaszewski

Jan 17, 2024

Jamie Tomaszewski, Acting Chief Procurement Officer / Date

Atif Chaudhry

Mar 14, 2024

Atif Chaudhry, Secretary, DGS / Date

Attachment

PROCUREMENT OFFICER'S DETERMINATION

Intergovernmental Cooperative Purchasing

COMAR 21.05.09.04

Department/Procurement Agency: Department of Information Technology

Contract Term: 1/5/2024 – 9/15/2026

Amount: \$231,132.31

Category: Information Technology

Contract Type: Fixed Price

Name and address of selected Contractor: SHI – 290 Davidson Avenue, Somerset, NJ 08873

Scope Description:

The Department of Information Technology (DoIT), Office of Security Management (OSM) is charged with managing security awareness training for all appropriate employees of units of State government. OSM would like to procure a software-as-a-service (SaaS) security awareness training platform/solution that is the best fit for the state based on the requirements outlined by a Statewide cybersecurity assessment and the needs of the state during the time of this evaluation.

After the development of numerous requirements and multiple vendor demos, OSM determined that Proofpoint meets and exceeds the requirements for a security awareness training and phishing simulation platform and is the best fit for OSM's managed security awareness training program/service. Proofpoint provides the following capabilities and features:

- Supports security awareness training for general business users and general user groups.
- Supports role-based training for users in positions required to handle and access sensitive data, administer information systems, privileged access, or have technical/operational security responsibilities
- Includes a simulated phishing platform built into the existing tool
- Integrates reporting to support monitoring of training completion, participation, and trending analysis over time across multiple agencies and central IT
- Provides technical support via email/phone/chat
- Supports multiple browsers (e.g., Chrome, Firefox)
- Supports multiple languages
- Provides support for audio/visual impairment support
- Has APIs and other integrations with email platforms
- Allows different file types to be downloaded such as SCORM and MP4
- Includes restricted self-service options and administrative options for agency security awareness training managers to add/remove users as staffing changes
- The solution is SaaS/ Cloud-based, including the primary management console and content library
- The solution has automated options for auditing user accounts and permissions
- The solution has trackable scoring and assessment completion reports/certificates for each end user as they complete courses to test their understanding of concepts
- Courses and modules have knowledge-based assessments to test individuals

- Reporting includes preconfigured templates for dashboards, graphs, and lists
- Training for general users
- Includes general security modules for new employees or annual training
- Role-based has modules and courses
- Integrates with a phishing platform/simulator to conduct phishing campaigns and automate phishing responses

Basis for Selection:

The DoIT OSM selected vendors identified in the FORRESTER WAVE infographic Leaders and Strong Performers section (see Figure 1) for evaluation of security awareness and training products. OSM evaluated Infosec Institute, Knowbe4, Proofpoint, and SANS against a list of functional and non-functional requirements based on the operational needs of the State and the service it provides to units of state government. Among these requirements are:

- Supports security awareness training for general business users and general user groups
- Supports role-based training for users in positions required to handle and access sensitive data administer information systems, privileged access, or have technical/operational security responsibilities
- Integrates reporting to support monitoring of training completion, participation, and trending analysis over time across multiple agencies and central IT
- Multitenancy
- Provides granular role-based access to tenants
- Supports Single Sign-On (SSO)
- API support
- Section 508 compliance
- Provides phishing simulations and automates email analysis and response

The Forrester Wave uses a transparent methodology to compare the players in a software, hardware, or services market so our buyers can make well-informed purchasing decisions.

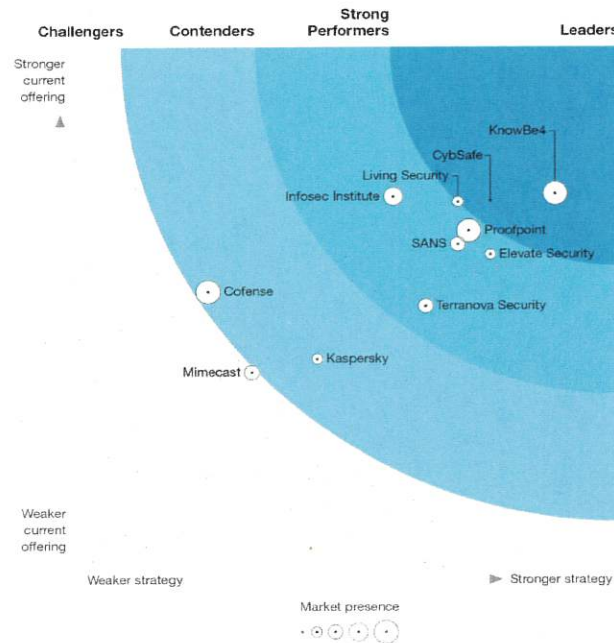
FIGURE 1

Forrester Wave™: Security Awareness And Training Solutions, Q1 2022

THE FORRESTER WAVE™

Security Awareness And Training Solutions

Q1 2022



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 1 Forrester Wave infographic

After an initial capability assessment, the OSM team determined the only solution that could potentially provide the requisite functionality needed by the state was Proofpoint. The principal limitations that excluded other vendors were:

- The solution(s) placed limits on the number of Active Directories that can synchronize to the platform.
- The solution(s) parent account did not have roll-up reporting capabilities from all child accounts and the ability to roll out training and phishing campaigns to any/all child accounts.
- The solution(s) did not have a setting to configure the relative duration end date for users enrolled in a training campaign.
- The solution(s) did not offer robust Role-Based Training.

