Centrum Systemów Informacyjnych Ochrony Zdrowia

Znak sprawy: WZP.510.1.2019 **Załącznik nr 1 do Protokołu**

Pytania i odpowiedzi
do Dialogu technicznego dotyczącego „Usług chmurowych dla Centrum Systemów Informacyjnych Ochrony Zdrowia"

Lp.	Treść Pytania	Treść odpowiedzi
1.	Czy wymagania dotyczące dostępu użytkowników opisane w punkcie 1 strona 4 dotyczą portalu do zarządzania chmurą, czy również obowiązują w systemach operacyjnych i innych komponentach działających w chmurze?	Postawione wymagania dotyczą platformy zarządzania usługą. Wymaganie ma również zastosowanie w przypadku usług świadczonych na zasadach PaaS.
2.	Czyim zadaniem będzie aktualizacja systemów operacyjnych, bazodanowych i innych w trakcie użytkowania chmury? To zadanie administratorów CSIOZ czy administratorów operatora chmury? Jeżeli aktualizacja leży po stronie administratorów operatora chmury, muszą mieć oni założone konta i stworzony dostęp z odpowiednimi uprawnieniami do systemów hostowanych w chmurze – nie wiemy, jak ma się to do polityki bezpieczeństwa CSIOZ. 4. Dotyczy punktu 2 b) strona 5 i punktu 2 d) 5) strona 7	W przypadku usługi IaaS CSIOZ za aktualizację software odpowiada CSIOZ. Dla usługi PaaS za aktualizację odpowiada Wykonawca, przy czym każda aktualizacja mogąca wpłynąć na stabilność systemu musi być konsultowana z CSIOZ. W przypadku zarówno IaaS, jak i PaaS oczekujemy aktualizacji na poziomie firmware.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

3.	Jeżeli systemy operacyjne stracą wsparcie producenta, kto jest odpowiedzialny i ponosi koszt zakupu potrzebnych licencji na nowy system operacyjny/bazodanowy/inny (o ile to konieczne) oraz migrację danych, przeprowadzenie testów, dokumentację związaną z migracją na nowy system operacyjny? 4. Dotyczy punktu 2 b) strona 5 i punktu 2 d) 5) strona 7	W przypadku IaaS za instalowane systemy odpowiada CSIOZ, dla PaaS to Wykonawca jest zobowiązany za przestawienie Zamawiającemu informacji o wygasających licencjach lub wsparciu. Opisywane systemy operacyjne to systemy, których utrzymanie leży po stronie usługodawcy - w przypadku IAAS wszystko "poniżej" wirtualizatora a w przypadku PAAS wszystko poniżej Dockera - zatem jedynie systemy operacyjne będące "platformą" świadczenia usług.
4.	W jaki sposób w środowisku chmurowym miałby funkcjonować NAC? To są technologie dotyczące bezpieczeństwa end-point'ów. Prosimy o przykłady wykorzystania NAC w chmurze. Czy nie ma tu pomyłki z np. mikrosegmentacją?8. Dotyczy punktu 2 e) 1) strona 7	Mechanizmy klasy NAC nie oznaczają urządzeń ale dostępność usług równoważnych z NAC
5.	Jakie technologie są obecnie używanie do centralnego zarządzania uwierzytelnianiem, czy jest to tylko Active Directory? Prosimy o zarys architektury związanej z uwierzytelnianiem, Active Directory.	Na chwilę obecną do centralnego zarządzania uwierzytelnianiem służy Active Directory. W przyszłości planuje się wdrożenie systemu klasy IAM/IDM.
6.	Dotyczy punktu VI podpunkt 2 strona 35. W podpunkcie opisana jest konieczność zapewnienia wsparcia dla systemów działających w klastrach rozciągniętych między ośrodkami. Czy to oznacza konieczność rozciągania geograficznego sieciowej warstwy drugiej (L2), aka "failure domain"? Czy komplikowanie rozwiązania, a co za tym idzie, podwyższenie ryzyka awarii jest konieczne?	CSIOZ wymaga możliwość skonfigurowania klastra geograficznego pomiędzy ośrodkami przetwarzania danych w warstwie L2.
7.	Jaki ruch do/z Internetu generują (lub mogą generować) poszczególne platformy?	Organizator dialogu wymaga łącza do sieci Internet w przepływności minimum 700 Mbit/s.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

8.	Dotyczy punktu VIII podpunkt 2 c) strona 42. Czy minimalna przepustowość połączenia dedykowanego na potrzeby platformy 40Gbps symetrycznie dotyczy łączności między centrami danych czy lokalnej w ramach środowiska w jednym centrum?	Przepustowość pomiędzy centrami danych powinna wynosić min. 40Gbps w podziale na 4 trakty.
9.	Dotyczy punktu VIII podpunkt 2 c) strona 42. Jakie są wymogi, które wymuszają akurat przepustowość 40Gbps?	Organizator dialogu wykorzystuje obecnie podobne zaosby w celu synchronizacji baz danych. Podane parametry dotyczą połączenia ośrodków CPD w podziale na 4 trakty.
10.	Do jakiego poziomu ma być zaangażowany operator chmury w przypadku występowania problemów z systemem Poltransplant, Ekrew, ZSMOPL, Platforma P1? Prosimy o przykłady, podział obowiązków między operatorem chmury i administratorami CSIOZ, również w odniesieniu do polityki bezpieczeństwa CSIOZ.	W przypadku udostępnienia infrastruktury typu Iaas Operator Chmury odpowiada za warstwę sprzętową oraz wirtualizator. W przypadku udostepnienia infrastruktury typu PaaS oczekujemy od Operatora odpowiedzialności za wszystko, co znajduje się poniżej kontenera. W obu przypadkach po stronie operatora chmury są także warunki bezpieczeństwa sieci opisane w materiale pomocniczym.
11.	Prosimy o podanie lokalizacji Data Center biorących obecnie udział w kolokacji/hostingu.	Warszawa, ul. Dubois, Warszawa, ul. Grochowska, Warszawa, ul. Konstruktorska
12.	Czy opisywane wymogi dotyczące bezprzerwowej pracy należy traktować dosłownie i proponować/projektować pod tym kątem rozwiązania?	Tak. Chodzi o bezprzerwową pracę systemów. CSIOZ chciałby poznać jakie są możliwości techniczne i kosztowe takiego rozwiązania.
13.	Co dokładnie oznacza to sformułowanie? Czy panel obsługi chmury ma być minimum w 2 wersjach językowych: Polski oraz Angielski i to wystarczy?	Instrukcje obsługi dostarczone jako dokumentacja - dwie wersje językowe: polska i angielska. Język interfejsu - co najmniej wersja angielska.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

14.	Dotyczy punktu 2 strona 5. W akapicie dotyczącym Redundancji, zapisy sugerują, że CSIOZ oczekuje 100% dostępności. Czy jest możliwa zmiana zapisów odnosząca się np. do SLA? Mimo zapewnienia redundancji, klient może czasem odczuć skutki awarii i obecny zapis jest nierealny do spełnienia w odniesieniu do rzeczywiście funkcjonujących systemów.	Tak. SLA 99,98%. Oczekujemy także oszacowania wpływu parametrów dostępności na cenę rozwiązania.
15.	Czy dla obecnych systemów CSIOZ ma wykupione wsparcie np. Premier Support w Microsoft? Prośba o listę takich wykupionych supportów. Czy w trakcie korzystania z chmury będzie można korzystać w wykupionego wsparcia przez CSIOZ? Co w przyszłości ze wsparciem po jego zakończeniu - czy CSIOZ wykupi wsparcie na kolejne lata, czy to zadanie operatora chmury?4. Dotyczy punktu 2 b) strona 5 i punktu 2 d) 5) strona 7	Należy założyć, że CSIOZ nie posiada kontraktów serwisowych.
16.	Czym jest podyktowana konieczność wykorzystania jedynie systemów operacyjnych posiadających wsparcie producenta systemu? W przypadku systemów linuksowych następuje ograniczenie do platform np. RHEL, Ubuntu. 4. Dotyczy punktu 2 b) strona 5 i punktu 2 d) 5) strona 7	Konieczność dotyczy jedynie systemów operacyjnych, których utrzymanie leży po stronie operatora usługi chmurowej i podyktowane jest obawą o właściwy poziom świadczenia usług.
17.	Kto ma być odpowiedzialny za opracowanie i prowadzenie takich testów? Zespół CSIOZ czy operator chmury? 5. Dotyczy puntu 2 b) 3) strona 6	Organizator oczekuje propozycji testów związanych z procedurą migracji.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

18.	Czy już są prowadzone takie testy i można je wykorzystać w przyszłości? Kto obecnie wykonuje takie testy, ile one kosztują, czy CSIOZ jest zadowolone z prowadzonych testów i można kontynuować współpracę z obecnym wykonawcą testów? 5. Dotyczy puntu 2 b) 3) strona 6	Na potrzeby dialogu należy przyjąć, iż takie testy nie są prowadzone.
19.	Czy znane są pracochłonności i koszty przeprowadzenia testów, aby można ująć je w kosztorysie? 5. Dotyczy puntu 2 b) 3) strona 6	Przedstawione kosztorysy powinny dotyczyć jedynie kosztów po stronie operatora bez uwzględniania kosztów innych jednostek takich jak CSIOZ lub MZ.
20.	O jaką platformę chodzi? Dotyczy punktu 7 podpunkt 5 strona 9	Chodzi o platformy serwerowe X86 - 64
21.	Prosimy o sprecyzowanie listy narzędzi wspomagających migrację. Bez dogłębnej znajomości systemów CSIOZ trudno na tym etapie przewidzieć narzędzia i obliczyć koszt ich zakupu/użycia.	Organizator dialogu oczekuje propozycji od dostawcy usług w tym zakresie.
22.	W wymaganiach na chmurę IaaS, w punkcie 11 f. na stronie 36 podana jest informacja, iż platforma wirtualizacyjna powinna umożliwiać powołanie dowolnej ilości maszyn wirtualnych bez ograniczeń zasobów. Takiego wymagania nie można spełnić, platformy wirtualizacji mają swoje ograniczenia, operator chmury też ma ograniczone zasoby. Czy można zastąpić ten zapis innym, który jest realny do spełnienia?	TAK. Organizator oczekuje, iż parametry platformy wirtualizacji dają możliwości nie mniejsze niż opisana w materiale skala wzrostu potrzeb tzn. 20% rocznie przez okres nie krótszy niż 3 lata. Wzrost liczony zawsze w odniesieniu do zasobu roku poprzedniego.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

