LARRY HOGAN
Governor

BOYD K. RUTHERFORD
Lieutenant Governor

MICHAEL G. LEAHY
Secretary

Department Of
INFORMATION
TECHNOLOGY

State of Maryland
Department of Information

Questions and Answers #1
RFP No. 060B8400104
Domain-Based Message Authentication, Reporting and Conformance (DMARC)
Support Services
March 7, 2019

Ladies and Gentlemen:

This list of questions and responses is being issued to clarify certain information contained in the above referenced RFP. The State's responses are italicized. The statements and interpretations contained in responses to any questions, whether responded to verbally or in writing, are not binding on the Department unless the RFP is expressly amended. Nothing in any response to any questions is to be construed as agreement to or acceptance by the Department of any statement or interpretation on the part of the entity asking the question.

1. Can you please provide a list of all emailing subdomains under Maryland.gov that are to be included under the contract?

    ANSWER: *There are no other sub-domains.*

2. What is the typical outbound email volume across all emailing domains to be included under the contract (i.e. average daily or weekly outbound email volume)?

    ANSWER: *Avg. Bi-Weekly: Sent - 175,931, Received: 955,746*

3. Are there additional Maryland domains other than Maryland.gov that will be included under the contract (such as md.gov, md.us, or other Maryland state domains that may be targeted by hackers for fraudulent use)? If so, what other domains are to be included, and what is the typical daily/monthly email volume from these domains and associated subdomains?

    ANSWER: *At this time, there is only one domain, Maryland.gov, that will be covered under the Contract. However, the State could request DMARC enforcement for other State-owned domains through the Work Order process listed in RFP Section 3.8. Information regarding sub-domains and email volume may be found in the answers to Questions 1 and 2.*

4. Requirement 2.3.1 states "The Contractor shall enact full enforcement of DMARC on the State's Maryland.gov email domain no later than three (3) years following Notice to Proceed (NTP)." Is Maryland defining DMARC enforcement consistent with the guidance provided by Department of Homeland Security Binding Operational Directive 18-01 for US Federal Agencies https://cyber.dhs.gov/bod/18-01/ . If not, please define the specific DMARC policies that must be enabled for "full enforcement" (i.e. p=quarantine or p=reject, subdomains included, percentage =100, etc.).

   ANSWER: *To DoIT, DMARC is "fully enforced" when the Contractor's solution is configured, tested, documented, implemented, and running on the Maryland.gov domain with a DMARC policy of p=quarantine.*

5. Requirement 2.3.1 states "The Contractor shall enact full enforcement of DMARC on the State's Maryland.gov email domain no later than three (3) years following Notice to Proceed (NTP)." Under this specification, Maryland.gov and its associated subdomains could remain unprotected for up to 3 years after contract award. Are there interim milestones or high priority domains that should be at enforcement prior to the end of the base contract period of 3 years?

   ANSWER: *No.*

6. Has the State implemented Domain Keys Identified Mail (DKIM) on the Maryland.gov domain?

   ANSWER: *Yes.*

7. Has the State implemented Sender Policy Framework (SPF) on the Maryland.gov domain?

   ANSWER: *Yes.*

8. Will the contractor have access to the Google Mail control panel?

   ANSWER: *The State cannot say at this time.*

9. Will the State provide a VM in either the State data center or existing AWS cloud to the contractor?

   ANSWER: *Yes, we can provide a VM.*

10. Given the time to respond to questions, and add them into the response, and the short deadline from date of issuance, will the state extend the response date by two weeks, to March 15, 2019?

    ANSWER: *Yes. See Amendment #1.*

11. Section 3.3.4 Information Protection: Please provide an overview of State of MD - DoIT's

- Data Loss / Leakage Prevention solution
- Internal / External / System (privileged/non privileged) user behaviour analytics and management
- Security Event & Incident Management (SEIM) and CDM (including Asset Management) tools and solutions

Is the current SOC at the State at SOC Level 2?

ANSWER: Section 3.3.4 refers to the Contractor's obligations in regards to the software (incl. software provided for the State's use) and hardware it uses for Contract. Consequently, the State does not believe that the requested information is relevant.

