Request for Information – Cybersecurity and Infrastructure Security Agency Protective Email Service

Agency: Cybersecurity and Infrastructure Security Agency / Cybersecurity Division / Capacity Building

Market Research Agency: CB

Notice Type: **Request for Information (RFI)**

NAICS: 541330 – Engineering Services; 541512 Computer Systems Design Services

GSA Reference: 47QFRA22K0005

Posted Date: November 17, 2021
Amended Date: November 23, 2021

I. GENERAL INFORMATION

This Request for Information (RFI) is being issued on behalf of the Cybersecurity and Infrastructure Security Agency (CISA). One of CISA's key missions is to protect federal networks and protect the Federal Civilian Executive Branch (FCEB) .gov domain enterprise from threats while strengthening cyber defenses. To that end, CISA is exploring a Protective Email Service (PES) to execute its mission to protect FCEB email traffic and to conduct threat hunting and incident response.

II. RFI OBJECTIVE

The purpose of this RFI is to assist the Government in conducting market research focused on feedback and insight from industry who offer a broad set of email security capabilities and those who have delivered similar complex solutions in the Federal Government or private sector space (see high level and functional capabilities listed in section IV). Feedback will assist the government in refining solution design, use cases, and functional requirements, provide insight into scalability of the potential service(s), assist the government in determining industry segmentation by capability and size, and provide insights into the current offerings of PES the federal and corporate landscape in developing a potential acquisition strategy.

The information provided as response to this RFI will be used for market research only. The Government is not obligated to release a future solicitation based on this market research.

III. BACKGROUND

CISA leads the national effort to defend critical infrastructure against the threats of today while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow. CISA's mission includes protecting the Federal Government's networks and physical infrastructure, helping entities in the public and private sectors manage potential risk, and enhancing public safety communications at federal, state, local, tribal, and territorial governments.

In support of the FCEB, CISA is exploring a PES solution to protect email traffic and to conduct threat hunting and incident response.

The CISA PES objectives are to:

- Normalize and provide baseline security and visibility for FCEB email.
- Detect and protect federal enterprise from malicious email content as part of the CISA mission to manage FCEB risk.
- Detect and prevent the federal enterprise email from being used as a vector for malicious threat actors against itself and non-federal entities.

- Provide appropriate visibility into agency email traffic to enable CISA Global Operators to conduct cyber hunt and incident response.
- Be able to leverage CISA's and FCEB entity data holdings in cyber hunt, prevention, mitigation, and incident response activities.

CISA will provide PES for FCEB agencies. PES management will be a shared responsibility between CISA and FCEB agencies.

The subsequent sections describe the concept and general requirements of an email security service that could support FCEB agencies with the handling of email security based on government-wide standards, policy, and business requirements. CISA has not defined or approved a PES solution architecture.

IV. OVERVIEW OF SECURITY OPERATIONS SERVICES OFFERING

PES will be cloud-based and accessible to authorized entities via a management console and application program interfaces (APIs). The figure below shows PES, the PES-provided CISA Global Operator functions, and the FCEB agencies. PES deployment configuration, including the location of enforcement points, is not defined in the figure. The PES solution may or may not include the email platform.

CISA understands that PES can be delivered using a variety of architectural designs. For example, PES could be implemented directly on email platforms as a native security capability of the email platform. PES could also be implemented as a gateway service (e.g., Secure Email Gateway) where FCEB email traffic is directed to the gateway. Or a hybrid method could be implemented that offers a combination of enforcement points. It is expected that individual agencies will continue to own and operate their email services and host them either on-premises, in the cloud (e.g., Microsoft Office 365 and Google workspace), or with supplemental products or services that support hybrid environment.

Figure 1. Protective Email Service (PES) Overview

PES Use Cases

From an operational perspective, PES supports three basic use cases:

1. In Line Active Email Protection. As email traffic flows to and from FCEB agency email platforms, PES provides real time filtering and advanced (e.g., anomaly-based) protection using a combination of PES-provider indicators and CISA indicators.

2. Hunt and Incident Response. CISA Global Operators conduct analysis in support of hunt and incident response operations for all FCEB agencies.
3. PES Management. CISA will manage PES collaboratively with FCEB agencies. This may include PES policy settings, operations, and maintenance. The shared responsibilities between CISA and each agency will depend on the solution design.

PES Stakeholders

1. CISA Global Operators. CISA Global Operators will use PES to execute the CISA protection mission for all FCEB agencies.
    a. Provision CISA indicators.
    b. Conduct hunt and incident response missions.
    c. CISA Global Operators will have both console and API access to the solution.
2. FCEB Agency Email Administrators. Agency email service operators and administrators will continue to perform their operational mission. They will have access to their agency PES data and additional policy settings but will not be able to override CISA globally provisioned policies.
3. FCEB Agency Email Users. Agency email users will continue to use the email system with no impact to day-to-day operations (i.e., PES transition is seamless, and PES is transparent to end users).