23.	Dotyczy systemu ZSMOPL.Jakimi kompetencjami i zasobami ludzkimi i w jakim czasie ma dysponować operator chmury, aby wykonać migrację. Informacje są niezbędne do opracowania kosztorysu, a operator chmury bez znajomości systemu ZSMOPL nie jest w stanie wykonać szacunków.	Organizator oczekuje doświadczenia w tym zakresie od uczestników dialogu. Nie mając kompetencji dotyczących procesów migracji baz danych oczekujemy propozycji uczestników zarówno dotyczących składu (kompetencji) zespołu oraz samych procedur migracji.
24.	Dotyczy systemu ZSMOPL.Jaki ma być podział prac podczas migracji między CSIOZ, a dostawcą chmury? Jaki jest szacowany czas migracji, testów? Jakie systemy, bazy wykorzystują systemy migrowane (nazwy, wersje)? Potrzebna jest dokładna architektura systemu.	Oczekujemy propozycji przeprowadzenia całego procesu migracji przez operatora. Udział CSIOZ w procesie będzie miał charakter nadzoru zasad bezpieczeństwa oraz koordynacji Pracownicy CSIOZ będą także przeprowadzali testy funkcjonalne migrowanych systemów po ich przeniesieniu do chmury.
25.	Dotyczy systemu ZSMOPL.Kto ma zaprojektować i wykonać testy kontroli dostępu, testy integracyjne? Prośba o oszacowanie zasobów ludzkich po stronie operatora chmury i czasu na wykonanie testów.	Organizator dialogu oczekuje propozycji w tym zakresie od uczestników dialogu.
26.	Czy planowana jest znacząca rozbudowa systemów Poltransplant, Ekrew, ZSMOPL, Platforma P1, co może wpływać na opisywaną ilość: CPU, RAM, przestrzeni dyskowej? Jeżeli tak, czy są szacunki jak zwiększą/zmienią się zapotrzebowanie na CPU, RAM, przestrzeń dyskową w perspektywie roku, trzech lat, pięciu lat?	Tak. 20% rocznie licząc rok do roku.
27.	Jakie są możliwości CSIOZ w zakresie przeniesienia/migracji licencji na systemy operacyjne i inne komponenty do chmury operatora?	W usłudze IaaS CSIOZ zamierza wykorzystać własne systemy operacyjne w maszynach wirtualnych, w usłudze PaaS systemy operacyjne są po stronie dostawcy usług.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

28.	W opisie wymagań dotyczących chmury IaaS, w podpunkcie 11 g) na stronie 36 podana jest informacja związana z dostarczeniem usług relacyjnej bazy danych w modelu IaaS. Prosimy o sprecyzowanie do jakiego poziomu mają sięgać kompetencje operatora chmury? Biorąc pod uwagę np. problemy wydajnościowe w działaniu systemu/aplikacji, jakie elementy związane z relacyjną bazą danych w modelu IaaS ma diagnozować operator chmury, a jakie administratorzy CSIOZ?	W przekazanej dokumentacji pojawił się błąd. W architektury IaaS Organizator Dialogu dostarcza licencje bazy danych
29.	W przypadku Platformy P1 łączna pojemność macierzy w każdym CPD to 124TB netto. Prosimy o uszczegółowienie: 124TB per CPD? Czy 124TB to pojemność dla całego środowiska z redundancją włącznie?	Na potrzeby dialogu należy przyjąć łączną pojemność dla całego środowiska 124TB danych, w każdym z ośrodków po 62 TB
30.	Jakiego producenta posiadają Państwo macierze?	Organizator dialogu nie ma preferencji w tym zakresie i oczekuje propozycji rozwiązań w oparciu o zasoby operatora usług chmurowych.
31.	Jakie są średnie czasy opóźnień komunikacji IP pomiędzy ośrodkami?	do 5 ms
32.	Jakich narzędzi używają Państwo do zarządzania CD/CI/CT?	Aktualnie używamy Jenkins, TeamCity, gitLab CI, Bamboo, Chef, Puppet; jednak nie ograniczamy się tylko do tych narzędzi w przyszłości

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

33.	Czy Zamawiający będzie wymagał by wykonawca był wyłącznym właścicielem budynków, terenów CPD oraz infrastruktury udostępnionej w ramach projektu?	Rozważany jest wymóg prawa użytkowanie CPD przez czas nie krótszy niż czas wykonywania usługi. Forma prawna inna niż własność notarialna jest dopuszczalna o ile nie narusza to opisanych w materiale wymagań bezpieczeństwa.
34.	Czy siedziba wykonawcy musi znajdowad się na terenie RP?	Wg opisanych warunków na terenie Polski muszą znajdować się CPD.
35.	Czy budynki CPD mają byd wykorzystywane wyłącznie jako Centra Przetwarzania Danych?	Nie
36.	Czy Zamawiający przewiduje na etapie postępowania wizytę on-site w Data Centerwykonawcy w celu weryfikacji zaoferowanych rozwiązao?	Tak. W trakcie postępowania przewidywany jest audyt CPD , którego celem będzie weryfikacja spełnienia warunku zgodności z wymaganiami Tier 3 lub normy EN 50600
37.	Czy ośrodki przetwarzania danych mają byd zgodne z wymaganiami ANSI/TIA 942 oraz TIER 3, to jest spełniad wymagania przedstawione w tabeli (tabela stanowi załącznik do niniejszych pytao)?	Organizator dialogu oczekuje, że CPD spełnia wymagania tych norm i certyfikacji jednak nie wymaga przedstawienia wymienionych certyfikatów. Przewidywana forma weryfikacji oświadczeń w tym zakresie to audyt i sprawdzenie spełnienia wymagań zgodnie z listą warunków zamieszczonych w dokumentacji ew. postępowania.
38.	Czy odległośd między dwoma CPD powinna zapewnid możliwośd replikacji synchronicznej, czyli odległośd nie większa niż 50 kilometrów?	Organizator nie określa odległości pomiędzy CPD a jedynie opóźnienie jako nie większe niż 5 ms.
39.	Czy wykonawca ma przedstawid referencje w zakresie migracji środowiskinformatycznych? Ile referencji ma przedstawid oferent i na jaką kwotę?	Na etapie dialogu technicznego nie są wymagane.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

40.	Czy wykonawca ma zaoferować usługę Security Operations Center, która obejmieobsługą wszystkie systemy?	Nie, przedmiotem Dialogu nie jest zakup usługi Security Operations Center. Na usługę SOC może być przeprowadzone niezależne postępowanie
41.	Czy wykonawca musi mied w swojej strukturze organizacyjnej wydzielony pionbezpieczeostwa oraz incydent management?	Wykonawca musi spełniać wymogi ustawy o krajowym systemie cyberbezpieczeństwa w zakresie wymaganym od dostawców usług cyfrowych
42.	Czy Zamawiający przewiduje sposób rozliczania pay-as-you-use? W szczególności czy Zamawiający planuje zastosowad standard powszechnie stosowany w zamówieniach publicznych? Dla przykładu przedstawiamy linki do kilku wybranych postępowao publicznych, gdzie zastosowano powyższy standard (linki do postępowao stanowią załącznik do niniejszych pytao).	Organizator dialogu oczekuje propozycji możliwych form rozliczania usług od operatorów. Wymieniona forma rozliczania jest jedną z możliwych opcji rozliczeń.
43.	Ilu użytkowników podstawowych i uprzywilejowanych będzie zarządzało środowiskiem?	Będzie to od 3-10 osób, w przypadku uwzględnienia administratorów IT liczba ta może wzrosnąć do 30 osób.
44.	Jakie systemy operacyjne są wykorzystywane w każdym z systemów (komercyjne i typu Open Source)	Windows, Linux RH, Linux SUSE, Linux CenTos,
45.	Dlaczego Zamawiający zakłada wykorzystanie ciemnych włókien dla projektów E-krew i Poltransplant (strony 30 i 33 „Materiałów pomocniczych ...")?	Zamawiający chciałby osiągnąć jak najniższe opóźnienia w przesyłaniu danych pomiędzy ośrodkami (maksymalnie 5 ms). Jesteśmy otwarci na inne rozwiązania techniczne, które zapewnią powyższe założenie.
46.	Czy używana jest lub będzie w przyszłości replikacja pomiędzy macierzami w różnych ośrodkach?	Na potrzeby dialogu proszę przyjąć że TAK.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

47.	Prosimy o informację na temat serwera aplikacyjnego ZSMOPL wymienionego na stronie 39. Czy to silnik aplikacyjny to IBM WebSphere?	Silnikiem aplikacyjnym systemu ZSMOPL jest ServiceMix
48.	Czy opisane w punkcie IX na stronie 44 parametry backupu: backup 1TB wykonywany do 0,5h, odtwarzanie 1TB w ciągu 1h są wartościami obowiązującymi operatora chmury? Oznacza to transfery z poziomie około 2,3Gb/s.	Na potrzeby dialogu należy przyjąć, że: backup 1TB wykonywany do 1h, odtwarzanie 1TB w ciągu 2h.
49.	Jaki jest tryb synchronizacji danych pomiędzy ośrodkami?	Na potrzeby dialogu należy przyjąć asynchroniczny tryb replikacji pomiędzy ośrodkami. Synchroniczny tryb można przedstawić w prezentacji jako opcję.
50.	Czy wykonawca musi mieć w swojej strukturze organizacyjnej wydzielony pion bezpieczeństwa oraz incydent management?	Wykonawca musi spełniać wymogi ustawy o krajowym systemie cyberbezpieczeństwa w zakresie wymaganym od dostawców usług cyfrowych
51.	Czy Zamawiający przewiduje sposób rozliczania pay-as-you-use? W szczególności czy Zamawiający planuje zastosowad standard powszechnie stosowany w zamówieniach publicznych? Dla przykładu przedstawiamy linki do kilku wybranych postępowao publicznych, gdzie zastosowano powyższy standard (linki do postępowao stanowią załącznik do niniejszych pytao).	Organizator dialogu oczekuje propozycji możliwych form rozliczania usług od operatorów. Wymieniona forma rozliczania jest jedną z możliwych opcji rozliczeń.
52.	Jakie systemy operacyjne są wykorzystywane w każdym z systemów (komercyjne i typu Open Source)	Windows, Linux RH, Linux SUSE, Linux CenTos,
53.	Prosimy o określenie dla każdego z systemów (E-krew, Poltransplant, ZSMOPL, P1) następujących parametrów: a)Minimalna oczekiwana	a) Całkowita przepustowość łącza symetrycznego do/z sieci Internet to 700Mbit/s

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

	przepustowośd z i do sieci Internet z każdego z ośrodków CPD; b) Minimalnej przepustowości i szacowana ilośd tuneli Site-to-Site (do innych systemów z którymi będą się komunikowały „hostowane" systemy); c) Określenie ilości i rodzaju komercyjnych systemów operacyjnych i baz danych; d) Oczekiwanych wydajności systemów dyskowych wraz z ich wolumenem.	b) Szacuje się, że łączna ilośd tuneli site-to-site nie będzie większa niż 10.
		c) Systemy operacyjne: 3 (Windows Server, Redhat, SuSe), Bazy danych: 5 (Percona xtraDB, DB2, Oracle, EDB, MsSQL)
		d) Na potrzeby dialogu należy przyjąd maksymalną wydajnośd dysków na poziomie
		- 150k IOPS (65% read, 35% write) - 300TB.
		- 100k IOPS (jw.) - 600TB.
		- 50k IOPS (jw). - 300TB.
		Na potrzeby dialogu należy przyjąd wolumen zasobów dyskowych: 1,2 PB.
54.	Dlaczego Zamawiający zakłada wykorzystanie ciemnych włókien dla projektów E-krew i Poltransplant (strony 30 i 33 „Materiałów pomocniczych ...")?	Zamawiający chciałby osiągnąd jak najniższe opóźnienia w przesyłaniu danych pomiędzy ośrodkami (maksymalnie 2 ms). Jesteśmy otwarci na inne rozwiązania techniczne, które zapewnią powyższe założenie.
55.	Jak synchronizowane są aktualnie dane pomiędzy ośrodkami?	Aktualnie replikacja danych odbywa się za pomocą mechanizmów bazodanowych. Nie wyklucza się w przyszłości wykorzystania replikacji macierzowej.
56.	Czy używana jest lub będzie w przyszłości replikacja pomiędzy macierzami w różnych ośrodkach?	Na potrzeby dialogu proszę przyjąd że TAK.
57.	Jakich mechanizmów tworzenia kopii zapasowych używa obecnie Zamawiający? Jakie używane jest oprogramowanie backupowe?	Aktualnie wykorzystywane jest oprogramowanie Commvault, DataProtector, TSM Spectrum Protect.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

