מענה לשאלות הבהרה ל RFI - בנושא PDNS

No.	Number of the section in the request	Question	Response
1	4.1.2.3	How many organizations roughly would be part of this project? Should the deployment assume and an hirarcial management? Whould this project be implemented in a pahsed approach, based on type of custmers (Municipalities, SMBs, etc.) or geographic/demographic? What are the phases?	The Israel National Cyber Directorate (INCD) has a market management structure that is updated from time to time, and in any case the assimilation (Deployment and Implementation) process depends on many parameters, such as the willingness/readiness of the end customer (the organization). Therefore, it is not possible to commit at this stage to the order and scope of the implementation.
2	4.1.3	What type of information is required for the manual submission/checks of suspicious domains? Should the search be also based on IP's, ASN (Autonomous Networks)? Should it show only a risk score or additional indicators? Should it be only using a GUI or should those investigations be based on API calls	It is necessary to specify which parameters can be checked manually. Also, is it possible to get the risk level score based on the tested parameters. The capability should be specified regarding both GUI and API.
3	4.1.9	Can you provide a rough estimations in regards to the amount of users/DNS queries that will be part of this project (a usuall DNS queries estimation consider ~3500 DNS queries per day/per user)	The Directorate cannot commit to specific quantities at this stage. The different steps/levels possible in the service must be presented. If the proposer wishes to share his experience regarding the average quantities according to the sizes of organizations or other parameters, he may do so.
4	4.1.9.6	Can you please provide the list of SIEM or other data collection/representation systems you are using?	The respondent is requested to specify the systems with which the service can integrate and transfer information, and also please indicate in which protocols/formats this can be done, for example Syslog, CEF.

No.	Number of the section in the request	Question	Response
5	4.2.2.1	What would be the pahses of the project implementation? (critical infrastructure first and additional segments later)? Does this project assumes security/content coverage for consumers as well? If consumers/residentials are included, are you considuring providing the service via an ISP?	The Directorate does not commit at this phase to execution phases, quantities, integration methods, etc.
6	4.2.5	The service is currently implemented for many paying customers in the Israel market, would this project include/cover those customers as well, hence, INCD will provide a PDNS service that will make the current service deployment theu hold redundant?	Not relevant at this point. This phase is only designed for receipt of information from the potential proposers.
7	4.2.6	Is (their) there a requirement for a minimal amount of time for the product in the market and do you require a minimal amount of organizations (WW or Israel) that have implemented and using the product?	Not relevant at this point. This phase is only designed for receipt of information from the potential proposers.
8	4.2.7	Will this project includes SMB's and Residentials?	Not relevant at this point. This phase is only designed for receipt of information from the potential proposers. The respondent is requested to provide details regarding the existing pricing/licensing model for the service for learning purposes.
9	4.2.7.1	Do you require that the respondent will suggest a model that allows flexible (flixible) user growth? Should the licensing be hard counted or do you expect the respondent to provide a 'trust based model'?	Not relevant at this point. This phase is only designed for receipt of information from the potential proposers. The respondent is requested to provide details regarding the existing pricing/licensing model for the service for learning purposes.

No.	Number of the section in the request	Question	Response
10	4.2.7.2	Would you require a limit on the amount of organiozations in the solution, or should it be flexible with no limit and based on the amount of overall users?	The Directorate cannot commit to specific quantities at this stage. The different steps/levels possible in the service must be presented. If the respondent wishes to share his experience regarding the average quantities according to the sizes of organizations or other parameters, he may do so.
11	4.2.7.4	What would be the users coverage? (Critical infrastructures, Government Offices, Municipalities, SMB, Consumers/Residentials)?	The Directorate cannot commit to specific quantities at this stage. The different steps/levels possible in the service must be presented. If the respondent wishes to share his experience regarding the average quantities according to the sizes of organizations or other parameters, he may do so.
12	4.2.7.6	Beyond the product/solution capabilities (Deployment and Implementation), what additional type of development do you inticipate?	Development of customized capabilities that do not exist in the current service.
13	4.2.7.8	In order to provide a suitable/Tangible answer, please provide the list of interfaces, integrations and other systems that the soluition is required to mitigate with.	The respondent is requested to specify which interfaces are supported by the service and their characteristics, for example, transfer of logs and alerts from the service to an external system, etc.
14	4.2.7.9	What type of development is required in this project beside the implementation of the product? Should the vendor be involved in the Go to Market phases (advertisment, Market penetration/adoption, etc.)	The pricing options for different types of development should be specified - whether according to a defined feature, whether according to development/work hours, etc.
15	4.1.20	Can INCD clarify question 4.1.20? We assume this question applies to how the PDNS dns filtering is administered at both the INCD and the “customer” or organizational level below it?	This means: 1. How is multi-tenant management and separation between different organizations using the service carried out? 2. How can a blocking policy be implemented at a high level that will trickle down the rest of the organizations? 3. How is the organization prevented from overriding the overarching policy? 4. How can different