PES General System Capabilities

Capability Area	Title	Description
Scalability	FCEB Agency Size	PES will provide PES to ~100 agencies and ~4 million users.
Technical Design and Architecture	FCEB Email System Platforms	PES will address all FCEB email platforms, including on-premises, cloud hosted, and hybrid.
	Email Protection Service Location(s)	Email protection services shall be 100% cloud-based. Physical appliances or other ancillary equipment (e.g., network taps, cabling) on agency premises will not be allowed.
Supportability	Customer Support	24/7/365 Customer support to CISA Global Operators and agencies.

PES Core Functional Capabilities

Capability Area	Title	Description
Email Protection Services	Email Attack Prevention	PES can prevent email attacks such as phishing, impersonation, account takeover, malware, spear phishing, and fraudulent email senders.
	Scanning and Filtering	PES can scan and filter email headers, attachments, email body, and file type extensions, and disable content URLs. Filtering decisions will be based on a combination of commercial and CISA proprietary threat intelligence feeds, and manual/custom rules created by email administrators.
	Sandbox (Local and Network)	PES can sandbox (quarantine) email on the email platform, on the endpoint (via application or browser),

Capability Area	Title	Description
		or at a point before it enters the network (e.g., at a gateway or on an appliance that sits in front of the email platform).
	Custom Filtering	PES can create custom email filtering according to specific organization policies
	Email Compromise and Data Loss Prevention	PES can prevent email compromise and data loss by inspecting emails with sensitive information (e.g., Social Security numbers, credit cards, license numbers, medical information).
	Advanced Protection	PES can perform advanced email protections (i.e., threat feeds, Machine Learning).
	Email Protection Service Roles	PES can provide identity and access management capability to support the following roles: 1) CISA Global Operator Access. CISA shall have access to the service as required by CISA protection mission across all FCEB agencies. a. Includes the ability to provision CISA indicators. b. Includes authorized contractors and service providers. c. Includes both console and API access to the solution. 2) FCEB Agency Email Administrator Access. Agency operators and administrators shall have access to the service. 3) FCEB Agency Email User Access. Agency email users shall have the ability to use the email system with no impact to day-to-day operations (i.e., any cutover or transition is seamless).
	API Access	PES can securely access various API services including the service required for log extraction.
Email Platform Configuration	Email Security Baseline Configuration	PES can include detailed engineering configuration guides for use in standardizing email platform security at all FCEB agencies.
	Agency Compliance Tracking	PES can identify FCEB agencies that do not have a compliant configuration.
Data Analyses, Visualization, and Dissemination	Metrics	PES can provide metrics around reports, offering FCEB and CISA insight into the reporting process. These may include: 1) Daily, weekly, or monthly threat trends. 2) Custom threat trends specific to threat campaigns or departments/agencies. 3) Identify behavioral threats based on behavioral intelligence. 4) Identify and track a variety of malicious threat campaigns. 5) Provide intel trends for malicious actors and threats.
	CISA Global Operator Query	PES can enable CISA Global Operators to conduct both single agency and across-FCEB queries for all FCEB email systems.

Capability Area	Title	Description
Data Access	Email Data Access	PES can access all FCEB agencies complete email storage for at least 1-2 years and malicious email storage for at least 2-3 years.
Real-Time Notifications and Situational Awareness	Alert/Block Notifications	PES can provide and enable CISA with immediate real-time notification (alert/block) notification/situational awareness on phishing, impersonation, account takeover, malware, spear phishing, and fraudulent email activities.

V. INDUSTRY MEETINGS

Based on responses provided by industry additional information may be requested. As a result, the General Services Administration with CISA, at the Government's discretion, may schedule a larger conference or meetings with industry to discuss responses to this RFI. If a follow-up meeting is required, the Government will reach out directly to the industry partner point of contact.

VI. RFI RESPONSE

Interested parties should respond to this RFI outlining their capabilities (as guided by the below comments/questions and the overview listed above) as well as approach recommendations to providing services associated with the broad scope of email security requirements. Responses may include references to examples that align with capabilities, existing offerings or services currently provided by the responder.

CONTENTS

"Section 1" of the response is for administrative information and shall include the following as a minimum:

A. Contractor name and facility address (list all relevant or significant office locations)
B. DUNS number and NAICS code
C. Socio-economic status (HUBZone, Service-Disabled-Veteran-Owned, Woman-Owned, 8(a), Small Business, Large Business)
D. Facility clearance level
E. POC name, phone, and email
F. Website URL

The number of pages in "Section 1" of the whitepaper shall be no longer than one (1) page in length. "Section 2" of the submissions shall answer/address the below questions and functional areas as they relate to the capabilities listed above. Respondents should highlight examples of current support or solutions that are deployed to federal or commercial organizations (if applicable):

1. Corporate Capabilities/Background:
    a. Indicate the number of years your company has offered email security solutions/services to federal or corporate entities.
    b. Identify acquisitions, joint ventures, or partnerships with other providers/companies related or similar to those with PES capabilities.
    c. Identify any existing Government contract vehicle(s) in place to provide PES (government-wide acquisition contracts, Federal Supply Schedules, blanket purchase agreements, etc.).
2. Email Service Design:
    a. Please describe a recommended approach to meeting PES requirements that the Government should consider.