58.	W związku z wymaganiem na ośrodki równorzędne pracujące w trybie Active-Active, czy dopuszczana jest możliwość trzeciego ośrodka poza granicami Polski na terenie UE w roli rozstrzygania (Quorum), czyli bez przetwarzania danych klienta?	Tak.
59.	Czy poniższe kryteria będą brane pod uwagę w ocenie proponowanych rozwiązań: a. opóźnienie w połączeniu z i między ośrodkami danych, b. SLA dla zasobów w ośrodkach danych, c. SLA dla systemu połączenia z ośrodkami danych?	Na potrzeby dialogu technicznego należy przyjąć SLA=99,98 dla wszystkich zasobów.
60.	Czy komunikacja pomiędzy systemami i/lub użytkownikami jest dozwolona przez Internet poprzez kanały szyfrowane?	Komunikacja administratorów do paneli konfiguracyjnych powinna być szyfrowana. Dozwolona jest komunikację przez Internet.
61.	Czy w zakresie projektowym zakładane jest przepisanie aplikacji – czy tylko zbudowanie środowiska chmurowego?	NIE
62.	Czy chmura ma być całkowicie prywatna – czy jednak może korzystać w pewnym zakresie z zasobów chmury publicznej, obecnej w Polsce?	Tak, ale należy uwzględnić możliwość chmury hybrydowej tworzonej tymczasowo na zasobach podmiotów trzecich.
63.	Czy w rozdziale VI, punkcie 11-g model relacyjnej bazy danych nie powinien być w modelu PaaS zamiast IaaS?	Tak, powinno być PaaS.
64.	Czy CSIOZ rozważa zastąpienie chmury prywatnej chmurą publiczną?	Na potrzeby dialogu technicznego należy założyć że NIE.
65.	Opis standardów wymiany danych przy założeniach technologicznych projektu E-krew jest bardzo ogólny. Czy mogę możliwym jest wskazanie konkretnych standardów?	Standardy komunikacyjne między komponentami, serwerami poszczególnych systemów PaaS, są w trakcie ustalania
66.	Jak daleko mogą być oddalone od siebie ośrodki danych?	Tak aby łączne opóźnienie nie przekroczyło 5 ms

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

67.	Nawiązanie do wymogów technologicznych projektu Poltransplant. Czy rozważane są inne sytemy operacyjne niż CentOS?	TAK, możliwe są inne systemy Linux.
68.	Czy oprócz skalowania wertykalnego zleceniodawca zamierza również przeprowadzać skalowanie horyzontalne?	Organizator Dialogu oczekuje propozycji w tym zakresie.
69.	Nawiązując do rozdziału VI pkt. 10. Jest tu określenie chmury publicznej – w naszej ocenie jest niespójne względem wymogów do innych aplikacji. Czy chodzi o chmurę publiczną czy po prostu publiczne zasoby, które byłyby dostępne dla współdzielonych systemów?	Chodzi o możliwość wykorzystania usług dostępnych w chmurze publicznej przez systemy uruchomione w chmurze CSIOZ. Medium komunikacyjnym w takim przypadku byłoby łącze do chmury publicznej.
70.	Czy rozwiązanie obejmuje całkowicie chmurę prywatną – czy jednak środowisko może korzystać z zasobów, w pewnym zakresie, z chmury publicznej?	Dopuszczamy rozwiązania hybrydowe pod warunkiem spełnienia wymagań bezpieczeństwa.
71.	Czy jako cel zakresu dialogu technicznego należy przyjąć: migrację posiadanych i planowanych przez ODT-CSIOZ systemów do lokalizacji Chmury Publicznej (CHPu)?	NIE
72.	Jaki model płatności przewiduje Organizator Dialogu Technicznego (ODT-CSIOZ)? Za zużyte zasoby, czy za zarezerwowane zasoby?	Organizator Dialogu oczekuje propozycji w tym zakresie ze strony uczestników dialogu
73.	Czy ODT-CSIOZ oczekuje utworzenia dwóch środowisk Chmury Prywatnej (CHPr) oraz Publicznej (CHPu) w ramach każdego z ośrodków przetwarzania danych (CPD). Czy jest znany podział systemów i elementów systemów które byłyby przynależne do odpowiednich chmur?	Organizator Dialogu wymaga dwóch CPD ze względu na określoną w materiale politykę bezpieczeństwa, dostępności i wymóg bezprzerwowej pracy aplikacji i baz danych. Organizator oczekuje propozycji rozwiązań w zakresie wykorzystania 2 CPD - replikacja backup itd. Rozmieszczenie aplikacji w dwóch CPD jest opcją do rozważenia.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

74.	Czy dostawca rozwiązania (INT) ma zrealizować integracje z Krajowym Węzłem (KW)?	Integracja z Węzłem Krajowym będzie odbywała się na poziomie aplikacji dostarczanych przez CSIOZ.
75.	Czy INT w ramach zakresu integracji ma dokonać ubezpieczenia OC w tym obszarze?	INT musi podjąć w tym zakresie decyzję samodzielnie. Na potrzeby dialogu technicznego można podać dwa warianty kosztorysowe pokazujące wpływ OC na wartość całego rozwiązania
76.	Czy ODT-CSIOZ jest już usługobiorcą KW (ePUAP)?	W zakresie przedstawionych w materiale systemów należy przyjąć że TAK.
77.	Czy ODT-CSIOZ w modelu docelowym chce by CHPr było realizowane w oparciu o posiadane przez INT kontrolery i orkiestratory udstępniane także innym podmiotom, czy też środowisko ma być wydzielone także w tym obszarze?	NIE.
78.	Czy wymagane SLA jest liczone rocznie czy miesięcznie?	Rocznie
79.	W związku z danymi wskazującymi na potencjalnie duży udział wirtualizacji opartej na VM Ware prosimy o informacje, czy ODT-CSIOZ bierze pod uwagę rezygnację z tej platformy? Czy też, zakupione licencje są w tzw. Okresie trwałości projektu dofinansowanego co implikuje dalsze ich wykorzystanie?	Środowisko VMWare nie jest wymaganym środowiskiem wirtualizacji a jedynie opcjonalnym.
80.	Czy w obecnej chwili ODT-CSIOZ wykorzystuje kanał komunikacji z innymi podmiotami poprzez WAN lub jakiekolwiek łącza dzierżawione czy też realizuje dostęp przez sieć Internet z szyfrowaniem?	Tak, wykorzystywane są połączenia poprzez łącza dzierżawione oraz Internet z szyfrowaniem.
81.	Jaki ODT-CSIOZ wykorzystuje orkiestrator dla technologii Doker (Openshift, Kubernetess)?	Kubernetes

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

82.	Jak wygląda procedura wykorzystania mechanizmu CI? (Continuous Integration)).	CSIOZ posiada środowisko CI w skład którego wchodzi Jenkins, Artifactory, Bitbucket, Sonarqube. Developerzy gromadzą kod na bitbucket. Aplikacje są budowane poprzez zastosowanie tzw. pipeline na Jenkinsie. Budowanie aplikacji oprócz kompilacji kodu posiada kroki automatycznych testów, pobierania bibliotek z Artifactory, testy kodu w oparciu o Sonarqube. W zależności od projektu, skompilowany obiekt może być automatycznie instalowany na środowiskach P1.
83.	Czy poza wymienionymi silnikami Bazy Danych MySQL/PostgreSQL w systemach wykorzystywane są inne?	tak wykorzystujemy DB2, Percona, Oracle, MsSQL, jednak prosimy o informacje które z silników są wspierane w modelu PaaS przez poszczególnych dostawców
84.	Czy silnik bazy danych MySQL jest w wersji freeware?	Nie
85.	Czy obecnie wykorzystywane są mechanizmy szyfrowania realizowane na poziomie systemów?	Tak, takie wymogi nakłada m.in. rozporządzenie o ochronie danych osobowych
86.	Czy wymaganiem ODT-CSIOZ jest dostarczenie Network Operation Center czy Operation Center?	Nie ma takiego wymagania
87.	Do jakich celów mają być stosowane ciemne włókna? (jakie usługi chcecie Państwo zrealizować na dedykowanych włóknach)	Do połączeń pomiędzy CPD - Organizator dopuszcza jednak łącza na zasobach obcych pod warunkiem nie powstawania opóźnień większych niż 5 ms

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

88.	Czy ODT-CSIOZ jest obecnie właścicielem własnych par włókien lub posiada umowę dzierżawy takowych?	Obecnie ODT-CSIOZ korzysta z włókien w ramach umowy na kolokację pomiędzy ośrodkami danych. Dodatkowo w ramach umowy z operatorem telekomunikacyjnym CSIOZ korzysta z dzierżawionych włókien pomiędzy swoją siedzibą a ośrodkami przetwarzania danych.
89.	Czy wszystkie systemy mają od dnia zero przekazywać dane do SOC CSIOZ (objętego oddzielnym postępowaniem)?	Nie, systemy mają mieć możliwość współpracy z SIEM CSIOZ i będzie to wdrażane osobnym harmonogramem.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

90.	Dodatkowe wymagania	W przypadku wyposażania infrastruktury teleinformatycznej środowiska chmurowego w rozwiązania klasy IPS/IDS, NGF, WAF, DLP (pkt. 5 podpunkt 3) oczekujemy zaoferowania rozwiązań sklasyfikowanych w grupie wiodących (Leaders) bądź rokujących (Challengers) producentów wedle klasyfikacji firmy Gartner rok bieżący i poprzedni. Dopuszczamy zarówno rozwiązania komercyjne, jaki i opensource pod warunkiem spełnienia naszych oczekiwań, jak i posiadania wsparcia producenta/suportu. Podstawowe założenia architektury bezpieczeństwa opieramy na wymaganiu, że zaproponowane rozwiązanie powinno uwzględniać fakt iż przestrzenie dyskowe, RAM, CPU dedykowane są wyłącznie dla CSIOZ. Dopuszczamy możliwość współdzielenia RAM, CPU, infrastruktury sieciowej wraz z urządzeniami bezpieczeństwa. W takim przypadku wymagane jest przeprowadzenie przez uczestnika dialogu analizy ryzyka opisującej możliwe zagrożenia, sposoby postępowania z nimi, aby bezpieczeństwo systemów IT CSIOZ, jak i przetwarzanych w nich danych było zagwarantowane na akceptowalnym przez nas poziomie. Analiza musi uwzględnić możliwe zagrożenia na warstwie hardware, software, jak i network. Dla przykładu, podatność w systemie innego klienta z którym będzie współdzielona infrastruktura może umożliwiać wydostanie się atakującego poza środowisko wirtualne tego klienta i umożliwić dostęp do zasobów CSIOZ po przejęciu maszyny fizycznej - w takim przypadku należy udzielić odpowiedzi jakie zabezpieczenia zostaną wdrożone aby nie dopuścić do takiego wariantu. Ponadto w przypadku współdzielenia środowisk oczekujemy wsparcia w przypadku incydentów bezpieczeństwa ze strony uczestnika dialogu wraz z zabezpieczeniem materiałów dowodowych