No.	Number of the section in the request	Question	Response
			and individual administrators be assigned to each and every organization?
16	4.1.32	Can INCD clarify question 4.1.32? Does INCD mean the DNS filtering service itself that INCD can control or the manufacturer of the DNS filtering service and what controls they have put in place to secure their system? Can you provide an example of a security feature you would expect on the service?	Please list all existing information security options. It should be added, for all the options, whether the options are enabled by default or whether they are required to be set.
17	4.1.1.1	Can the INCD Clarify why they require the service to run on Nimbus affiliated data centers? The basic principle in PDNS is to provide protection while stopping attacks as far as possible from the victim origin so by this principle having the service on Nimbus fundamentally weakens the INCD ability to protect itself at scale . Best in breed PDNS vendors will use anycast architecture and will not provide this capability on AWS or GCP, for example chosen vendor by CISA for PDNS is not providing this service on AWS government cloud in the US . We do however see value in having at least 2 independent Data centers in Israel for redundancy, data privacy as well as for a doomsday scenario when	The requirement to use Nimbus tender winners is in accordance with the regulation that applies to government ministries in this context. For the purpose of examining the meaning, the respondents are asked to specify whether the service can be offered in this way.

No.	Number of the section in the request	Question	Response
		Israel will be cut off from the world so this service could still run locally and independently .	
18	4.1.1.1	Can the INCD clarify in case of insisting on this point if they have ways to inforce AWS or GCP to host the chosen vendors services ? . As AWS and GCP are competitors of most best in breed PDNS vendors this request is almost impossible to fulfill by the submitter and only will harm the INCD from having the best solution in the market today as used by the US government and others who already implemented PDNS .	The requirement to use Nimbus tender winners is in accordance with the regulation that applies to government ministries in this context.
19		Is it necessary for the offering company to own two datacenters in Israel for redundancy?	This stage it is not about the requirements of the Directorate, but rather a request for information only. th erepondent should specify the implications of maintaining 2 data centers in Israel. Also, it must be clarified whether these are different vendors or the same vendor and whether these are vendors that offer co-location or providers that offer full IaaS capabilities.
20	4.1.1.3	We need clear requirements for data protection, privacy and terms of use for storage or information on Nimbus in order to respond to this question. Can you send a summary of the requirements in English?	In this section a link is attached https://mr.gov.il/ilgstorefront/he/p/4000553566
21	4.1.2.3	We do not fully understand this requirement. The goal is when the system implements a policy for organization XX, can the system send an alert to another superior entity? If so, what is the expected	This stage it is not about the requirements of the Directorate, but rather a request for information only. It must be specified how the multi-tenant model is implemented.

No.	Number of the section in the request	Question	Response
		method for sending this message? Can you explain, using an example, the multi-administrative model described in the RFI?	
22	4.1.2.9	What is the concept of an identity card? It is not clear to us, could you clarify the purpose of this requirement? The service can set different actions such as: no log, log, redirect, block... For each update, this update-defined action can be automatically changed by a UI action or an API trigger action. In the case of feed upload identifiers, regardless of the type of upload method, after uploading in the system via the script, the system can immediately change to log/block.	"Indicatorr" is defined in the terms specified in the RFI document. It must be specified whether after uploading/entering a new indicator into the service, automatic blocking is performed or whether there is only monitoring, and whether an attempt is made to access the indicator by an organization. For example: the indicator is a domain name test.test (we know that this name does not exist). Will the service perform immediate and automatic blocking after uploading/entering or is manual action required, and is it possible after uploading to set up monitoring that will detail who accesses this inicator, but without performing blocking.
23	1.9.5	There is no clear requirement, can you explain this request? Can ?you provide one example	Requirement 4.1.9.5- The meaning is whether when there is an indicator that you want to receive an indication about, but we do not want a superuser to be exposed to its existence and the findings of his monitoring - it is possible to filter so that the information is not received.
24	4.1.9.7	There is no clear requirement, can you explain this request? Can you provide one example? The purpose of this is to set a specific role or group that will have an option to export user log data?	The permission model of the service must be specified.