i. Hosting – Cloud hosted solutions are required. Describe the interoperability with portability to different cloud solutions and on premise.
ii. Customization – Describe any customization and tailoring that may be needed to meet the objectives described above (from your current commercial offering).
iii. Third-Party Dependencies – describe any third-party dependencies to implement a solution as described above (e.g., other vendors and providers are required or desired).
iv. Enforcement Points – Describe any filtering enforcement point(s) that would be relevant to the recommendation, including the technical approach to ensure each enforcement has full visibility of email traffic.
v. Solution Differentiators – Describe any unique aspects of your recommendation that differentiate it from other offerings that are in the marketplace (e.g., federated access to logs, Roles-Based Access Control provisioning techniques, data normalization and enrichment in supporting of CISA mission).
vi. Solution Security – What should the Government consider regarding the security of a PES approach? For example, due to the high sensitivity of email content, please highlight if any of your current offerings are Federal Risk and Management Program (FEDRAMP) authorized, if there plans for authorization for current offerings or if there are specific challenges associated with current offerings.

3. PES Scalability:
    a. What considerations or recommendations regarding vendors ability to scale to the mission as described (100 FCEB agencies, up to 4 million users)? Please share experiences, analysis, demonstrations, etc.
4. The Government is interested in learning more about industry's current email service features:
    a. Please highlight your current PES feature set.
    b. Please describe a notional technology roadmap as it relates to the PES mission.
    c. Describe any unique selling points.
    d. Spam and malware detection effectiveness: if applicable, please show evidence of detection rate and false positive rate.
    e. If applicable, please describe existing outbound content controls and data loss prevention capabilities.
    f. Response capability: if applicable please describe existing features which identify and remove malicious emails/attachments that bypass initial detection.
    g. Email spooling capabilities: if applicable, please describe existing ability to avoid the risk of losing emails due to server or internet connection.
    h. If applicable, please describe denial-of-service attack protection capabilities.
5. Operational Level of Effort:
    a. What considerations or recommendations should the Government review for a 24/7 staffing requirement of the service?
    b. Describe the level of support services including help with design, implementation, and on-going operations?
6. FCEB Outreach:
    a. What recommendations should the Government consider in terms of customer (FCEB agency) outreach?
7. Transition Strategy:
    a. What are the considerations for migrating a wide array of agencies to an email security service?
8. Technical Risks:
    a. What are the risks associated with PES that the Government should consider? Please identify any risks for alternate approaches that the Government should consider.
    b. What are the risks associated with vulnerability management and the delivery of security patches?
9. Recommendations for the Acquisition Approach:

a. What should the Government consider as part of their acquisition approach for this potential service offering?
b. Describe your understanding of the current federal landscape for PES capabilities.
    i. What existing vehicles exist to support large scale implementations?
    ii. Would a large scale CISA services offering overlap with existing vehicles? If so, how?
    iii. Do you see any gaps in current services offerings? If so, please describe.

10. Time to Implement:
    a. What should the Government expect as an estimated timeline required to implement PES?
11. Cost and Pricing Structure: **(PLEASE NOTE: The Gov is not requesting a cost/price quote for any specific pieces. We are looking for the how and/or why behind each of the points listed below.)**
    a. Please highlight the recommended licensing model you would recommend for this type of email security service, such as per seat, per traffic volume, etc.?
        i. How are costs addressed based on expansion of customer base?
    b. Identify pricing differentials for capabilities offered and/or bundled offerings (i.e., sophistication, complexity, or scale)?
    c. Please provide the method you would use or have used in the past to cost the implementation and long-term operations of a PES solution (i.e., separate services offerings versus specific stock keeping unit for operations and maintenance)?
    d. Indicate and describe the pricing model for managing/monitoring virtualized services to include data logging, storage, infrastructure, etc.

VII. CONTRACTOR NOTIFICATION AND SUBMITTAL INSTRUCTIONS

This RFI is for information and planning purposes only and does not constitute a Request for Quote; it is not to be construed as a commitment by the U.S. Government. No award will be made from this RFI. All information is to be submitted at no cost or obligation to the Government. Any information that the contractor considers proprietary should be clearly marked as such. All submissions become Government property and will not be returned, including any proprietary information. Contractors who do not respond to this RFI are not excluded from any resulting solicitation(s).

The Government may consider additional communications with submitting companies using the contact information provided in the “Corporate Overview” to further the Government’s market research for the email security services support.

- All responses are to use 11-point Times New Roman font and one-inch margins, single spaced in all sections in Microsoft Word.
- Contractor Information section (Section 1) shall be no longer than one (1) page in length.
- Response to questions (Section 2) should be no longer than nine (9) pages in length.
- All information submitted shall be UNCLASSIFIED.
- Any information that the contractor considers proprietary should be clearly marked as such.
- All submissions become Government property and will not be returned (including any proprietary information).