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

		znajdujących się we współdzielonej przestrzeni. Ze względu na istotność zasobów, które zamierzamy umieścić w chmurze oczekujemy bezzwłocznego reagowania na zlecenia wydziału bezpieczeństwa CSIOZ w zakresie zaleceń dotyczących konfiguracji np. blokada określonych adresów IP. Ponadto oczekujemy w takim wariancie pełnego monitoringu i rozliczalności użytkowników w środowisku nie zarządzanym przez CSIOZ. Nie dopuszczamy również możliwości fizycznego dostępu do elementów infrastruktury innych osób niż personel Wykonawcy tzn. inni klienci dzielący infrastrukturę nie mają prawa uzyskiwać dostępu fizycznego do infrastruktury. Wymagany jest również dostęp do wszystkich zdarzeń bezpieczeństwa w otoczeniu środowiska CSIOZ zarządzanych przez uczestnika dialogu. W tym celu oczekujemy wystawienia dedykowanego dashboard w systemie SIEM lub równoważnym, dostępu do konsoli IDS/IPS, NGF, WAF itd. W trybie read only w obszarze dedykowanym CSIOZ. W przypadku gdy środowisko uczestnika dialogu nie posiada takich możliwości prosimy o wskazanie alternatywnej metody dostępu do konfiguracji urządzeń, ustawionych alertów oraz alertów do w/w systemów. Prosimy o przedstawienia dwóch opcji ze współdzielonymi zasoby jak i bez współdzielonych zasobów.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

91.	Jaki punkt demarkacyjny w odpowiedzialności będzie po stronie usługodawcy i zamawiającego w zakresie IaaS	Odpowiedzialność dostawcy usługi będzie od warstwy wirtualizatora w dół.
92.	Jaki punkt demarkacyjny w odpowiedzialności będzie po stronie usługodawcy i zamawiającego w zakresie PaaS	IaaS do poziomu wirtualizatora, PaaS do poziomu orkiestratora
93.	Jakie jest przewidywany wzrost usług zamawiającego	20% rocznie liczone rok do roku
94.	w przypadku braku konieczności udostępniania pełnej zabezpieczonej infrastruktury – jakie SLA byłoby określone dla dostarczenia nowych zasobów	SLA na poziomie 99,98%
95.	Jaki minimalny dystans pomiędzy ośrodkami przetwarzania danych	Taki aby łączne opóźnienie w transmisji nie przekroczyło 5 ms
96.	Czy będą wymagane certyfikaty Tier 3 na ośrodki obliczeniowe, czy wystarczy tylko potwierdzenie spełnienia funkcjonalności. Jakie normy należy wypełnić?	Nie. Wymagana będzie zgodność potwierdzona audytem
97.	Rozwiązania typu vSAN oferują bardzo dobry stosunek wydajności do ceny dla budowania środowiska Storage - czy zamawiający zgadza się na dostarczenie usług opartych o nie przy zachowaniu odpowiedniego SLA ?	CSIOZ nie określa jakie technologie będą wykorzystywane przez dostawcę usługi.
98.	Jakie wymagania dotyczące sprzętu planowanego do budowy środowiska dla Zamawiającego. Produkcja dopuszczona w Europie, Polsce? Czy ma to być sprzęt fabrycznie nowy?	Urządzenia muszą posiadać gwarancję producenta.
99.	Celem zabezpieczenia poprawnego działania usług a w szczególności wydajności procesorów i pamięci czy zamawiający określi minimalne wymagania dotyczące zegarów i ilości corów, ewentualnie daty produkcji poszczególnych komponentów lub zastrzeżenia że sprzęt powinien być nowy	Tak. Zgodnie z testem porównawczym na stronie https://www.cpubenchmark.net/high_end_cpus.html procesor o Pass Mark >=25000

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

100.	Jaki powinien być interfejs do tworzenia nowych maszyn – czy konsola np. Vcenter będzie satysfakcjonująca czy też powinno być przedstawione inny interfejs (dedykowany)	CSIOZ oczekuje propozycji w tym zakresie.
101.	W jaki sposób zamawiający planuje chronić się przed oversubksrypcją – praktyką jest zabezpieczenie w umowie np.: ilości vCorów do fizycznych corów	CSIOZ oczekuje propozycji w tym zakresie.
102.	Jakiego typu interefacy sieciowe są oczekiwane	Oczekujemy propozycji w tym zakresie.
103.	W jakiej ilości i jakiej wydajności są oczekiwane przestrzenie dyskowe. Reguła jest określenie dostępności zasobów o określonej wydajności. Wydajność może być określana poprzez mechanizmy QoS (dla profili wydajnościowych)	Na potrzeby dialogu należy przyjąć maksymalną wydajność dysków na poziomie - 150k IOPS (65% read, 35% write) - 300TB. - 100k IOPS (jw.) - 600TB. - 50k IOPS (jw). - 300TB. Na potrzeby dialogu należy przyjąć wolumen zasobów dyskowych: 1,2 PB.
104.	Czy zamawiający będzie zainteresowany bezpośrednim połączeniem z chmurami publicznymi typu AWS, Azure ?	Tak, zamawiający jest zainteresowany bezpośrednim połączeniem z najpopularniejszymi chmurami publicznymi, w szczególności specyfikacją koniecznych usług, ich ceną oraz czasem realizacji
105.	W jaki sposób realizowana jest redundancja macierzy i ich synchronizacja	Aktualnie replikacja danych odbywa się za pomocą mechanizmów bazodanowych. Nie wyklucza się w przyszłości wykorzystania replikacji macierzowej.
106.	W jaki sposób mają być chronione zasoby wewnątrz sieci – ze schematów wynika, że pomiędzy systemami są postawione firewalle lub zony w firewallach	CSIOZ oczekuje usługi firewall również w wewnętrznych zasobach sieci.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

107.	Czy platformy bezpieczeństwa mogą realizować poszczególne funkcje w ramach jednego clustra urządzeń (pod jednym w każdym ośrodku obliczeniowym) – na nich byłyby konfigurowane zony – czy też powinno być kilka clustrów dodatkowo rozdzielających sieć (schemat P1)	Na potrzeby dialogu można przyjąć rozwiązanie pierwsze. Poszczególne funkcje mogą być spełniane w ramach jednego clustra.
108.	Czy platformy bezpieczeństwa mogą realizować kilka funkcji bezpieczeństwa lub być rozdzielone na platformy różnych dostawców	CSIOZ dopuszcza rozdzielenie platform bezpieczeństwa.
109.	Czy i jakie platformy posiada zamawiający	Posiadamy system SIEM IBM QRadar
110.	Czy zamawiający posiada własny SOC	Planowane jest budowanie SOC w strukturach CSIOZ
111.	Jakiego rodzaju urządzenia powinny być podłączone do SOCa zamawiającego	CSIOZ pod kątem logowania patrzy na typy logów np. zdarzenia bezpieczeństwa, user management, configuration (ze wszystkich urządzeń)
112.	Jaka jest podatność danych na kompresję w systemie backupu ?	Mała
113.	W ilu systemach powinien być zainstalowany agent do backupu - ewentualnie w jakim innym modelu powinien być przeprowadzony backup ?	Na potrzeby dialogu należy założyć instalację agenta integracyjnego na 60 hostach.
114.	Czy są w stanie Państwo określić w jakim tempie będzie rosnąć zapotrzebowanie na przestrzeń do backupu	20% rocznie - to założenie na potrzeby dialogu technicznego.
115.	Czy dopuszczają Państwo zastosowanie rozwiązania HCI (hyper-coverged) przy założeniu, że wspiera ono technologię stretched cluster\metro cluster ?	Tak

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

116.	Czy sprzęt składający się na obie platformy (PaaS ora IaaS) ma być dedykowany ? (serwery, macierze dyskowe, przełączniki sieciowe itd.)	Na potrzeby dialogu tak, oczekiwane jest jednak otrzymanie propozycji innych opcji (i ich korzyści) uwzględniających zapewnienie wymaganego bezpieczeństwa oraz wydajności.
117.	Czy dla części bądź całości rozwiązania wymagane są procesory o wysokim taktowaniu np. Intel® Xeon® Gold 6136 Processor ?	CSIOZ oczekuje dostępności procesorów o wydajności zbliżonej do Intel® Xeon® Platinum 8270.
118.	Czy platformy IaaS oraz PaaS muszą znajdować się w całości na terenie Polski ?	Na potrzeby dialogu należy przyjąć, że TAK
119.	Czy dopuszczają Państwo inny hypervizor dla platformy IaaS (np. Vmware vSphere) i inny dla platformy PaaS (np. KVM) ?	TAK
120.	Czy dla platformy PaaS mają państwo preferencje co do zastosowanej technologii (np. Pivotal Cloud Foundry, Kubernetes, vSphere integrated Containers,) ?	NIE
121.	Do jakiej warstwy abstrakcji platforma PaaS ma zwierać wsparcie? Czy do warstwy aplikacyjnej tzw. Application PaaS (pełne rozumienie kodu przez platformę oraz automatyka tworząca kontenery np. Pivotal) Czy tylko do warstwy konteneryzacji tzw. Container PaaS (np. Kubernetes, Docker etc.)	IaaS do poziomu wirtualizatora, PaaS do poziomu orkiestratora
122.	Dla jakiego profilu zapisu/odczytu wymagane jest 200 000 IOPS? Czy chodzi o profil SQL (100% Random 35% Write 65% Read, Block 64K)?	Na potrzeby dialogu należy przyjąć maksymalną wydajność dysków na poziomie
		- 150k IOPS (65% read, 35% write) - 300TB.
		- 100k IOPS (jw.) - 600TB.
		- 50k IOPS (jw). - 300TB.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

		Na potrzeby dialogu należy przyjąć wolumen zasobów dyskowych: 1,2 PB.
123.	Czy wymagane jest rozwiązanie All-Flash czy dopuszczają Państwo rozwiązanie Hybrydowe (SSD\SAS) ?	Dopuszczone będą rozwiązania hybrydowe.
124.	Czy dla storage wymagane jest szyfrowanie danych tzw. Data-at-Rest encryption ?	Tak.
125.	Czy ze względów licencyjnych (np. Oracle) wymagane będą osobne dedykowane host wydzielone z całej platformy IaaS?	CSIOZ oczekuje propozycji dostawcy usługi w zakresie możliwości wydzielenie dedykowanego clustra na potrzeby serwerów DB Oracle.
126.	Czy dla obu platform należy zapewnić ochronę przeciw malware\APT\ransmoware do poziomu maszyny wirtualnej? Czy taka ochrona ma być zapewniona bezagentowo (np. poprzez mechanizmy takiej jak Vmware NSX)?	Na potrzeby dialogu należy przyjąć, że TAK
127.	Czy wymagany jest dedykowany Sandbox?	Na potrzeby dialogu należy przyjąć, że TAK
128.	Czy dostawca odpowiada za zarządzanie regułami WAF? Czy są przygotowywane i zarządzane przez zamawiającego ?	Prosimy o przedstawienie obu możliwości pod kątem finansowym
129.	Prośba o doprecyzowanie punktów 7.1 oraz 7.2 dotyczących „Centralnych słowników i katalogów” ?	Punkty zostały usunięte z materiału.
130.	Czy podczas migracji maszyn wirtualnych na nową platformę dopuszczają Państwo przerwy w działaniu systemów?	Tak. Prosimy o szacowanie zależności pomiędzy długością przerwy a kosztem migracji.
131.	Czy migracja ma zostać przeprowadzona jednorazowo czy usługi będą migrowane grupami ?	Usługi mogą być migrowane grupami zapewniając ciągłość działania aplikacji.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