12. Please indicate how many 3rd party services the state uses to send email, and name them (bulk delivery services by agency)

ANSWER: Currently, the State uses Granicus/Gov Delivery for mass mailing. Also, a few agencies use Constant Contact and Mail Chimp.

13. Section 2.3.13 Please specify why type of network support is anticipated in this section, or provide an example

ANSWER: No network support will be needed.

14. Can the State please confirm that DMARC as a service response is acceptable (can be conducted off-prem)?

ANSWER: No, DMARC needs to be hosted internally.

15. Please provide a list of locations by server and agency, where the State servers are located. Are all email servicers in Maryland, or other states?

ANSWER: The State of Maryland uses Google Email Servers.

16. Is this a new project or is there an incumbent?

ANSWER: This is a new project.

17. If this is not a new project, what we the previous budget/ awarded amount for the program?

ANSWER: See response to question #16.

18. How many users?

ANSWER: Currently, there are 44,400 users on the Maryland.gov domain, but this figure could grow to 46,000.

19. How many sub-domains under Maryland.gov are to be included?

   ANSWER: *See response to Question #1.*

20. What is the total monthly or annual inbound and outbound average email volume for the maryland.gov domain?

   ANSWER: *See response to Question #2.*

21. Can MD DoIT provide a user count for this opportunity?

   ANSWER: *See response to Question #18.*

22. Can MD DoIT provide an approximate authentic e-mail volume on a monthly/annual basis?

   ANSWER: *See answer to Question #2.*

23. Does MD DoIT want to consider sub-domains under maryland.gov or just the TLD?

   ANSWER: *See response to Question #1.*

24. Please provide any currently known third party senders using the maryland.gov domain or a sub-domain.

   ANSWER: *See response to Question #12.*

25. Regarding Section 2.2.1, who is providing your Tier I IT support?

   ANSWER: *DoIT.*

26. Regarding Section 2.3.14, can you please describe your current LI-LIV support construct?

   ANSWER: *The State is unsure as to what this question refers. If it regards support levels like Tier I IT support, please see the response to Question # 25.*

27. What ticketing system, PSA/RMM systems are in use today?

   ANSWER: *The State uses ServiceNow.*

28. This question addresses support requirements and the Problem Escalation Procedure (PEP) covered in RFP Section 3.4.

   Section 2.1 only references Email Managers who are presumed to be your onsite Google staff. Tier I support is not mentioned. Section 2.3.14 describes contractor Tier II-IV requirements. Tier I support is not mentioned.

3.4 describes the need for a Problem Escalation Procedure (PEP). A thorough understanding of the existing or preferred support roles and responsibilities is needed to develop a PEP that will effectively augment or replace your existing capability.

ANSWER: *DoIT handles Tier I support using its Service Desk. The MD Google team would be Tier 2 support. Tier 3 would be vendors/contractors.*

29. Can you please clarify the scope of work and responsibilities of the contractor?

ANSWER: *The Scope of Work can be found in RFP Section 3. The Contractor will assist in implementing DMARC and train State of Maryland employees on how to ensure all email senders comply with DMARC requirements.*

30. With regards to Section 3.3.4, can you confirm remote monitor and management (RMM) functions are part of the performance requirements?

The title and beginning content of the RFP focus on DMARC implementation but deeper in the RFP there are more robust requirements that appear to expand scope of work and performance expectations.
Section 2.3 describes DMARC implementation tasks.
Section 3.3.4 describes activities normally associated with an IT managed services agreement. These tasks and responsibilities appear to be outside the scope of the requirements outlined in Section 2.3. These tasks and responsibilities require tools and software to be installed on network devices and computers as well as full administrative access.

ANSWER: *No. Please see the response to Question #11. The State is not interested in the Contractor installing network management or remote monitoring software on State-owned hardware or remotely and proactively monitoring State that hardware.*

Section 3.3.4 outlines the Contractor's responsibilities regarding its software and hardware usage. The State is not looking for the Contractor to manage the State's IT security operations or provide broad IT support.