No.	Number of the section in the request	Question	Response
25	4.1.15	There is no clear requirement, can you explain this request? Can you provide one example? The purpose of this is to have a specific option for cutting off all of Israel's traffic? Could you clarify this?	It must be specified how, in the event of a disconnection from the world or cyber attacks on the gateways to the State of Israel, it will be possible to continue to receive service in the system as well as manage it without exceeding the service standards/levels.
26	4.1.22	There is no clear requirement, can you explain this request? Can ?you provide one example	The permission model of the service must be specified.
27	4.1.27	There is no clear requirement, can you explain this request? Can you share one example of what kind of development or adaptation might be ?required	Development of customized capabilities that do not exist in the current service.
28	4.1.29	There is no clear requirement, can you explain this request? Can ?you provide one example	It must be specified whether the respondentr has a permanent team engaged in Threat Intelligence and Threat Hunting that can provide professional consulting services in the field. Also, does the team regularly engage in research and development of new capabilities for the service and, in addition, can the team carry out research in accordance with the request of the INCD and does it make proactive publications regarding cyber incidents and relevant innovations in the field.
29	4.2	There is no clear requirement, can you explain this request? Can ?you provide one example	An answer must be specified in accordance with the subsections.
30	4.2.2.1	There is no clear requirement, can you explain this request? Can ?you provide one example	Please specify as requested in this section.
31	4.2.4	There is no clear requirement, can you explain this request? Can you provide one example? We sell the service	Please specify as requested in this section.

No.	Number of the section in the request	Question	Response
		according to the number of users/employees in the company.	
32	1.1	Please define the scope of the organisations to be protected, such as: Isreali Goverment and Government organisations Ciritical infrastructure operated for or by government organisations and indicate the number of such organsiations as "tenants" of the solution	The Israel National Cyber Directorate (INCD) has a market management structure that is updated from time to time, and in any case the assimilation (Deployment and Implementation) process depends on many parameters, such as the willingness/readiness of the end customer (the organization). Therefore, it is not possible to commit at this stage to the order and scope of the implementation.
33	1.1	Are there specific networking requirements or arrangements for governmental organisations connecting to the service ?	Architectures that are supported for work with the service must be specified. Reference should be included to organizations that work on-prem only and those that work with a public cloud, including a hybrid cloud.
34	1.1	For the target organisations / end user base, how are the assigned DNS addresses managed today ?	There are several work configurations, for example, the organization uses an internal DNS server that addresses the ISP's DNS server or the internal DNS server calls a DNS Firewall type security component, and from there the request is directed to the ISP's DNS server. The respondent will specify the ways to perform integration with the service.
35	4.1.1	In terms of SaaS and deployment, we understand the items below, is this correct ?: (a) The INCD will be managing the security service as "administrator" (b) The infrastructure will be provided by AWS & GCP What is/are the expected production operational model(s) in terms of managing, monitoring and operation of the Protective DNS platform components ?	The work configurations based on which the service can work must be specified, while referring to the disadvantages and advantages of each configuration.
36	4.1.1.1	Is it important that the PDNS system is to be deployed only on the Nimbus	It must be specified whether the service can work on Nimbus infrastructures and if not, what the consequences are as a result of this

No.	Number of the section in the request	Question	Response
		approved AWS and GCP data centres in Israel ?	(establishment, management, responsibility, information sovereignty, working capabilities disconnected from the world, etc.) while also referring to time and cost aspects.
37	4.1.1.1	Is it important that the PDNS system will be procured to INCD via Nimbus?	It must be specified whether the service can work on Nimbus infrastructures and if not, what the consequences are as a result of this (establishment, management, responsibility, information sovereignty, working capabilities disconnected from the world, etc.) while also referring to time and cost aspects.
38	4.1.1.1	Would you consider a pure cloud based option with servers in another cloud in Israel but potentially using components outside the country for redundancy and some forms of data processing ?	Architectures that are supported for work with the service must be specified. Reference should be included to organizations that work on-prem only and those that work with a public cloud, including a hybrid cloud.
39	4.1.1.1	Can you consider deployment in your own or third party data centres of specific service components for additional resilience ?	It must be specified whether the service can work on Nimbus infrastructures and if not, what the consequences are as a result of this (establishment, management, responsibility, information sovereignty, working capabilities disconnected from the world, etc.) while also referring to time and cost aspects.
40	4.1.2.1	How are end users of the service to be identified and what parameters are available to identify the user ?	The options available within the service must be specified.
41	4.1.2.1	Do you consider an end user of the service to be one network access location (e.g. router or CPE with multiple users behind it) or ultimate end user (e..g. a government employee or their computer) ?	This stage is not about the INCD's requirements, but a request for information only. Details regarding the existing pricing/licensing model for the service should be provided.
42	4.1.2.1	Approximately how many users are in the scope here, in terms: (1) Real end users? (2) End points (e.g. CPE with multiple users behind them) ?	This stage is not about the INCD's requirements, but a request for information only. Details regarding the existing pricing/licensing model for the service should be provided.