132.	Czy podczas migracji wymagane jest dostarczenie tymczasowego łącza L2 aby np. uniknąć zmiany adresacji maszyn wirtualnych oraz umożliwić migrację etapami? Czy łącze to musi spełniać wymagania bezpieczeństwa np. szyfrowanie sprzętowe ?	CSIOZ oczekuje propozycji w tym zakresie.
133.	Czy podczas migracji dopuszczają państwo wykonanie backupu całego środowiska aby później wykonać tzw. Seeding i replikować tylko zmiany powstałe od wykonania kopii środowiska?	Tak, dopuszczamy.
134.	Jaki jest wymagany maksymalny czas migracji obecnego środowiska na nową infrastrukturę ?	Prosimy o oszacowanie w Państwa propozycji czasu niezbędnego na wykonanie tej operacji.
135.	Czy dostawca jest zobowiązany do przedstawienia referencji w zakresie usług migracji?	Na czas dialogu nie ma takiej potrzeby.
136.	Czy będą wymagane łącza transmisji danych pomiędzy nowym środowiskiem a lokalizacjami Zamawiającego ? Jeżeli tam to prosimy o pełną specyfikację wymaganych łączy.	Na potrzeby dialog należy założyć, że potrzebne będzie łącze 1 Gbit/s
137.	Prosimy o informacje jakie parametry powinno mieć łącze dostępowe do Internetu w nowym środowisku ?	Organizator dialogu wymaga łącza do sieci Internet w przepływności minimum 700 Mbit/s.
138.	Czy wymagana jest obsługa chmury, czy tylko udostępnienie zasobów i narzędzi?	W IaaS obsługa do poziomu wirtualizatora włącznie, w PaaS do poziomu orkiestratora.
139.	Czy CSIOZ oczekuje realizacji chmury prywatnej jako odseparowanych niewspółdzielonych i wydzielonych fizycznie elementów dla przestrzeni dyskowej i warstwy compute (np. separacja na poziomie szafy rack)?	Nie, oczekujemy aby dostęp do przydzielonej nam infrastruktury ograniczony był wyłącznie do personelu obsługi Wykonawcy

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

140.	Czy dostawca ma zapewnić rozwiązanie active-active czy tylko udostępnić zasoby, które taki model umożliwiają?	Oczekiwana jest tylko dostępność zasobów.
141.	Czy dostawca powinien zapewnić automatyczne przełączenie pomiędzy ośrodkami, czy udostępnić narzędzia to umożliwiające?	Na potrzeby dialogu dostawca powinien zapewnić automatyczne przełączenie pomiędzy ośrodkami.
142.	Prosimy o rozwinięcie architektury systemu ZSMOPL – np. schemat logiczny, użyte komponenty itp	Nie możemy przedstawić diagramu architektury na tym etapie postępowania.
143.	I.2.c,d (serwery WWW i aplikacje WWW) Wymagania te odnoszą się do aplikacji, czy są nie istotne dla dostawcy chmury?	Odnoszą się jedynie do zakresu nadzorowanego przez operatora usług chmurowej
144.	I.2.c i d) Czy dostawca powinien również dostarczyć usługi związane z aplikacją?	NIE
145.	I.2.f) Czy dopuszczalne jest wykorzystanie 2 oddzielnych CPD umożliwiające pracę active-active, ale znajdujących się na terenie 1 kampusu (2 oddzielne budynki oddalone o kilkaset metrów od siebie) + trzecie CPD w trybie "passive"?	CPD mają spełniać wymagania normy EN50600 w zakresie bezpieczeństwa i infrastruktury.
146.	I.7.6-7) Czy zamawiający wymaga dostarczenia usług związanych z integracją aplikacji?	Intencją Organizatora jest poznanie usług PaaS umożliwiających integrację poszczególnych komponentów aplikacji
147.	III-IV - Prośba o zdefiniowanie zakresu odpowiedzialności dostawcy poza dostarczeniem platformy chmurowej, np. w zakresie CI/CD.	IaaS do poziomu wirtualizatora, PaaS do poziomu orkiestratora
148.	IV.4 Czy liczba HD space zawiera w sobie również przestrzeń SSD, czy należy te wartości zsumować dla otrzymania całkowitej wymaganej powierzchni?	HD space [GB] zawiera w sobie pojemność SSD.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

149.	IV.5 i V.3: Czy wymagane jest tylko zapewnienie narzędzia czy pełna obsługa? dla przykładu konfiguracja WAF wymaga znajomości aplikacji, do której jest wykorzystywany.	Na potrzeby dialogu prosimy o wycenę dla obu opcji
150.	IV.5 i V.3: Czy obsługa NOC i SOC ma zostać zapewniona przez dostawcę?	W zależności od modelu świadczenia i to wyłącznie do punktu styku. W przypadku PaaS do poziomu usług, w przypadku IaaS do poziomu sprzętu. Ponadto należy zakładać udostępnienie wglądu w dedykowany dashboard oraz zasilanie określonymi logami systemu SIEM Zamawiającego
151.	VI.7 Czy dopuszczalne jest zapewnienie separacji na poziomie VXLAN zamiast VLAN?	Od strony bezpieczeństwa TAK.
152.	VIII. Czy dla platformy P1 wymagane są usługi chmurowe takie jak możliwość samodzielnej zmiany zasobów czy konfiguracji (dostęp przez portal WWW), kontenery, itp.?	Nie.
153.	Czy możliwe jest zastosowanie „flavorów” (zdefiniowanych wcześniej wielkości przydzielanych zasobów, np. serwer o parametrach 4 vCPU, 16 GB RAM, itp.) czy wymagana jest pełna dowolność w tym zakresie?	W architekturze IaaS pełna dowolność, w PaaS mogą być usługi predefiniowane.
154.	VIII. Czy dla platformy P1 dopuszczalne jest wykorzystanie innego wirtualizatora, np. KVM zamiast VMware?	CSIOZ nie określa jakie technologie będą wykorzystywane przez dostawcę usługi.
155.	VIII.2.e) Jaka jest wymagana przestrzeń dyskowa? Informacja z tego punktu nie pokrywa się z tabelą w pkt. 1.n Jakie są wymagania wydajnościowe dla tej przestrzeni?	Na potrzeby dialogu należy przyjąć wolumen zasobów dyskowych: 1,2 PB

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

156.	IX. Czy dla potrzeb wyceny należy przyjąć podstawowy scenariusz wykonywania kopii zapasowych dla wszystkich danych?	CSIOZ nie określa na etapie dialogu scenariusza backupu. Należy przyjąć pojemność systemu backupowego na poziomie 700 TB.
157.	XI.4.a) Czy skalowalność bez restartu dotyczy rozszerzenia platformy, czy konkretnych maszyn wirtualnych na niej działającej?	Dotyczy platformy a nie maszyn wirtualnych.
158.	Czy jest wymagane zestawienie sieci dedykowanej WAN/MPLS do CPD dla administratorów i/lub integracji z innymi systemami?	Tak.
159.	Czy chmury IaaS i PaaS powinny być dostarczone w tej samej technologii ze względu na użyty wirtualizator?	Tak, to jest preferowane rozwiązanie.
160.	Czy chmury IaaS i PaaS powinny być dostarczone w tej samej technologii ze względu na użyty panel administracyjny do udostępniania zasobów?	Tak, to jest preferowane rozwiązanie.
161.	Które produkty lub typy produktów będące elementami systemu powinny spełniać wymagania Common Criteria ISO/IEC 15408?	ISO/IEC 15408-1 Norma definiuje podstawowe pojęcia, zasady oceny systemów informatycznych oraz ogólny model przeprowadzania takiej oceny.
		ISO/IEC 15408-2 Norma definiuje katalog komponentów funkcjonalnych pogrupowanych w grupy i klasy, za pomocą których można tworzyć szablony wymagań bezpieczeństwa dla środków teleinformatycznych.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

		ISO/IEC 15408-3 Norma definiuje wymagania w celu osiągnięcia wskazanych poziomów zaufania, przedstawiono w niej kryteria oceny profilu zabezpieczeń i zadania zabezpieczeń, jak również wprowadzono poziomy zaufania (EAL – Evaluation Assurance Levels). - oprócz samych urządzeń należy zweryfikować także procedury w zakresie bezpieczeństwa i budowy zaufania.
162.	Czy w miejsce proponowanej weryfikacji z zachowaniem Common Criteria ISO/IEC 15408 (str. 6) można zaproponować inne obiektywne opisy dotyczące architektury, w szczególności architektury bezpieczeństwa?	Tak
163.	Jakiego rodzaju informacje muszą udostępniać logi (lub raporty) systemowe? Czy mają one dotyczyć pełnej rozliczalności użytkowników w systemie? Czy mają też udostępniać wszelkie zmiany konfiguracyjne poczynione przez użytkowników (w tym administratorów)?	Minimum zmiany konfiguracji z informacją umożliwiająca identyfikacje autora + informacje umożliwiające rozliczalność usług na poziomie systemów
164.	Czy serwery www mają być oparte o usługi IaaS czy PaaS?	Powinna być możliwość uruchomienia serwera www zarówno jako usługa IaaS jak i PaaS.
165.	Czy wymagany będzie dostęp warunkowy dla administratorów oparty o role, a więc ograniczony precyzyjnie zdefiniowanym zakresem.	Tak.
166.	Czy wymienione na początku opracowania zasady bezpieczeństwa dotyczą wszystkich systemów i ich komponentów?	Dotyczą całości lub części rozwiązania proponowanego przez dostawcę usługi. zależnie od podrozdziału.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

