



Република Србија
МИНИСТАРСТВО ПРАВДЕ

Број: 404-02-51/2018-12/16
Датум: 11. фебруар 2019. године
Београд

На основу члана 63. став 3. Закона о јавним набавкама („Службени гласник РС“, бр. 124/12, 14/15 и 68/15), Комисија за јавну набавку припремила је

ДОДАТНЕ ИНФОРМАЦИЈЕ И ПОЈАШЊЕЊА
У ВЕЗИ СА ПРИПРЕМАЊЕМ ПОНУДЕ
у отвореном поступку јавне набавке услуга
- одржавање и унапређење комуникационе мреже правосуђа -
редни број 36/2018

на писани захтев заинтересованог лица, упућен путем електронске поште дана 8. фебруара 2019. године у 15.20 сати:

1. Питање заинтересованог лица:

Предмет јавне набавке су услуге одржавања и унапређења комуникационе мреже правосуђа. Самом конкурсном документацијом је дефинисано да опрема посредством које ће понуђач пружати услуге остаје у власништву понуђача, те да набавка саме опреме није предмет јавне набавке. Молимо за појашњење који је правни основ за прописивање техничких услова у погледу опреме посредством које ће бити пружане услуге, уместо дефинисања функционалности услуга одржавања и унапређења комуникационе мреже правосуђа из предмета јавне набавке. Конкретно, из ког разлога наручилац ограничава понуђаче којом опремом морају да пруже захтеване услуге, када је одговорност за пружање услуга, обезбеђивање опреме (која остаје у власништву понуђача) и функционалност и одржавање опреме искључива обавеза понуђача, а не наручиоца? Начин на који ће изабрани понуђач пружити услугу мора одговарати у потпуности техничким захтевима наручиоца у погледу услуга, што је неспорно. Међутим, строго дефинисање карактеристика опреме коју понуђач мора користити за реализацију опреме није у логичкој вези са предметом јавне набавке, нити представља дефинисање техничких спецификација у складу са Законом, обзиром да су предмет јавне набавке услуге, а не добра. Компаративним приступом, када наручилац набавља услугу интернета, он мора описати минималне техничке карактеристике саме услуге (брзину уплод и даунлоад-а, евентуално технологију преноса сигнала), а не и опреме посредством које ће му бити испоручена услуга, у ситуацији када не планира куповину и опреме уз услугу.

1. Одговор Комисије:

Наручилац нема у виду циљ да одређује конкретну опрему, већ само функционалност коју опрема треба да пружи. С тим у вези, прихватљиве су понуде опреме које ће пружити исте или боље функционалности. У супротном, Понуђачу би било дозвољено

да инсталира опрему квалитета који није одговарајући сервисима који се захтевају. На основу наведеног, Наручилац остаје при дефинисаним минималним функционалностима.

2. Питање заинтересованог лица:

Имајући у виду да сте у техничкој спецификацији представили технички опис тачно одређених произвођача опреме, изузев навођења произвођача опреме, уз додатне услове дефинисане на начин који ћемо појаснити у наредним питањима, недвосмислено указује на чињеницу одређивања услова које само одређени понуђач (односно група понуђача која је већ поднела понуду у ранијој фази овог поступка) може да испуни. Примера ради, технички параметри за мрежну баријеру са системом за заштиту од напада су копирани из произвођачке спецификације произвођача Фортинет за уређај Фортигате серије 200е, чији дата sheet прилажемо, а што је сваком стручњаку из области предмета јавне набавке јасно и врло лако доказиво. Слична је ситуација и за системе за заштиту од веб претњи и емаил саобраћаја, чији су параметри карактеристике опреме произвођача Форцепоинт (датасheet такође у прилогу), те молимо за појашњење који је интерес наручиоца да понуђач користи искључиво опрему ових произвођача?

2. Одговор Комисије:

Наручилац је Конкурсном документацијом дефинисао минималне карактеристике опреме коју треба понудити. То значи да Понуђач може да понуди опрему датих или бољих карактеристика. У техничким карактеристикама нису наведене својствене карактеристике које указују само на једног произвођача опреме, што отвара могућност да понуђачи могу да понуде опрему различитих произвођача.

