סייבר ישראל
משרד ראש הממשלה
מערך הסייבר הלאומי

Israel National Cyber Directorate

Request for Information (RFI)

No. 0205/2023

Subject: Protective DNS Service (PDNS)

May 2023

Preliminary Request for Information (RFI) for:
Protective DNS Service (PDNS)

1. Background and purpose of the RFI

1.1 The National Cyber Directorate wishes to receive information about Protective DNS (PDNS) service in cloud configuration (SaaS) that will constitute a component of the Cyber defense national solution for the market known as the Cyber Dome and will enable the implementation of protection at a state level in the DNS protocol layer.

1.2 The purpose of the service is to increase the resilience of the market by preventing access to malicious domains for the purpose of safe internet usage.

1.3 As part of this request, the Israel National Cyber Directorate wishes to examine, among other things, the possibility of operating the service internally, as well as allowing organizations and users in the market to operate this service, at the level of the various sectors, of critical state infrastructures and more, so that each user and/or organization can operate the service in an independent and direct manner (including registration for the service). The Israel National Cyber Directorate will be able to operate the service for the Directorate itself as well as to manage, at a super-management level, the service for certain groups of organizations, from various aspects (for example, basic policies required for protection) at the same time as the ongoing operation of the organizations for themselves.

2 General

2.1 This is a preliminary **request for information** in accordance with Regulation 14A of the Mandatory the TenderRegulations, 1993. It is not designed to establish any obligation towards any of the respondents and/or to be considered as an agreement of any kind. The request is intended for receiving information only, and following it the Directorate will consider its next actions in accordance with professional and practical considerations.

2.2 If and whenever a tender or other procurement procedure will be carried out in the future, the Directorate will be entitled to change or add conditions and requirements, all according to its professional judgment and according to its needs.

2.3 The Directorate will be entitled to make use of the information provided to it in response to this request, and the supplier will have no copyright claims.

2.4 Response to this request will not constitute a condition for participation in the tender, if and should a tender be conducted subsequently, and no advantage will be given in the tender to

those who responded to the request just because they responded to it, and it will not require his participation in the tender or obligate entering an agreement with him in any other way.

2.5 You can view and download the complete documents of the RFI on the website of the Government Procurement Administration: https://www.mr.gov.il/Pages/HomePage.aspx or on the website of the National Cyber Directorate at: http://cyber.gov.il.

2.6 Below is a table listing the dates for this RFI:

Activity	Date	Hour
Date of publication of the RFI	2.5.23	14:00
The deadline for submission of clarification questions from the suppliers	14.5.2023	12:00
The deadline for the Directorate's answers to the clarification questions	23.5.2023	12:00
The deadline for submitting answers	30.5.2023	12:00

3 Basic Terms:

3.1 **Security service Protective DNS (PDNS) -** a service that analyzes queries / translation requests (DNS Queries) and takes actions to deal with threats using the DNS protocol and existing architecture. The service prevents access to malware, ransomware, ransoms, phishing attacks, viruses, spyware, access and/or use of malicious communications and/or websites and more.

3.2 **Indicator -** an identification item, for example a domain, IP address, etc. that can be checked as suspected of malicious activity and/or access to it can be blocked.

4 Specification of requirements

As part of this RFI, the National Cyber Directorate (hereinafter: "**the Directorate**") requests information about the service that provides a response as detailed below.

It should be clarified that the requested solution is intended to be integrated into organizations with different characteristics operating in the market (infrastructures, government organizations,

industrial organizations, etc.) according to the needs and characteristics of the organization and group of organizations.

4.1 **The respondent will detail the service capabilities with reference to the following aspects:**

4.1.1 Is the service a SaaS?

4.1.1.1 Is the respondent capable of operating the service based on the cloud infrastructures selected in the "Nimbus" tender (central tender 01-2020 for the provision of cloud services on a public platform for government ministries and auxiliary units), AWS or GCP and can the bidder establish a data center in the Israeli region with the cloud infrastructures selected in the "Nimbus" tender in order to provide the service from this center?