167.	Czy definicja chmury prywatnej jest tożsama z definicją przyjętą w Uchwale Rady Ministrów w sprawie Inicjatywy “Wspólna Infrastruktura Informatyczna Państwa” z 24 września 2019?	Tak
168.	Czy otrzymamy szczegółowe dokumentacje systemów, które będą podlegać migracji do chmury?	NIE. Na etapie dialogu technicznego nie ma możliwości udostępnienia tych danych.
169.	Czy CSIOZ ma preferowaną metodykę analizy ryzyka jaką należy zastosować?	Nie. Oczekujemy propozycji uczestników dialogu w tym zakresie.
170.	Z jakich aktów prawnych wynika wymaganie lokalizacji przetwarzania danych na terenie Polski? Jeśli takie wymagania są niejawne prosimy o umożliwienie zapoznania się z nimi zgodnie z procedurą (nasza firma posiada certyfikat bezpieczeństwa przemysłowego).	Wynika z dokumentów źródłowych projektu e-Krew. Na potrzeby dialogu technicznego należy przyjąć takie założenie. Dalsze kroki w celu wyjaśnienia czy wystarczy warunek "CPD na terenie UE" zostaną rozstrzygnięte po ustaleniu klasyfikacji danych jakie można składować w chmurze.
171.	Czy wymaganie zgodności architektury DC z Tier III można dla nowoczesnych DC zastąpić innym wymaganiem – na przykład potwierdzonymi audytami certyfikacjami i normatywami określającymi poziom dostępności i niezawodności infrastruktury – takimi jak UK G-Cloud, ENISA IAF, SOC 1, SOC 2.	Można. Organizator dialogu oczekuje informacji na temat metod certyfikacji oraz standardów w tym zakresie panujących na rynku.
172.	Czy w miejsce przeprowadzania audytów DC akceptowane będą wyniki niezależnych audytów przeprowadzonych przez uznane podmioty?	Organizator Dialogu gromadzi dane na ten temat. Audyt jest jedną z proponowanych metod.
173.	Czy wymaganie połączenia DC „ciemnymi włóknami” można zastąpić wymaganiem dedykowanego łącza światłowodowego?	Tak. CSIOZ dopuszcza takie rozwiązanie.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

174.	Czy dostępne będą szczegółowe dane na temat systemów pozwalające wykonać analizę ryzyka migracji do i z chmury? Czy określenie „analiza ryzyka" jest równoznaczne z wymienieniem listy potencjalnie ryzykownych czynności?	Oczekujemy analizy ryzyka (zarysu) w oparciu o dostarczone dane oraz w oparciu o doświadczenia uczestników dialogu w tym zakresie.
175.	Czy dostawca usług chmurowych pełni wyłącznie rolę podmiotu przetwarzającego (strona 12 i nast.)?	Nie. Uczestnik dialogu powinien przewidzieć także zawarcie umowy podpowierzenia danych osobowych.
176.	Jeśli tak - Z czego wynika powtórzenie w zapisie dotyczącym Powierzenia Danych (str.14) zapisów wprost wynikających dla podmiotu przetwarzającego z prawa (przykłady: punkty b), f) i) itd., również zapisy na str. 15)	Organizator dialogu przewiduje możliwość podpowierzenia danych osobowych. Należy rozważyć taką opcję.
177.	Czy należy oddzielnie przygotowywać odpowiedź do Powierzenie Danych punkt e) – bezpieczeństwo i jego realizacja jest szeroko omawiane w innych rozdziałach.	Tak
178.	Czy w Powierzenie Danych (punkt o) chodzi o lokalizację miejsca przechowywania danych osobowych przy normalnej eksploatacji systemów?	Tak, chodzi o architekturę bezpieczeństwa. Organizator dialogu rozważa przechowywanie w chmurze danych medycznych. W przypadku awarii dane te nie mogą opuścić terytorium objętego jurysdykcją RP jako dane systemów kluczowych i dane wrażliwe. Organizator dialogu jest w trakcie prac nad dokładnym opracowaniem tych zagadnień.
179.	Czy zapis „Spełnienie wymagań ustawy o cyberbezpieczeństwie będzie wymogiem zamawiającego" (str. 15) dotyczy spełniania wymagań ustawy o krajowym systemie cyberbezpieczeństwa?	Tak - zapis dotyczy wymagań zawartych w ustawie o krajowym systemie cyberbezpieczeństwa.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

180.	Czy Zamawiający jest Operatorem Usługi Kluczowej w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa?	TAK
181.	Które z projektów wymienionych w materiałach pomocniczych do dialogu technicznego są Usługami Kluczowymi w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa?	Na potrzeby dialogu należy przyjąć, że wszystkie wymienione w materiale pomocniczym są Usługami Kluczowymi.
182.	Jeśli Zamawiający jest Operatorem Usługi Kluczowej, a przynajmniej jeden z projektów wymienionych w materiałach jest Usługą Kluczową w rozumieniu uksc w jaki sposób dostawca chmury obliczeniowej ma potwierdzić status Dostawcy Usługi Cyfrowej w rozumieniu tej ustawy, a w szczególności spełnianie wymagań wynikających z Rozporządzenia 151/2018?	Celem dialogu jest pozyskanie wiedzy w tym zakresie - wiedzy nt. możliwości technicznych i organizacyjnych operatorów usług. Brak takich możliwości po stronie operatorów pozwoli organizatorowi na podjęcie stosownych decyzji. Celem dialogu jest w istocie określenie możliwości wykonania zamierzonego celu - wykorzystania zasobów operatora chmury - chmury prywatnej.
183.	Jeśli niektóre projekty wymienione w materiałach są Usługą Kluczową w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa, a pozostałe takimi Usługami nie są to czy Zamawiający przewiduje zróżnicowanie wymagań dotyczących dostępności, bezpieczeństwa itd. Itp. dla poszczególnych projektów?	Na potrzeby dialogu należy przyjąć, że wszystkie wymienione w materiale pomocniczym są Usługami Kluczowymi.
184.	Czy Zamawiający przewiduje dodatkowe wymagania wobec Dostawcy Usługi Cyfrowej wychodzące poza zakres opisany w uksc, jaka jest ich podstawa prawna oraz czego dotyczą?	Na obecnym etapie prac nie można mówić o wymaganiach Zamawiającego. Prowadzony jest jedynie dialog techniczny w celu pozyskania wiedzy o możliwych do wykorzystania rozwiązaniach technicznych i organizacyjnych.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

185.	Co oznaczają „dane wrażliwe” wymienione w Rozdziale VI p. 10 strona 36?	Dane wrażliwe zgodnie z RODO: dane ujawniające pochodzenie rasowe lub etniczne, dane ujawniające poglądy polityczne, dane ujawniające przekonania religijne lub światopoglądowe, dane dotyczące seksualności lub orientacji seksualnej, dane o stanie zdrowia.
186.	Czy istnieje wstępny zakres kompetencji zespołu opisanego w Rozdziale VII p. 2 Migracja systemu ZSMOPL do środowiska chmury obliczeniowej oraz czy można się z nim zapoznać?	Właśnie opisu kompetencji wymaganych od zespołu oczekuje organizator dialogu od uczestników ponieważ sam pragnie tę wiedzę pozyskać lub zweryfikować.
187.	W jakim zakresie operator (dostawca usługi chmurowej?) ma szacować ryzyko w procedurach wyjścia z chmury (Rozdział X).	W zakresie możliwości przeniesienia usług do innego operatora w przypadku nagłej konieczności.
188.	Czy i kiedy projekty opisane w materiałach zostaną przeniesione do Rządowej Chmury Obliczeniowej (w rozumieniu projektu opisanego w Uchwale Rady Ministrów z 24 września 2019r dot. Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”)?	W tym zakresie CSIOZ oczekuje na uzgodnienia. Do momentu ich pozyskania planowane jest wykorzystanie usług operatorów komercyjnych.
189.	Czy Zamawiający będzie wymagał od dostawcy usług chmurowych realizacji tych usług na podstawie licencji przygotowanej przez Zamawiającego?	Organizator dialogu rozważa takie rozwiązanie.
190.	Czy przez pojęcie serwera logów można rozumieć mechanizm zbierania, analizy i udostępniania logów – nie będący sensu stricto serwerem?	Tak.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

191.	W celu umożliwienia wsparcia w procesie migracji systemów na infrastrukturę Chmury Obliczeniowej niezbędne będzie wsparcie programistyczne w celu dostosowania aplikacji elementów aplikacji. W związku z powyższym w jakich językach programowania napisane zostały Państwa Aplikacje?	Wszelkie zmiany w aplikacjach będzie wykonywał CSIOZ w oparciu o uzgodnienia w ramach zespołu ds. migracji.
192.	Z racji obecnych zaleceń bezpieczeństwa wszelka komunikacja do aplikacji webowych powinna być realizowana jako połączenia szyfrowane z wykorzystaniem mechanizmów w tym wypadku SSL. Gdzie w Państwa infrastrukturze jest terminowany tunel SSL dla połączeń szyfrowanych na urządzeniu dedykowanym czy też na serwerach aplikacyjnych?	Na potrzeby Dialogu należy przyjąć, że ruch szyfrowany terminowany jest na serwerach aplikacyjnych
193.	Czy w ramach zarządzania oraz administrowania infrastrukturą oraz systemami wykorzystują Państwo lub zamierzają Państwo wykorzystywać rozwiązania klasy PAM (Privileged Account Management), zapewniających: - zarządzanie hasłami i ich rotacją,; - zabezpieczenie kont uprzywilejowanych przed operatorami, ; - zabezpieczenie konsol przed krytycznymi poleceniami (reload, erase), ; - utrzymania bezpiecznego magazynu kluczy (HSM), ; - utrzymanie bezpiecznego centrum certyfikacji (CA).	Na potrzeby Dialogu należy przyjąć że CSIOZ wykorzystuje rozwiązania klasy PAM

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

194.	Jakimi systemami bezpieczeństwa dysponujecie Państwo obecnie, które mogłyby Państwa zdaniem znaleźć zastosowanie w infrastrukturze operatora Chmury? (mamy tu na myśli rozwiązania klasy LoadBalanser, WAF, FW, IPS, AntyDDOS, Global Site Selektor, VPN, Sandbox, AntyMalware, AntySpam,…) Czy obecne systemy są w postaci HW czy też SW?	Na potrzeby dialogu należy przyjąć, że Uczestnik dialogu dostarcza wymienione rozwiązania z przyjętym założeniem: "W przypadku wyposażania infrastruktury teleinformatycznej środowiska chmurowego w rozwiązania klasy IPS/IDS, NGF, WAF, DLP (pkt. 5 podpunkt 3) oczekujemy zaoferowania rozwiązań sklasyfikowanych w grupie wiodących (Leaders) bądź rokujących (Challengers) producentów wedle klasyfikacji firmy Gartner rok bieżący i poprzedni. Dopuszczamy zarówno rozwiązania komercyjne, jaki i opensource pod warunkiem spełnienia naszych oczekiwań, jak i posiadania wsparcia producenta/suportu. Podstawowe założenia architektury bezpieczeństwa opieramy na wymaganiu, że zaproponowane rozwiązanie powinno uwzględniać fakt iż przestrzenie dyskowe, RAM, CPU dedykowane są wyłącznie dla CSIOZ. Dopuszczamy możliwość współdzielenia RAM, CPU, infrastruktury sieciowej wraz z urządzeniami bezpieczeństwa. W takim przypadku wymagane jest przeprowadzenie przez uczestnika dialogu analizy ryzyka opisującej możliwe zagrożenia, sposoby postępowania z nimi, aby bezpieczeństwo systemów IT CSIOZ, jak i przetwarzanych w nich danych było zagwarantowane na akceptowalnym przez nas poziomie. Analiza musi uwzględnić możliwe zagrożenia na warstwie hardware, software, jak i network. Dla przykładu, podatność w systemie innego klienta z którym będzie współdzielona infrastruktura może umożliwiać wydostanie się atakującego poza środowisko wirtualne tego klienta i umożliwić dostęp do zasobów CSIOZ po przejęciu maszyny fizycznej - w takim przypadku należy udzielić odpowiedzi jakie zabezpieczenia zostaną wdrożone aby nie dopuścić do takiego wariantu. Ponadto w przypadku współdzielenia środowisk oczekujemy wsparcia w przypadku incydentów