3. Питање заинтересованог лица:

Техничком спецификацијом на страни 32-34 конкурсне документације описане су карактеристике уређаја/система мрежне баријере са системом за заштиту од напада. Обзиром на чињеницу да је предмет набавке услуга одржавање и унапређење комуникационе мреже правосуђа, молимо да појасните у каквој је логичкој вези и из којих разлога су технички захтеви у погледу карактеристика уређаја за овде описани уређај прилагођени спецификацији произвођача Fortinet серије Fortigate 200e. Наиме, ако је обавеза понуђача пружање услуге, посредством својих уређаја, који остају у власништву понуђача, захтев у погледу карактеристика уређаја није у логичкој вези са предметом јавне набавке те у том смислу техничка спецификација није сачињена на начин који је објективан и који одговара потребама наручиоца. Обзиром да наведене чињенице нису паушалне тврдње, прилажемо data sheet наведеног уређаја који потврђује циљано дефинисање тачно одређеног уређаја у техничкој спецификацији конкурсне документације. Производњом ИТ опреме која служи пружању предметних услуга баве се и други произвођачи, међу којима су, нпр. Cisco, Checkpoint i Palo Alto (Cisco i Checkpoint data sheet-ови се налазе у прилогу, а за Palo Alto се могу наћи на веб адреси <https://www.paloaltonetworks.com/products/product-selection.html>), међународно признати произвођачи опреме који покривају значајан део тржишта у производњи опреме за ову намену. Међутим, уређаји ових добављача по правилу не испуњавају апсолутно све услове које сте захтевали техничком спецификацијом, обзиром да су стандарди за сваког произвођача (који не утичу на квалитет услуге) другачији. Примера ради, да ли одређени уређај има 3 или 4 усб порта не утиче апсолутно никако на квалитет услуге за чију намену је произведен уређај, већ представља искључиву одлуку произвођача опреме о броју усб улаза. Као доказ наведеном, достављамо data sheet-ове поменутих произвођача ИТ опреме за уређаје/системе посредством којих се на адекватан начин може пружити услуга из предмета јавне набавке. У прилог изнетим чињеницама достављамо и извод из вештачења судског вештака за ИТ струку г-дина Драгана Стевановића (вештачено на околности које се тичу уређаја за које су data sheet-ови приложени или наведени линком)

који је уједно и сертификовани службеник за јавне набавке, вештак са листе вештака Републичке комисије за заштиту права у поступку јавних набавки, као и инжењер са лиценцом 353 што све доказује компетенције ангажованог стручњака. Приложеним вештачењем вештак је утврдио околност да су уређаји произвођача Cisco, модел Figerover 2130, такође адекватни за пружање услуге мрежне баријере са системом за заштиту од напада. Молимо и за појашњење из ког разлога су описани уређаји наведених произвођача, те због чега су дате карактеристике уређаја на које указујемо, ако наручилац набавља услугу, а одговорност за обезбеђивање и одржавање опреме је у домену понуђача?

3. Одговор Комисије:

Наручилац је Конкурсном документацијом дефинисао минималне карактеристике опреме коју Понуђачи треба да понуде. То значи да понуђачи могу да понуде опрему датих или бољих карактеристика, као што су, на пример: проток, број сесија, да подржава IPv6, URL филтрирање... У техничким карактеристикама нису наведене својствене карактеристике које указују само на једног произвођача опреме, што отвара могућност да понуђачи могу да понуде опрему различитих произвођача, као што су Palo Alto или Cisco. У вези са примером о броју USB портова, подвлачимо да је захтевом из конкурсне документације тражен 1 USB порт, а не 3 или 4, како се наводи у питању.

4. Питање заинтересованог лица:

На сличан начин, молимо за појашњење захтева у погледу уређаја за заштиту од web претњи и имејл саобраћаја, који су прекопирани опис уређаја произвођача Forcepoint (прилажемо data sheet-ове система овог произвођача који потврђују наводе)? Обзиром на кумулативно прописане услове у погледу техничких спецификација уређаја (произвођач Forcepoint), те услова у погледу техничког капацитета понуђача (мора доказати да је овлашћен за продају понуђених система на територији Републике Србије, имати статус партнера или ранија имплементација истог система), лако се на основу јавно доступних података доказује да тачно одређени понуђач из Београда једини испуњава оба услова. У прилог наведеноме говори чињеница да је управо тај понуђач доставио понуду у овом поступку са уређајима наведеног произвођача, те да на територији Србије представља јединог партнера овог произвођача (доказ досупан на интернет страници произвођача Forcepoint на линку: <https://www.forcepoint.com/partners/find-a-partner>). Дакле, услови који опредељују тачно одређеног произвођача опреме (без стриктног навођења робне марке) уз захтеван ниво партнерства кумулативно, када те услове испуњава само један понуђач, недвосмислено искључују било какву конкуренцију противно члановима 10. и 12. Закона о јавним набавкама.