4.1.1.2 If the answer is negative, how long will it take to set up the service as described above?

4.1.1.3 You can learn about the government's requirements in terms of cyber protection, privacy, terms of use, storage and processing of information, as well as additional requirements in terms of information security in relation to working in the cloud, which the proposed solution is required to meet, in accordance with the details in the central tender for adding services to the government digital market in the cloud, which was conducted as part of the Nimbus project, and its documents are published on the Procurement Administration's website in the following link:

https://mr.gov.il/ilgstorefront/he/p/4000553566

4.1.2 What is the blocking mechanism activated as part of the service and what are the response options that the user can receive in case of blocking (general, dedicated blocking message, adjusted according to the client's needs, referral to a certain server, and more).

4.1.2.1 Is it possible to change/update the blocking policy for a certain user without it affecting other users?

4.1.2.2 Is it possible to make a change/update in the blocking policy for a certain user without the change being revealed to other users and/or being able to choose to whom the change will be revealed?

4.1.2.3 Does the service allow disclosure of the change in the blocking policy of a certain organization also to an organization in charge of it (for example, the National Cyber Directorate)?

4.1.2.4 Is it possible to define that a superuser (a user who is in charge of other organizations) will not be exposed to the updating of a user's blocking policy? Is there flexibility in blocking exposure to certain updates only?

4.1.2.5 Does the service use information and intelligence feeds to enrich information as a basis for updating the blocking policy?

4.1.2.6 What is the information and what are the intelligence feeds used for enrichment?

4.1.2.7 Is it possible for intelligence feeds to be added both by the respondent and by the user, and in what manner?

4.1.2.8 What is the number of indicators (quantity) that can be uploaded to the service as part of an intelligence feed in order to update the blocking policy?

4.1.2.9 Is it possible to set an indicator in monitoring mode only or once it is uploaded for service corresponding enforcement / blocking is implemented?

4.1.2.10 How is the risk level determined for an indicator / intelligence feed that is entered into the service (what is the formula)? On what basis is a decision about blocking / warning made (for example, what is the risk level threshold) and can it be changed by the user?

4.1.3 Does the service allow checking suspicious domains manually and/or automatically and how?

4.1.4 How does the service recognize that the DNS query originates from an authorized organization (an organization that uses the PDNS service)?

4.1.5 How does the service perform Threat Intelligence and Threat Hunting? Is there a methodology for this?

4.1.6 Does the service allow the use of IPV4 and IPV6 addresses and domains respectively?

4.1.7 What are the possible malware and attacks that the service identifies and how does it deal with them (for example, ransomware, viruses, spyware, phishing, command infrastructure, diversion, etc.)?

4.1.8 As part of the service, is it possible that files that the user uploads to the Internet or downloads from the Internet will also be blocked?

4.1.9 Does the service save and/or enable the saving of all the information created and processed in it?

4.1.9.1 What types of information are saved? For example, all browsing data for an IP or domain or some of it? What logs are kept? Are files that are uploaded to the Internet by the user saved? Are the names of the files uploaded to the Internet saved?

4.1.9.2 Where is the information stored?

4.1.9.3 How long is the information saved?

4.1.9.4 Can this information be exported and how? Is it possible to filter the exported information according to the user's request? Are there different options in this regard?

4.1.9.5 Is it possible to define in advance that a superuser will not be exposed to a certain type of information? (privacy protection aspects) If so, the various options must be listed.

4.1.9.6 To which systems can the information be exported without the need for modification?

4.1.9.7 Is there a hierarchy of system access privileges that is used in the process of exporting the information to users?

4.1.9.8 Examples of log files and alerts generated by the service must be attached to the response.

4.1.10 Does the service include mechanisms or architecture aimed at meeting privacy by design requirements?

4.1.11 Does the service have a Fail Safe capability that is "transparent" to the user, so that if there is a substantial failure in the provision of the service, it will be possible to switch to a normal working configuration without an operational shutdown. If this feature exists, will the transition to the work configuration without the service require the organization to make changes on its side?

4.1.12 Does the service base its blocking policy on the information accumulated in it and/or information from external and/or other intelligence feeds and in what way?

4.1.13 How does the service defend against DDOS attacks on the service itself, including reference to the types of attacks themselves and the number of requests per time period and/or volume rate per time period used for the attack?