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

		bezpieczeństwa ze strony Uczestnika Dialogu wraz z zabezpieczeniem materiałów dowodowych znajdujących się we współdzielonej przestrzeni. Ze względu na istotność zasobów, które zamierzamy umieścić w chmurze oczekujemy bezzwłocznego reagowania na zlecenia wydziału bezpieczeństwa CSIOZ w zakresie zaleceń dotyczących konfiguracji np. blokada określonych adresów IP. Ponadto oczekujemy w takim wariancie pełnego monitoringu i rozliczalności użytkowników w środowisku nie zarządzanym przez CSIOZ. Nie dopuszczamy również możliwości fizycznego dostępu do elementów infrastruktury innych osób niż personel Wykonawcy tzn. inni klienci dzielący infrastrukturę nie mają prawa uzyskiwać dostępu fizycznego do infrastruktury. Wymagany jest również dostęp do wszystkich zdarzeń bezpieczeństwa w otoczeniu środowiska CSIOZ zarządzanych przez uczestnika dialogu. W tym celu oczekujemy wystawienia dedykowanego dashboard w systemie SIEM lub równoważnym, dostępu do konsoli IDS/IPS, NGF, WAF itd. W trybie read only w obszarze dedykowanym CSIOZ. W przypadku gdy środowisko uczestnika dialogu nie posiada takich możliwości prosimy o wskazanie alternatywnej metody dostępu do konfiguracji urządzeń, ustawionych alertów oraz alertów do w/w systemów. Prosimy o przedstawienia dwóch opcji ze współdzielonymi zasoby jak i bez współdzielonych zasobów."

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

195.	Czy Zamawiający oczekuje przedstawienia koncepcji uwzględniającej możliwość zaoferowania rozwiązania które m.in. wykorzysta posiadaną przez Państwa moc obliczeniową? W celu zaproponowania oferty opartej także na Państwa zasobach prosimy o przesłanie zestawienia użytkowanych przez Państwa urządzeń i ich podzespołów lub zbiorczych wartości (ilość serwerów, ilość i rodzaj procesorów, ilość pamięci ram, ilość i prędkość połączeń sieciowych, czy mogą być objęte suportem na oczekiwany czas eksploatacji)?	Na potrzeby dialogu proszę przyjąć, iż wszystkie zasoby będą należały do operatora usługi. Wyjątkiem będą urządzenia bezpieczeństwa typu HSM. W ich przypadku należy przedstawić opcję - czy możliwe jest umieszczenie tych urządzeń w zasobach operatora lub zestawienie połączeń tak aby te urządzenia pozostały w siedzibie Organizatora dialogu.
196.	Czy Zamawiający oczekuje koncepcji uwzględniającej możliwość dynamicznej rozbudowy infrastruktury fizycznej, gwarantujących możliwość zestawiania do klastra kolejnych urządzeń w fizycznych w oparciu o zastosowane już ustawienia, w ciągu dziesiątek minut.	TAK
197.	Czy w związku z rozbieżnością pomiędzy metodologią testów syntetycznych Zamawiający oczekuje zastosowania dedykowanych klas pamięci masowej odpowiednich dla wydajności, pojemności, itp., zapewniających konkretne parametry fizyczne?	Tak. Organizator jest zainteresowany przedstawieniem szczegółowych parametrów rozwiązania.
198.	Czy przez wzgląd na narzut warstw: systemu operacyjnego, wirtualizacji, kontenerów oraz jego zmienność, Zamawiający oczekuje zaprezentowania w koncepcji założeń ochrony realnej dostarczanej wydajności (compute)?	Tak. Organizator jest zainteresowany przedstawieniem szczegółowych parametrów rozwiązania.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

199.	Czy w związku z rozbieżnością pomiędzy technologiami wykorzystywanych przez poszczególne elementy platform kontenerowych Zamawiający jest w stanie określić zależności (dependencies) oprogramowania dla aktualnie uruchamianych i testowanych kontenerów?	Na potrzeby dialogu należy przyjąć, iż organizator dialogu jest w stanie zaakceptować każdą, wiodącą platformę kontenerową.
200.	Czy przez wzgląd na wymagania co do ciągłości działania Zamawiający oczekuje koncepcji opartych wyłącznie o pamięć masową (storage) zapewniającą warstwę wirtualizacji, gwarantującą bezprzerwowe działania zasobów obliczeniowych niezależnie od awarii jakiegokolwiek komponentu pamięci masowej lub też dwóch takich komponentów?	CSIOZ nie określa jakie technologie będą wykorzystywane przez dostawcę usługi.
201.	Czy Zamawiający oczekuje zaprezentowania koncepcji zapewniającej mechanizmy katalogu usług umożliwiającego automatyczne kretowanie elementów środowisk w oparciu o zdefiniowane schematy?	TAK
202.	Czy Zamawiający oczekuje zaprezentowania koncepcji zapewniającej mechanizmy bilingowania zewnętrznego i wewnętrznego umożliwiających monitorowanie zużycia?	TAK
203.	Czy Zamawiający oczekuje zaprezentowania w koncepcji wariantu klastra rozciągniętego pomiędzy dwie główne lokalizacje w trybie Active-Active?	CSIOZ oczekuje prezentacji wariantu klastra rozciągniętego active-passive oraz opcjonalnie klastra active-active.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

204.	Czy szyfrowanie danych ma odbywać się również wewnątrz środowiska, czy jednie do komunikacji na zewnątrz	Na potrzeby dialogu należy założyć, że dane mają być szyfrowane również wewnątrz środowiska. Jeśli chodzi o komunikację zewnętrzną to ruch oczywiście musi być szyfrowany.
205.	Jakiego typu licencje zamawiający planuje dostarczyć samodzielnie do środowisk IaaS	CSIOZ rozważa dostarczenie licencji RedHat, SUSE, Windows, VMWare
206.	Czy platforma sprzętowa dla omawianych środowisk może być wspólna, czy też każde powinno posiadać dedykowane dla siebie zasoby sprzętowe	Platforma sprzętowa może być wspólna przy czym środowiska muszą być odseparowane sieciowo (VLAN) oraz zabezpieczone przez firewall
207.	Czy możliwe jest, po podpisaniu stosowanych dokumentów uzyskanie informacji nt rzeczywistych konfiguracji środowisk, obciążeń, wzajemnych powiązań, aktualnych platform. Jest to niezbędne do dokładnej wyceny rozwiązań - prezentowane dane mają charakter zbyt ogólny	Organizator dialogu nie ma upoważnienia do przedstawiania szczegółów budowy systemów. Na potrzeby dialogu technicznego należy przyjąć założenia:. 1. 4 FW o wydajności: - W zakresie Firewall'a obsługa nie mniej niż 8 mln jednoczesnych sesji oraz 185.000 nowych połączeń na sekundę. - Przepustowość Firewall: nie mniej niż 75 Gbps - W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. - Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 20 Gbps 2. 4 FW o wydajności:

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

		- W zakresie Firewall'a obsługa nie mniej niż 3 mln jednoczesnych sesji oraz 125.000 nowych połączeń na sekundę. - Przepustowość Firewall: nie mniej niż 15 Gbps - Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 4.5 Gbps - W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q 3. 2 LoadBalancery: Przepływność dla warstwy 4 Nie mniej niż 80 Gbps z możliwością rozbudowy do 320 Gbps dla całości systemu. W przypadku rozbudowy urządzenia niemodularnego dopuszcza się rozwiązanie, które umożliwia rozbudowę przepływności do 160Gbps per urządzenie fizyczne za pomocą zmiany licencji. Przepływność dla warstwy 7 Nie mniej niż 80 Gbps z możliwością rozbudowy do 320 Gbps dla całości systemu W przypadku rozbudowy urządzenia niemodularnego dopuszcza się rozwiązanie, które umożliwia rozbudowę przepływności do 120Gbps per urządzenie fizyczne za pomocą zmiany licencji. Ilość jednocześnie obsługiwanych połączeń dla warstwy 4 Nie mniej niż 48 000 000 z możliwością rozbudowy do 192 milionów dla całości systemu

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

		Ilość transakcji SSL na sekundę dla klucza o długości 2048 Nie mniej niż 40 000 z możliwością rozbudowy do 160 tysięcy dla całości systemu. Dla urządzenia niemodularnego musi być zapewniona możliwość rozbudowy transakcji do nie mniej niż 50 000. Ilość jednocześnie obsługiwanych połączeń SSL Nie mniej niż 10 000 000 z możliwością rozbudowy do 40 milionów dla całości systemu Przepływność ruchu szyfrowanego Nie mniej niż 32 Gbps z możliwością rozbudowy do 128 Gbps dla całości systemu. Dla urządzenia niemodularnego musi być zapewniona możliwość rozbudowy do nie mniej niż 48Gbps. Ilość połączeń na sekundę w warstwie 4 Nie mniej niż 1 000 000 z możliwością rozbudowy do 4 milinów dla całości systemu Sprzętowa ochrona DDoS Nie mniej niż 15 000 000 SYN cookies na sekundę. Ilość wirtualnych instancji Nie mniej niż 20 z możliwością rozbudowy do 80 dla całości systemu.
208.	Jak dokładnie należy rozumieć zapis : 1 VCore = 1 VCPU x 2,5 Ghz 64-bitowy ? Czy jest to mapowanie 1vCPU na 1 fizyczny rdzeń procesora taktowanego min 2,5GHz ?	TAK

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

209.	Prosimy o wyjaśnienie czemu ma służyć spełnienie wymogu dostarczenia platformy IaaS spełniającej parametry wydajności storage. d. IOPS w przestrzeni dyskowej skalowanej min. wg przedziałów: do 1000; 1000 - 20000; 20000-50000; 50000 - 100000; 100000 - 200000; 200000 i więcej	W dialogu technicznym niczego nie trzeba dostarczać. Chodzi o pokazanie organizatorowi jakie są zależności pomiędzy wyceną przestrzeni dyskowej a jej wydajnością. Organizator dialogu ma potrzeby w zakresie wydajności systemów baz danych ale musi też mieć wiedzę o kosztach stosowania wysokiej wydajności.
210.	1. str. 4"Opis podstawowych wymagań, które ma spełniać dostarczone rozwiązanie z ww. obszarów, zamieszczono w kolejnych punktach, przy czym należy uwzględnić, że CSIOZ opracowuje i aktualizuje swoją polityką bezpieczeństwa w sposób ciągły i sukcesywny, a jej aktualizacje/modyfikacje będą musiały być zaimplementowane w dostarczonych środowiskach chmurowych" str. 4Istnieje ryzyko w trakcie trwania kontraktu że powstanie wymóg który spowoduje, że niezbędne będzie poniesienie dodatkowych kosztów na dostosowanie do nowej polityki. Co w takiej sytuacji?	Na potrzeby dialogu należy przyjąć iż zmienność w zakresie polityki bezpieczeństwa nie powoduje skutków finansowych.
211.	2 str. 5Architektura systemu Architektura chmury/platformy ma spełniać wymogi (ISO 15408) czy też architektura systemów po przeniesieniu do chmury?	Przedmiotem świadczonej usługi będzie utrzymanie zasobów chmurowych. Systemy umieszczone przez CSIOZ w chmurze będą utrzymywane przez CSIOZ.
212.	2.b str. 5Systemy operacyjne1) W ramach systemu możliwe jest wykorzystanie jedynie systemów operacyjnych posiadających wsparcie producenta systemu." O jakim poziomie wsparcia jest mowa? - czy wystarczy wydawanie poprawek do systemu? w dalszej części jest mowa o Centosie (str.32) więc czy można założyć że nie będzie wymagany support komercyjny?	Chodzi jedynie o systemy instalowane przez dostawcę usługi. Systemy operacyjne, którymi zarządza CSIOZ nie są przedmiotem tego wymogu.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