4. Одговор Комисије:

У погледу опреме за заштиту од web и e-mail претњи, Наручилац сматра да је оптимално испоручити признато enterprise решење од истог произвођача, које има могућност да у будућности може да штити и од неовлашћеног одлива информација (DLP – data leak prevention). Ова функционалност је пожељна, али није неопходна за одабир Понуђача. Остале техничке карактеристике не указују само на једног произвођача опреме, што отвара могућност да понуђачи могу да понуде опрему различитих произвођача

5. Питање заинтересованог лица:

Молимо за појашњење из ког разлога је техничком спецификацијом захтевано да уређај/систем који је у власништву понуђача и служи за пружање услуге мрежне баријере са системом за заштиту од напада има минимум 2 RJ45 порта за менаџмент уређајем? Појашњења ради, RJ 45 менаџмент порт служи за управљање уређајем када

администратор уређаја (у овом случају понуђач) није у прилици да приступи даљинским путем уређају, већ се физички конектује са уређајем на лицу места преко RJ 45 менаџмент порта. Имајући у виду да је обавеза понуђача набавка и одржавање опреме и функционалност система, који је основ и техничка оправданост наручиоца за прописивањем оваквог услова? Коначно, избор понуђача је да, приликом пружања предметних услуга оптира за најефикаснији начин менаџмента уређајем, те тиме не би требало да се бави наручилац, нити је овлашћен да захтева одређени начин администрирања уређајем према тексту конкурсне документације. Из data sheet-ова уређаја, може се видети да 2 RJ45 менаџмент порта подржава уређај Fortinet произвођача из серије Fortigate 200E, док уређаји еминентних произвођача Cisco, Checkpoint и Palo Alto не укључују такву опцију. Са друге стране, према приложеном вештачењу, и уређај произвођача Cisco model Firepower 2130 је адекватан за пружање захтеваних услуга, те молимо и за појашњење да ли прихватате испоруку услуге посредством овог уређаја, чији је data sheet у прилогу и у вештачењу? Обзиром на чињеницу да наручилац има ангазоване стручњаке који располажу адекватним знањем за израду овако захтевне конкурсне документације, вероватно је и да ће бити у могућности да увиди доказану чињеницу да је и уређај произвођача Cisco подједнако адекватан за пружање услуге мрежне баријере са системом за заштиту од напада. По сличном принципу, молимо за појашњење да ли наручилац прихвата да се услуге заштите од веб претњи и имејл саобраћаја уместо Forcepoint уређајима пружају посредством Cisco Web Security Appliance са највисом Premium, корисничком лиценцом и Cisco Email Security Appliance са највисом Premium, корисничком лиценцом о којима се надлежни вештак изјаснио у достављеном вештачењу као о системима који су адекватни за пружање дефинисаних услуга? У противном, неспорно је ограничење конкуренције међу понуђачима са чиме сте и сами након увида у приложене доказе упознати.

5. Одговор Комисије:

У вези са тумачењем захтева за mgmt порт, сматрамо није исправно протумачен захтев. За потребе управљања које се наводе од стране стручњака, користио би се console порт, а не mgmt порт. Mgmt порт би се користио за потребе out-of-band надзора. Улога out-of-band мреже је да буде одвојена од продукционе мреже, како би услед пада мреже и даље био омогућен приступ уређају. Два захтевана mgmt порта су важна, како би Понуђач што квалитетније отклањао сметње у мрежи. Оба порта треба да буду RJ45, од чега један порт мора да буде console, а други гигабитни.