4.1.14 Does the service allow locating the IP address at the level of the organization's network (internal IP) from which the browsing request (DNS Query) originated? Does the service allow locating a username within the organization from which the browsing request originated?

4.1.14.1 If so, how and is this feature activated automatically or manually (according to the user's choice)?

4.1.14.2 Is it necessary to install any type of software component within the organization's network for this purpose?

4.1.15 Does the service provide a solution to the situation where there is a communication disconnect between the State of Israel and the world and what is this solution?

4.1.16 What protocols does the service support?

4.1.16.1 Does the service support the provision of DNS over HTTPS (DoH) services?

4.1.16.1.1 It is necessary to specify how the service implements the support and deals with DoH.

4.1.16.1.2 In the event that the service does not currently deal with DoH, is such future support planned within the PDNS service and when?

4.1.17 Which DNS query records does the service support?

4.1.18 Does the service support remote work (Roaming Clients) and in what way? What are the Best Practices when working with users working from home (BYOD)?

4.1.19 What are the Best Practices when working with organizations that have a public cloud environment?

4.1.20 What is the structure of administration interfaces at different organizational levels (user, organization, group of organizations)?

4.1.21 Does the service support the use of White Labeling Domain / URL so that when a user accesses the PDNS service from an internal portal of the organization that uses the service (for example, the National Cyber Directorate), the user will see in the browser address bar that he is working in the organization's domain and not the respondent's?

4.1.22 What are the system access / edit privileges granted at each organizational level?

4.1.23 The report options that can be generated as part of the service.

4.1.24 The notification and alert options sent by the service.

4.1.25 The options for using the API and all the data that can be transferred through it.

4.1.26 The service's options for integration with third-party systems and tools.

4.1.27 The options for development and adaptation of the service and how they are implemented.

4.1.28 The international standards to which the service complies.

4.1.29 Options for implementing expert services (analysts, etc.) in addition to use of the service.

4.1.30 Implementation options and support for settings aimed at full utilization of the service (for example, support for adapting the existing infrastructures in the organization to use the service, such as FireWall settings, etc.).

4.1.31 The support, service, training and response time (SLA) model.

4.1.32 The service's information security features.

4.1.33 Is there a model for sharing the service with the market as a basic protection service which is free of charge?

4.1.34 In addition to the requested response as detailed above, the respondents may present additional and/or integrated capabilities and services (for example - protection service against a DDoS attack on the user / organization) as well as existing and future concepts and ideas.

4.2 **The respondent will provide information about the respondent company:**

4.2.1 Is the responding company the company that develops the service and its owner?

4.2.2 Is the implementation and support of the service provided directly by the responding company? If not, who provides the implementation and support?

4.2.2.1 What is the assimilation model, how and by whom is it carried out?

4.2.2.2 What is the support model, how and by whom is it implemented?

4.2.3 Does the responding company have a development and/or support center in Israel?

4.2.4 How many paying clients does the service currently have?

4.2.5 Are some of the paying clients financial and/or government clients? If so, how many are there and are they in Israel? For how many years?

4.2.6 How long has the service been on the market, used by the paying clients listed above, in Israel and around the world?

4.2.7 What is the pricing model, referring to the content of a license to use the service:

4.2.7.1 What does a user license include and in what quantities (number of endpoints, organization according to the range of endpoints, actual use of endpoints and/or amount of conversion requests per time period, etc.)?

4.2.7.1.1 Is there a limit to the amount of queries (DNS Queries) for a specific IP address?

4.2.7.2 How many organizations are included in the user license?

4.2.7.3 The maximum number, if any, of organizations that can be managed under a service license (at the super-management level).

4.2.7.4 Are there pricing levels for different amounts of user licenses? What is the cost estimate for the different levels?

4.2.7.5 If the answer to at least one of the two sections, concerning the operation of the service based on the winners of the Nimbus tender and a data center in the Israeli

region, is negative, what is the cost of implementing the service this way? If this issue is a condition for providing the service to Government ministries in Israel, what is the solution proposed by the respondent?