31. Is there a no later than date stipulated for implementation of the first agencies?

ANSWER: *See answer to Question #19.*

32. Is there a prioritized list of those agencies to identify which agencies need to be cutover first? This requirement states, "The Contractor shall enact full enforcement of DMARC on the State's Maryland.gov email domain no later than three (3) years following Notice to Proceed (NTP)." In the pre-proposal conference, staff indicated there are approximately 52 agencies using the Maryland.gov domain.

ANSWER: *No. The State asks that offerors propose how, specifically, they intend to ensure full enactment of DMARC within 3 years of the Notice to Proceed. Therefore, offerors can propose their own work milestones or completion plan.*

33. Is the web-based portal requirement just during implementation or are you asking for a web-based dashboard and reporting capability as a persistent element of the contractor solution?

    ANSWER: *The A web based dashboard should be a persistent element of the contractor's solution.*

34. With regards to Section 2.3.14, can you please clarify and define "emergency"?

    ANSWER: *When messages are bouncing against DMARC policies.*

35. With regards to Sections 2.3.14 and 2.4, what is the response target for emergency calls?

    ANSWER: *The State, instead of listing response times/targets, wants offerors to propose response times.*

36. With regards to Section 2.4, what are resolution targets for non-emergency and emergency calls both during and outside normal business hours? Section 2.4 states an SLA is not applicable.

    ANSWER: *This State is allowing offerors to propose resolution targets.*

37. With regards to RFP Section 3.3.4, can you please confirm what tools and applications are already in use on Maryland.gov IT assets?

    Is it expected that contractor will provide these tools and applications? This section describes the need to conduct regular vulnerability testing. It directs contractor to implement and ensure compliance with local security policies, password controls. It describes the requirement to ensure all systems are current and up to date with required software and security patches and updates.

    ANSWER: *Please see the response to Question #11. Section 3.3.4 covers the Contractor's hardware and software solutions used to carry out its contractual duties. The State isn't looking for the Contractor to enact or manage the State's IT security.*

38. With regards to Section 2.3.12 Contractor – Supplied Hardware, Software and Materials – will software and network support tools be installed on current hardware? What if hardware is outdated?

    ANSWER: *This Section outlines the Contractor's requirements when providing software or network support to carry out its contractual duties. This may include, based on the Contractor's solution, the installation of Contractor-supplied software on State hardware.*

Contractors should outline hardware requirements for any proposed software in their proposals.

39. With regards to RFP Section 2.3.14.F – the State shall be provided with information on software problems encountered at other locations, along with the solution to those problems, when relevant to State software. Can you clarify "other locations"?

    ANSWER: *Locations used by other, non-State entities. Essentially, the State wants to know if other, non-State system/solution users are experiencing problems, if those problems are relevant to the State.*

40. Regarding RFP Section 3.4 Problem Escalation Procedure – can the process incorporate the use of a ticketing system (e.g. JIRA, SM9)?

    ANSWER: *Yes. Please note that the State uses Service Now as its ticketing system.*

41. Is there a specific template for the work plan referenced in Section 5.3.2.F?

    ANSWER: *No.*

42. For clarification, the Financial Proposal Instructions and Excel Attachment listed in Table 1 of Section 7 is submitted with the Financial Volume?

    ANSWER: *Yes.*

43. Regarding, Section 5.3.2, TAB I – if the company does not have current or past contracts with the State of Maryland, can other contracts (federal or commercial) be listed in this section?

    ANSWER: No. However, information for other, non-State contracts may be included in Tab G.

44. How many FTEs are allocated for this effort?

    ANSWER: The State will, as outlined in RFP Section 2.2.1, provide some staff to assist the Contractor. However, the State will not provide dedicated FTEs for this effort.

45. Can the Contractor perform its contractual duties offsite or does it need to ensure that employees are onsite at a State facility?

    ANSWER: *Other than knowledge transfer (see RFP 2.3.5) or training, the Contractor may perform its contractual duties offsite.*