6. Питање заинтересованог лица:

У погледу уређаја/система мрежне баријере са системом за заштиту од напада захтевано је техничком спецификацијом да уређај мора подржавати експлицитни проху начин рада. Експлицитни проху начин рада је сервис који омогућава одређени степен контроле, кеширања садржаја којима приступају рачунари из локалне мреже. По природи ствари и правилима струке, за функционисање система и пружање предметних услуга ову опцију је битно да подржава систем/уређај за заштиту од веб претњи. Конкурсном документацијом је у погледу система/уређај за заштиту од веб претњи већ захтевана могућност рада у експлицитном проху режиму те је наведени услов за уређај/систем мрежне баријере са системом за заштиту од напада сувишан, непотребан у погледу квалитета услуге и није у логичкој вези са системом мрежне баријере са системом за заштиту од напада, јер, како је наведено, наведену функционалност обезбеђује систем/уређај за заштиту од веб претњи. Молимо да размотрите измену конкурсне документације и уклоните овај захтев у погледу уређаја/система мрежне баријере са системом за заштиту од напада јер исти није у логичкој вези са овим системом/уређајем и представља дефинисање конкурсне документације супротно одредбама Закона о јавним набавкама.

6. Одговор Комисије:

Експлицитни проху начин рада уређаја преставља начин обраде пакета и није везан за то да ли је заштита од Web претњи или неких других сигурносних претњи, те Наручилац остаје при овом захтеву.

7. Питање заинтересованог лица:

Законом о јавним набавкама, у члану 54. прописан је обавезан састав комисије за јавну набавку код наручиоца. Ставом 7. цитираног члана, прописано је „За чланове комисије се именују лица која имају одговарајуће стручно образовање из области из које је предмет јавне набавке”, док је ставом 8. истог члана прописано „Ако наручилац нема запослено лице које има одговарајуће стручно образовање из области из које је предмет јавне набавке, у комисију се може именовати лице које није запослено код наручиоца”. Како је комисија за јавне набавке у овом поступку код наручиоца састављена од 5 дипломираних правника и једног дипл. инжењера организације рада, молимо да појасните који од чланова комисије има одговарајуће стручно образовање из области из које је предмет јавне набавке? Подсећамо да су неке од обавеза комисије за јавну набавку, према члану 54. Закона: „припрема конкурсну документацију, огласе о јавним набавкама, измене или допуне конкурсне документације, додатне информације или објашњења у вези са припремањем понуда или пријава”. Сагласно наведеном, за израду конкурсне документације, те давање адекватних, стручних и поузданих одговора и појашњења у јавној набавци чији је предмет одржавање и унапређење комуникационе мреже правосуђа, сагласно Закону је нужно да један од чланова комисије има одговарајуће стручно образовање (степен стручног образовања, а не искуство у пракси је интенција Законодавца) из области ИТ струке, те се поставља питање правне ваљаности конкурсне документације, досадашњих објављених појашњења конкурсне документације, као и свих предузетих радњи у поступку ове јавне набавке.

7. Одговор Комисије:

Чланом 54. став 7. Закона о јавним набавкама прописано је да се за чланове комисије именују лица која имају одговарајуће стручно образовање из области из које је предмет јавне набавке. Ставом 8. истог члана прописано је да ако наручилац нема запослено лице које има одговарајуће стручно образовање из области из које је предмет јавне набавке, у комисију се може именовати лице које није запослено код наручиоца. Дакле, наручилац нема обавезу да, уколико нема лице које има одговарајуће стручно образовање из области из које је предмет јавне набавке, у комисију именује лице које није запослено код наручиоца а које има одговарајуће стручно образовање из области из које је предмет јавне набавке. Напомињемо, такође, да лица која чине комисију имају доказано вишегодишње искуство у раду на пословима које чине предмет набавке, да имају адекватно формално образовање, те да су додатно сертификовани за обављање послова прописивања критеријума и праћења реализације извођења радова на развоју и одржавању информационалних система.