No.	Number of the section in the request	Question	Response
43	4.1.2.4	What is the use case for a superuser / master organisation only being able to view specific policy changes or a subset of those policy changes for a tenant organsation ?	At this stage, it must be specified whether there is support for what is detailed in this section in the RFI document and whether there are alternatives in case there is no support.
44	4.1.2.10	Where you ask whether the risk threshold can by changed by the user, do you mean: (1) The ultimate service end user such as an individual government employee ? (2) An administrative user for an enterprise using the service ? (3) An administrative user for the service ?	This means: 1. How is multi-tenant management and separation between different organizations using the service carried out? 2. How can a blocking policy be implemented at a high level that will trickle down the rest of the organizations? 3. How is the organization prevented from overriding the overarching policy? 4. How can different and individual administrators be assigned to each and every organization?
45	4.1.8	File (file) upload and download, is this a capability you would be looking for: (a) Specific subsets of applications or domains based on those domains being somehow suspect ? (b) Specific applications or domains including legitimate domains ? (c) All Internet traffic ?	At this stage, the capabilities built into the service must be specified.
46	4.1.9.3	Do you have specific security or compliance guidelines which determine how long you need to store logs / records for - in which case how long is this period , or of what order of magnitude is this requirement (days. months, years) ?	At this stage, the information storage capabilities and their consequences in terms of pricing aspects, etc., must be specified.
47	4.1.9.6	For data export, do you have a set of preferred target system(s) ?	The respondent is asked to specify the systems with which the service can perform integration and transfer information, and it must also be specified in which protocols/formats this can be performed, for example Syslog, CEF.

No.	Number of the section in the request	Question	Response
48	4.1.14	Do you have a definition of "username" in this context - real name (Bob Smith), login name (bob@example.com) , machine name (PC1234), other ?	It is necessary to specify whether each of the options is supported by the service, including supporting several languages and specify the languages and formats accordingly, as well as whether there are additional supported options.
49	4.1.33	Is there a specific target for this basic free service - specific enterprises, Small Medium Business, residential citizens ?	It should be specified whether such an option is generally offered by the respondent and if so, what is the respondent's policy in this regard.
50	4.1.1.3	We note the need to review documents from the Nimbus project to understand the security, privacy, and other terms of use expectations and requirements that would apply to this PDNS service. However, a couple of the documents do not load. Would it be possible for NCD to confirm the precise documents that should be reviewed to get a good idea of these requirements, please?	In this section, a link is attached https://mr.gov.il/ilgstorefront/he/p/4000553566
51	1	Requesting a general clarification of the intent of the RFI, whether the request is for a managed service to be purchased by the National Cyber Directorate and will be distributed to the various entities supervised by the National Cyber Directorate, or is the intention that any entity under the Directorate can/is obligated to purchase the service independently from the manufacturer and the Directorate will be able to receive the logs of each?	This stage is about receiving information only.
52	4.1.1	Is the requested solution SaaS? Is it mandatory or is	It is necessary to specify what the operating options are included in the service today.

No.	Number of the section in the request	Question	Response
		it possible to propose a solutions?	
53	4.1.1.1	Is Nimbus a mandatory condition or is the ability to run the service over AWS\GCP infrastructure sufficient? Are both required or only one of them?	At this stage, the Directorate does not present requirements, this is only a request for information.
54	4.1.2.1+2	Please clarify what is meant, in this section, by a certain user and other users?	This means: 1. How is multi-tenant management and separation between different organizations using the service carried out? 2. How can a blocking policy be implemented at a high level that will trickle down the rest of the organizations? 3. How is the organization prevented from overriding the overarching policy? 4. How can different and individual administrators be assigned to each and every organization?
55	4.1.2.3+4	What are the connections between the organization and the appointed organization?	Several management configurations will be possible, for example, the INCD will define a blocking or monitoring policy that will permeate groups of organizations and/or organizations that consume the service. Another example, the INCD will define a policy that will trickle down and then a regulator or other authorized entity will be able to define a stricter policy, which will apply to organizations for which it is responsible. It is important to note that these are illustrative examples only, and the possible work configurations within the offered service must be specified.