213.	2.c.Serwery WWW / aplikacje WWW Mowa o serwerach/usługach na których zbudowana jest platforma, czy o tych które zainstalowane są w ramach środowiska CSIOZ? Co rozumiemy przez aktualną wersję? Pkt d wygląda na skierowany bardziej do dostawcy aplikacji?	W modelu PaaS możliwe jest świadczenie usługi "serwer WWW jako serwis" i tylko o takie serwery chodzi.
214.	3.3 str. 7"Wdrożenie mechanizmów zarzadzania pojemnością infrastruktury, minimum w zakresie wysycenia pamięci, zajętości procesora, wysycenia łącza, zajętości powierzchni dyskowej (próg ostrożnościowy ustawiony maks. na poziomie 75%, próg krytyczny ustawiony maks. na poziomie 90% wysycenia zasobu)."Co po przekroczeniu zasobów fizycznych?	Organizator dialogu pragnie zdobyć wiedzę w tym zakresie - czy możliwe jest powiększenie zasobu chmury prywatnej i jakim kosztem. Organizator dialogu przewiduje, że dla zasobu chmury prywatnej zostanie określone maximum w zakresie powiększania skali.
215.	2.f.4 str. 7Load balancing Prosimy o doprecyzowanie o jaki rodzaj load balancingu chodzi (w której warstwie, na jakich zasadach)? Czy można otrzymać szacunki odnośnie oczekiwanej wydajności/przepływności/sesji(z szyfrowaniem i bez)	Load balancera używamy w warstwie 7. Poza rozkładaniem ruchu load balancer pełni następujące funkcje: - terminacja SSL - modyfikacja nagłówków http - modyfikacja treści w pakiecie - wystawianie stron serwisowych (w tym automatyczne na podstawie aktywnych sesji) - podtrzymywanie sesji w oparciu o cookie, identyfikatory SSL - są również wdrożone różne mechanizmy rozkładania ruchu w oparcie o jezyk skryptowy.
216.	6. Wymagania dot. bezpieczeństwa połączeń zewnętrznych3) Czy są jakieś konkretne wymagania funkcjonalne dla tych rozwiązań?	Tylko wymagania w zakresie bezpieczeństwa opisane w materiale pomocniczym.
217.	8 str. 10 Zgodność z normami. O jakie konkretnie normy chodzi ?	Normy wymienione w materiale pomocniczym

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

218.	II.4 str. 12Certyfikaty, normy ISO pkt. 7.II.4 Normy ISO: a) ISO 27001,b) ISO 27017c) ISO 27018d) ISO 22301e) ISO 31000Czy pojawią się inne wymagania dotyczące środowisk chmurowych np. CSA STAR czy danych medycznych np. HIPAA?	Organizator pragnie pozyskać wiedzę w tym zakresie .
219.	W przypadku zapisu "Zamawiający wymaga możliwości odtworzenia wybranego serwera lub usługi w wydzielonym od produkcji środowisku" jakie zasoby dla celów odtwarzania należy założyć ?	Chodzi o możliwość odtworzenia maszyny wirtualnej lub kontenera
220.	Prosimy o dokładne, najlepiej tabelaryczne przedstawienia rozdziału kompetencji pomiędzy Dostawcą i Zamawiającym	Prosimy o propozycje takiego podziału w Państwa prezentacji
221.	Czy możliwe jest, dla potrzeb dokładnego przedstawienia scenariusz-y i harmonogramów migracji, otrzymanie bardziej precyzyjnych informacji nt sposobu funkcjonowania poszczególnych platform? Chodzi tutaj głównie o sposób w jaki kontaktują się ze światem zewnętrznym, w jaki sposób wymieniają dane i w jaki sposób efekty ich pracy są prezentowane. Pamiętajmy, że w przypadku migracji wszystko powyższe powinno zostać utrzymane	Na etapie dialogu CSIOZ nie przewiduje przekazania bardziej szczegółowych informacji
222.	1.b.6 str. 5Integracja mechanizmów blokowania/odblokowania z mechanizmami AD / równoważnymi. Czy autoryzacja do chmury/platformy ma być zrealizowana w oparciu o zewnętrzne źródło autentykacji? Czy będzie integracja z AD?	Oczekujemy, że uczestnik dialogu przedstawi możliwe sposoby w jego rozwiązaniu. CSIOZ przewiduje możliwość integracji z AD oraz systemem klasy PAM.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

223.	5 i 6 str. 85. Monitorowanie i zarządzanie incydentami bezpieczeństwa1) Czy jest wymóg, aby wymieniane systemy bezpieczeństwa (WAF, FW, IDS/IPS, DLP itp.) były rozwiązaniami komercyjnymi?2)Jakie są wymagane wydajności dla tych rozwiązań?	Oczekujemy zaoferowania rozwiązań sklasyfikowanych w grupie wiodących (Leaders) bądź rokujących (Challengers) producentów wedle klasyfikacji firmy Gartner rok bieżący i poprzedni. Na potrzeby Dialogu należy przyjąć wymagania wydajności urządzenia stojącego na styku z Internetem zbliżone do Fortigate 300C. W systemie P1 wykorzystywane są urządzenia 4xFortiGate-6301F oraz 4xFortiGate-501E
224.	6. str. 8 Wymagania dot. bezpieczeństwa połączeń zewnętrznych" str. 81) Czy rozwiązania opensource są brane pod uwagę czy wyłącznie narzędzia komercyjne? 2) Czy dopuszczalne są rozwiązania hybrydowe (część w oparciu o opensource, a część w oparciu o rozwiązania zamknięte)?3) Czy istnieje wymóg wykorzystania urządzeń dedykowanych (np. serwery VPN) ?	Tak

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

225.	7. str. 97. Wymagania dotyczące zgodności w zakresie bezpieczeństwa. Prosimy o doprecyzowanie w jakiej części wymagania dotyczą dostawcy usług chmury(jej API/interfejsów)?, a w jakiej dostawcy oprogramowania uruchomionego/stworzonego na potrzeby CSIOZ? Prosimy o wyjaśnienie wsparcia np. dla Visual Studio czy Google API– w kontekście chmury IaaS / PaaS?	"Jedynie tej części, którą uczestnik dialogu powinien zarządzać dostarczając rozwiązanie: w usłudze Iaas - wszystko poniżej wirualizatoar, w usłudze PaaS wszystko poniżej orchestratora - odpowiedź należy czytać łącznie z odpowiedzią wydziału bezpieczeństwa o nazwie ""Dodatkowe wymagania"" z 11.10.2019 : """"W przypadku wyposażania infrastruktury teleinformatycznej środowiska chmurowego w rozwiązania klasy IPS/IDS, NGF, WAF, DLP (pkt. 5 podpunkt 3) oczekujemy zaoferowania rozwiązań sklasyfikowanych w grupie wiodących (Leaders) bądź rokujących (Challengers) producentów wedle klasyfikacji firmy Gartner rok bieżący i poprzedni. Dopuszczamy zarówno rozwiązania komercyjne, jaki i opensource pod warunkiem spełnienia naszych oczekiwań, jak i posiadania wsparcia producenta/suportu. Podstawowe założenia architektury bezpieczeństwa opieramy na wymaganiu, że zaproponowane rozwiązanie powinno uwzględniać fakt iż przestrzenie dyskowe, RAM, CPU dedykowane są wyłącznie dla CSIOZ. Dopuszczamy możliwość współdzielenia RAM, CPU, infrastruktury sieciowej wraz z urządzeniami bezpieczeństwa. W takim przypadku wymagane jest przeprowadzenie przez uczestnika dialogu analizy ryzyka opisującej możliwe zagrożenia, sposoby postępowania z nimi, aby bezpieczeństwo systemów IT CSIOZ, jak i przetwarzanych w nich danych było zagwarantowane na akceptowalnym przez nas poziomie. Analiza musi uwzględnić możliwe zagrożenia na warstwie hardware, software, jak i network. Dla przykładu, podatność w systemie innego klienta z którym będzie współdzielona infrastruktura może umożliwiać wydostanie się atakującego poza środowisko wirtualne tego klienta i umożliwić dostęp do zasobów CSIOZ po przejęciu maszyny fizycznej - w takim przypadku

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

226.		należy udzielić odpowiedzi jakie zabezpieczenia zostaną wdrożone aby nie dopuścić do takiego wariantu. Ponadto w przypadku współdzielenia środowisk oczekujemy wsparcia w przypadku incydentów bezpieczeństwa ze strony uczestnika dialogu wraz z zabezpieczeniem materiałów dowodowych znajdujących się we współdzielonej przestrzeni. Ze względu na istotność zasobów, które zamierzamy umieścić w chmurze oczekujemy bezzwłocznego reagowania na zlecenia wydziału bezpieczeństwa CSIOZ w zakresie zaleceń dotyczących konfiguracji np. blokada określonych adresów IP. Ponadto oczekujemy w takim wariancie pełnego monitoringu i rozliczalności użytkowników w środowisku nie zarządzanym przez CSIOZ. Nie dopuszczamy również możliwości fizycznego dostępu do elementów infrastruktury innych osób niż personel Wykonawcy tzn. inni klienci dzielący infrastrukturę nie mają prawa uzyskiwać dostępu fizycznego do infrastruktury. Wymagany jest również dostęp do wszystkich zdarzeń bezpieczeństwa w otoczeniu środowiska CSIOZ zarządzanych przez uczestnika dialogu. W tym celu oczekujemy wystawienia dedykowanego dashboard w systemie SIEM lub równoważnym, dostępu do konsoli IDS/IPS, NGF, WAF itd. W trybie read only w obszarze dedykowanym CSIOZ. W przypadku gdy środowisko uczestnika dialogu nie posiada takich możliwości prosimy o wskazanie alternatywnej metody dostępu do konfiguracji urządzeń, ustawionych alertów oraz alertów do w/w systemów. Prosimy o przedstawienia dwóch opcji ze współdzielonymi zasoby jak i bez współdzielonych zasobów.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

227.	,,Czy parametry dla rozwiązań FW oraz LB zawarte w pkt. 17 w dokumencie "Odpowiedzi na pytania do dialogu technicznego_Usługi chmurowe dla CSIOZ Część 3.pdf" są parametrami wymaganymi (np. minimalna przepływność FW 75 Gbps)? Tego rodzaju wydajność niesie wysoką cenę a z pozostałych parametrów nie wynika aby taka przepływność była potrzebne."	Podane parametry wydajnościowe oparte są o urządzenia aktualnie wykorzystywane w systemie P1. W przypadku migracji systemu P1 konieczne będzie zapewnienie infrastruktury nie gorszej niż aktualnie wykorzystywana.

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706