У наставку су неки од сертификата које поседују чланови Комисије, а односе се на области релевантних стандарда:

Марио Малетић:

ISO/IEC 20000: 2011 Information technology – Service management – Part 1: Service management system requirements,

ISO 22301: 2012 Societal security – Business continuity management systems - Requirements

ISO/IEC 27001: 2013 Information technology – Security techniques – Information security management systems - Requirements

ISO 31000: 2009 Risk management – Principles and guidelines

ISO 21500: 2012 Guidance on project management

Владимир Пејчић:

ISO/IEC 20000: 2011 Information technology – Service management – Part 1: Service management system requirements,

ISO 22301: 2012 Societal security – Business continuity management systems - Requirements

ISO/IEC 27001: 2013 Information technology – Security techniques – Information security management systems - Requirements

ISO 31000: 2009 Risk management – Principles and guidelines

ISO 21500: 2012 Guidance on project management

ISO/IEC 27001 Lead Auditor

Ана Ђилас (девојачко Милошевић):

ISO 21500:2012 Guidance on project management

ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements

ISO 31000:2009 Risk management – Principles and guidelines

ISO/IEC 27001 Lead Auditor

ECDL/ICDL Advanced Word, Spreadsheets, Database, Presentation.

Гордана Лазић, дипломирани инжењер организације рада (Организационо-кибернетски смер):

ISO/IEC 20000: 2011 Information technology – Service management – Part 1: Service management system requirements,

ISO 22301: 2012 Societal security – Business continuity management systems - Requirements

ISO/IEC 27001: 2013 Information technology – Security techniques – Information security management systems - Requirements

ISO 31000: 2009 Risk management – Principles and guidelines

8. Питање заинтересованог лица:

Као додатни услов у смислу члана 76. ЗЈН-а, за учествовање у поступку јавне набавке је захтевано да понуђач располаже одређеним кадровским капацитетом. Доказ о испуњености наведеног услова је достављање: пријаве на обавезно социјално осигурање и уговора о раду или потврда послодавца о врсти радног односа или уговора о делу или уговора о допунском раду или уговора о привременим и повременим пословима. Да ли је у случају ангажовања по основу уговора о делу довољно, уговора о допунском раду или уговора о доставити само уговор о делу, или уговора о привременим и повременим пословима довољно доставити само наведене уговоре или је потребно достављати и неки додатни доказ: потврду послодавца и сл.?

8. Одговор Комисије:

Као што је наведено у Конкурсној документацији у делу III УСЛОВИ ЗА УЧЕШЋЕ У ПОСТУПКУ ЈАВНЕ НАБАВКЕ ИЗ ЧЛ. 75. И 76. ЗЈН И УПУТСТВО КАКО СЕ ДОКАЗУЈЕ ИСПУЊЕНОСТ ТИХ УСЛОВА 2. додатни услови тачка 7. Кадровски капацитет ДОКАЗА О ПРАВНОМ ОСНОВУ РАДНОГ АНГАЖОВАЊА -пријава на обавезно социјално осигурање и уговор о раду (одређено или неодређено време) **или** потврда послодавца о врсти радног односа **или** уговор о делу **или** уговор о допунском раду **или** уговор о привременим и повременим пословима.

9. Питање заинтересованог лица:

Као додатни услов у смислу члана 76. ЗЈН-а, за учествовање у поступку јавне набавке је захтевано да понуђач поседује инсталирану Provider Edge мрежну опрему IP/MPLS мреже на минимално 80% локација из табеле Г конкурсне документације. Пре свега, указујемо на злоупотребу овлашћења из ЗЈН-а дефинисањем предметног услова на

наведени начин из разлога што је апсолутно неоправдано захтевати од понуђача да пре доделе и закључења уговора о ЈН располажу предметном опремом на локацијама (адресама) наручиоца. Поврх тога, као доказ о испуњености овог услова је захтевано достављање потврде од стране испоручиоца IP/MPLS Provider Edge мрежне опреме да је опрема у складу са RFC 4364 BGP/MPLS IP VPN, у складу са потписаним уговором са испоручиоцем на минимално 80% локација наведених у табели Г. Молимо и за појашњење на који начин испоручилац било које опреме може знати тачну локацију опреме коју након извршене продаје купац инсталира на жељеним локацијама. На који начин је наручилац у могућности да на основу потврде чију истинитост објективно не може да провери у могућности да приликом стручне оцене понуда утврди да понуђач располаже наведеним техничким капацитетом? Коначно, по ком основу наручилац захтева да понуђач има инсталирану опрему на локацијама наручиоца, те по ком правном основу би понуђач уопште могао да приступи локацијама наручиоца ради инсталације наведене опреме, пре закључења уговора о јавној набавци?