This evaluation, between April 2023 and June 2023, 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 the current and projected future needs of the team and to satisfy the reporting requirements.

Proofpoint is the vendor that could successfully integrate into the OSM service model and provide a mechanism to centrally manage multiple customer training requirements. It also takes a holistic approach to cybersecurity education and awareness and will provide the State of Maryland with a proven framework that drives behavior change and real security outcomes. With Proofpoint Security Awareness Training (PSAT), the State of Maryland can tailor cybersecurity education online to target the

vulnerabilities, roles, and competencies of State of Maryland employees. Additionally, Proofpoint Security Awareness Training (PSAT) provides education in bite-sized chunks, so it creates sustainable habits.

Training Platform Pricing:

| Security Awareness Platform (56,000 licenses) | Price per License | 3 Year | Total [three [(3) year base] | 1 Year Option | 2nd Year Option |
|--|--------------------------|---------------|-------------------------------------|----------------------|------------------------|
| <i>Proofpoint (PSAT - Enterprise Vr.2) 90-day Fixed Onboarding Package \$7,368.42</i> | \$3.82 | \$213,920.00 | \$221,288.42 | 78K | 78K |
| <i>InfoSec Institute (Infosec IQ Enterprise)</i> | \$1.50 | \$252,000.00 | \$252,000.00 | 84K | 84K |
| <i>KnowBe4 (Platinum) Does not include Managed Services</i> | \$7.20 | \$403,200.00 | \$403,200.00 | 134,400.00 | 134,400.00 |
| <i>SANS Institute (Security Awareness)</i> | \$14.74 | \$825,540.00 | \$825,540.00 | 288,439.00 | 288,439.00 |

Conclusion

The use of this procurement method will reduce the time between need determination and delivery of the solution; will ensure an expedient time to value for the State of Maryland; and reduce the administrative burden on DGS. NASPO is the nation’s largest and most experienced cooperative purchasing organization for the public sector. Additionally, all contracts available through NASPO are competitively solicited and publicly awarded by a lead agency, using a competitive solicitation process consistent with applicable procurement laws and regulations. In accordance with COMAR 21.05.09.04, it is determined that this ICPA will provide cost benefits to the State, will promote administration efficiencies, and promote intergovernmental cooperation. The ICPA 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:

Carla Thompson

DoIT, Procurement Officer

Date: 12/9/2023

Approved by:

Melvin L. Leman

DoIT, Secretary or Designee

Date: Dec 11, 2023











DGS OSP ICPA POD for DOIT Proofpoint Contract


Final Audit Report

2024-03-14


| | |
|-----------------|---|
| Created: | 2024-01-17 |
| By: | JAMIE TOMASZEWSK (JAMIE.TOMASZEWSKI@MARYLAND.GOV) |
| Status: | Signed |
| Transaction ID: | CBJCHBCAABAAJjuFhGdMhy1Pash9RxH5ydCMJGF6Na0D |

"DGS OSP ICPA POD for DOIT Proofpoint Contract" History


-  Document created by JAMIE TOMASZEWSK (JAMIE.TOMASZEWSKI@MARYLAND.GOV)
2024-01-17 - 3:12:06 AM GMT- IP address: 166.137.175.41
-  Document emailed to Cheryl Howard-Bond (cheryl.howard-bond@maryland.gov) for signature
2024-01-17 - 3:13:44 AM GMT
-  Email viewed by Cheryl Howard-Bond (cheryl.howard-bond@maryland.gov)
2024-01-17 - 3:19:20 PM GMT- IP address: 66.249.83.40
-  Document e-signed by Cheryl Howard-Bond (cheryl.howard-bond@maryland.gov)
Signature Date: 2024-01-17 - 3:19:47 PM GMT - Time Source: server- IP address: 167.102.225.96
-  Document emailed to JAMIE TOMASZEWSK (JAMIE.TOMASZEWSKI@MARYLAND.GOV) for signature
2024-01-17 - 3:19:49 PM GMT
-  Email viewed by JAMIE TOMASZEWSK (JAMIE.TOMASZEWSKI@MARYLAND.GOV)
2024-01-17 - 3:25:19 PM GMT- IP address: 66.102.8.76
-  Document e-signed by JAMIE TOMASZEWSK (JAMIE.TOMASZEWSKI@MARYLAND.GOV)
Signature Date: 2024-01-17 - 3:25:52 PM GMT - Time Source: server- IP address: 167.102.225.96
-  Document emailed to Atif Chaudhry (atif.chaudhry@maryland.gov) for signature
2024-01-17 - 3:25:54 PM GMT
-  Email viewed by Atif Chaudhry (atif.chaudhry@maryland.gov)
2024-01-17 - 3:26:00 PM GMT- IP address: 66.102.8.64
-  New document URL requested by Cheryl Howard-Bond (cheryl.howard-bond@maryland.gov)
2024-02-06 - 8:49:34 PM GMT- IP address: 167.102.225.96

 New document URL requested by Cheryl Howard-Bond (cheryl.howard-bond@maryland.gov)

2024-02-06 - 11:32:16 PM GMT- IP address: 166.137.19.60

 Email viewed by Atif Chaudhry (atif.chaudhry@maryland.gov)

2024-03-14 - 9:03:13 PM GMT- IP address: 66.249.83.41

 Document e-signed by Atif Chaudhry (atif.chaudhry@maryland.gov)

Signature Date: 2024-03-14 - 9:08:02 PM GMT - Time Source: server- IP address: 167.102.225.96

 Agreement completed.

2024-03-14 - 9:08:02 PM GMT