4.2.7.6 How are development hours priced with reference to dedicated tasks and entire projects?

4.2.7.7 How are Professional Services (PS) hours priced?

4.2.7.8 Is it possible to price a project for interfacing with systems and portals that are external to the service according to the client's requirements and what is the pricing mechanism?

4.2.7.9 Is it possible to price a development project according to the client's requirements and what is the pricing mechanism?

4.2.7.10 Are there other services that are not included in the license, and what are their prices?

4.2.8 Are there documents detailing terms of use of the service and terms of agreement? If so, please attach them.

4.2.9 The respondent may add any additional relevant information related or relevant to these issues.

5 Requested response

The proposals must provide responses that refers to each of the requirements listed in section 4 above, including reference to the following issues:

5.1 For all proposals:

5.1.1 Presentation of capabilities as specified in section 4.

5.1.2 Proposal solutions that are capable of adapting to different organizations - size, classification (unclassified, classified, operational) and open / closed network structure.

5.1.3 Ease of installation, operation and updating.

5.1.4 Proposals or ideas regarding the establishment of the infrastructures, tools or systems required to fulfill the requirements from the proposed system.

5.1.5 In addition to the requested responses as detailed above, respondents may also present existing and future concepts and ideas, as well as additional services that expand the overall response.

6 How to submit clarification questions and respond to this request

6.1 Contact person

The contact person on behalf of the Directorate regarding this request is Sharon Bousidan, phone **072-3388578** email cyber-michrazim@cyber.gov.il

6.2 Clarification questions

6.2.1 Clarification questions regarding this request must be submitted in writing only, no later than the deadline for provision of clarification questions as detailed in the table in section 2.6, to the contact person, by email cyber-michrazim@cyber.gov.il. The supplier must make sure that his questions have reached the contact person at, phone no. **072-3388578**.

6.2.2 The Directorate reserves the right to conduct one or more rounds of clarification questions at its sole discretion.

6.2.3 The clarification questions will be submitted in Hebrew or in English, in the following structure:

Number of the section in the request	Question

6.2.4 Answers to the clarification questions will be forwarded by the Directorate to the applicants, and will also be published on the website of the Government Procurement Administration and the National Cyber Directorate at the addresses specified in section 2.5 above. It is clarified that the clarification answers will be worded in a way that does not reveal the identity of the questioners.

6.3 Submission of a response to the request

6.3.1 The response to the request will be submitted **in Hebrew or English**, and will total up to 50 pages that present the response. In addition to this, appendices and technical specifications can be attached without a scope limitation.

6.3.2 The answer to the request for information must be submitted in a digital copy by the deadline for submitting responses, as detailed in the table in section 2.6

above, via an email box Cyber-Michrazim@cyber.gov.il. Receipt must be confirmed at Tel: .**072-3388578**. In the email's subject line will be: "Preliminary request for information (RFI) on the subject of Protective DNS (PDNS) service ".

6.3.3 The Directorate may postpone the deadline for submitting a response at its sole discretion. A notice of this will be sent to everyone who responded to the request, and will also be published on the websites of the Government Procurement Administration and of the Directorate, at the addresses specified in section 2.5 above. The notice will indicate the new date for submitting the responses.

6.3.4 As part of the response, the respondent will provide the following information:

No.	Requested information	Response
1	Respondent's name	
2	Respondent's address	
3	Phone Number	
5	Name of contact person for respondent	
6	Contact person's phone number	
7	Contact person's email	

7 Examination of the response

7.1 The Directorate reserves the right to contact, as necessary, the respondents with requests for information and clarifications, for presentations and demonstrations, for visits to the client's sites and the sites of those who responded to this request, at the discretion of the Directorate.

7.2 As part of the examination of the responses, the Directorate reserves the right to invite any respondent to present the solution proposed by him to a professional team on his behalf at a location and at a time determined by the Directorate.

7.3 As part of the examination of the responses, the Directorate reserves the right to invite the respondents to hold a pilot that will be up to two months long. It is hereby clarified that the Directorate reserves the right to invite only some of the respondents to hold the aforementioned pilot, at its sole discretion, according to the needs and capabilities of the Directorate and the availability of the respondents.