9. Одговор Комисије:

Према констатацији садржаној у питању, наводи се да се Provider Edge (PE) рутери налазе на локацији Наручиоца, што представљају клијентски SE рутери. Provider Edge рутери се налазе у мрежи провајдера и они су повезани са клијентским рутерима који се налази на локацији корисника.

Наручилац захтева ВПН повезивање преко ИП/МПЛС мреже провајдера, што управо представља да су Provider Edge (PE) рутери имплементирани по моделу ИП ВПН сервиса заснованог на RFC 4364 (BGP / MPLS VPN). RFC 4364 (BGP / MPLS VPN) је IETF стандард за ВПН (виртуелне приватне мреже) на нивоу 3, што пружа могућност повезивања наших локација у једну заштићену и функционалну мрежу а то се представља: у пуној мрежну повезаност између локација, у могућности више ВПН-ова на локацији са различитим путевима за контролу и приступ и у олакшавању комуникације у нашој динамичној организацији и окружењу заштићених пословних апликација. MPLS / BGP VPN технологија (RFC 4364) се показала способном да прилагоди великом броју ВПН-овима и корисникове путање саобраћаја, док истовремено осигурава агрегатне способности управљања И безбедности. MPLS / BGP VPN-ови (RFC

4364) пружа сигурну повезаност између локација у широкој мрежи, што је значајно за институцију која обавља послове државне управе од значаја и са локацијама распоређеним широм Републике Србије.

MPLS / BGP VPN (RFC 4364) приступ може пружити додатне могућности у поређењу са било којим другим начином повезивања као што су:

1. QoS : data, voice и видео конвергирају на једној мрежи и MPLS / BGP VPN (RFC 4364) технологија може најбоље осигурати тип саобраћаја од критичне важности и осетљиве на кашњење

2. Високу доступност и скалабилност: подржава ВПН-ове великих величина, распоређивање и имплементацију базирану на MPLS-у (RFC 4364) обезбеђује лаку промену, раст и миграције у нашој организацију тако што додавање нове локације код MPLS захтева само успостављање reeving-а између Провајдера и нове локације и не захтева промене конфигурације на другим локацијама.

Такође, отвара могућност усмеравање информације односно да по ВПН-у може да се тражи одвајање саобраћаја у зависности од локације и раздвајање са рутним табелама на PE рутерима

3. Сигурност мреже: саобраћај Министарства правде не сме се излагати интернету, и на тај начин не сме се оставити могућност повезивања интернетским ИП ВП тунелима који пате од сигурносних проблема и недостатка гаранција за горе наведене перформансе.

Због наведеног и у циљу квалитетног сервиса на захтеваном нивоу за L3VPN, сва наведена усмеравања се одвијају на рутерима Пружиоца услуга, односно на PE

рутерима провајдера сервиса који морају да складиште и обрађују путање корисничког саобраћаја, а управо ПЕ рутери су базирани на RFC 4364, BGP / MPLS виртуелним приватним мрежама, а испоручилац опреме треба да је у могућности да потврди да иста подржава тражени RFC механизам за пружање VPN услуга Layer 3 на начин који омогућава најбољи избор за мрежну функционалност Наручиоца.

10. Питање заинтересованог лица:

Техничким спецификацијама је, у односу на претходну верзију конкурсне документације, измењен захтев у погледу система за детекцију, спречавање и извештавање о DDoS нападима на мрежу на начин да је сада захтевано да комплетна инфраструктура система за заштиту треба да се налази у сервисној мрежи понуђача у Републици Србији. Као што је неспорно познато наручиоцу, услугу детекције, спречавања и извештавања о DDoS нападима на мрежу је подједнако ефикасно могуће пружити и системом који је заснован на клауд решењу у ком случају је небитна географска локација опреме, такве услуге заштите мреже се редовно пружању државним органима (Министарство правде, Управа за трезор, Министарство рада, Градска управа Града Београда чији је рад такође од виталног значаја за функционисање државне управе. Штавише, сам наручилац годинама уназад користи услугу детекције, спречавања и извештавања о DDoS нападима на мрежу системом који је заснован на клауд решењу, без икаквог приговора на рад система (наручиоцу познато, по потреби и лако доказиво). Молимо за појашњење који је мотив наручиоца за оваквом изменом управо након подношења понуда у ранијој фази поступка, те за техничко образложење овакве измене конкурсне документације у погледу предметног система. Уједно указујемо и да ограничавање конкуренције и израда техничких спецификација на овакав начин представља повреду одредаба Закона о јавним набавкама. Даље, доказ о могућности пружања услуга детекције, спречавања и извештавања о DdoS нападима на мрежу и испуњењу услова из члана 76. ЗЈН-а је фотокопија фактуре или уговора о куповини уређаја или фотокопија фактуре и документ којим је описана техничка спецификација уређаја/система, као и изјава одговорног лица понуђача или потврда испоручиоца система да је инсталирана комплетна инфраструктура система за ДДоС заштиту у сервисној мрежи понуђача. Молимо за појашњење због чега је за наручиоца битан правни основ коришћења система за заштиту од DdoS напада? Како је наручилац и на основу којих овлашћења дефинисао да једино власник наведеног система може пружити предметну услугу, а да то није у могућности да учини на пример оператор који такав систем користи на основу уговора о дугорочном закупу или неког другог правног посла? На који начин и којим методом при стручној оцени понуда је наручилац у могућности да оцени да предметни услов за учествовање у поступку јавне набавке у смислу чл. 76. ЗЈН-а може да испуни једино власник таквог система, а не и понуђач који таквим системом располаже по другом правном основу? Посебно напомињемо да је понуђач којем буде додељен уговор о ЈН у обавези да достави банкарску гаранцију као средство финансијског обезбеђења за уредно извршење посла, да сноси и последицу негативне референце у случају раскида уговора о ЈН због неизвршења обавеза, те да ниједном понуђачу није у интересу да достави понуду за уговор који није у могућности да реализује.

10. Одговор Комисије:

У конкурсној документацији наводи се тип заштите од напада и брзина линка коју мора да поседује уређај преко кога иде заштита. На тржишту постоје другачији видови заштите од DDoS напада којима се пружа заштита, али који су по питању безбедности лошији од траженог захтева. Пружање заштите од DDoS напада код оператора који такав систем користи на основу уговора о дугорочном закупу уговора а који може да се налази било где па чак и у иностранству је лоше у погледу кашњења (латенције), тако

да се не можемо сложити да је за систем за заштиту од DDoS напада небитна географска локација опреме. За поједине типове напада то може представљати изузетан проблем.

Наручилац и у овом случају поступа у складу са Законом о заштити података о личности и другим релевантним прописима, заузимајући важно место у систему заштите личних података грађана. Са техничког аспекта, за тражени систем за заштиту који треба да има могућност филтрирања, односно ублажавања последица напада наведеног капацитета нежељеног саобраћаја није прихватљиво да се обавља ван територије Републике Србије. Разлог томе је што би у супротном био случај да у долазном, регуларном смеру саобраћаја, пакети морају да прођу кроз опрему и системе других или можда чак иностраних провајдера при чему је могуће да се изврши инспекција пакета и обави увид у њихов садржај, а самим тим нема више никакве контроле од стране Понуђача када пакет изађе из његове сервисне мреже, могуће и из Републике Србије. Захтев Наручиоца представља логичнији избор с обзиром на то да се тражи да се комплетна инфраструктура и пропратни софтвер за заштиту налази у Републици Србији и да се налази у самој мрежи Понуђача, што даље повлачи чињеницу да не постоји зависност од других провајдера/оператора.

Наручилац може да се сложи да заштита од DDoS напада ради у “cloud” режиму при чему мора да задовољава тражене техничке карактеристике наведене у конкурсној документацији, али да свакако остаје при томе да треба да се налази на територији Републике Србије и да је у мрежи Понуђача. Дакле, Наручилац остаје при захтеву из конкурсне документације.

Комисија за јавну набавку

- Марио Малетић, дипломирани правник;
- Владимир Пејчић, дипломирани правник;
- Жељка Дрчелић, дипломирани правник, службеник за јавне набавке;
- Гордана Лазих, дипломирани инжењер организације рада;
- Ана Ђилас, дипломирани правник;
- Јована Анђелковић, дипломирани правник, службеник за јавне набавке.

објавити на:

- Порталу јавних набавки
- интернет страници наручиоца