

Informatīvais ziņojums "Par Centrālās vēlēšanu komisijas e-pakalpojuma "2018. gada Saeimas vēlēšanu organizēšana" nodrošināšanu"

Informatīvais ziņojums izstrādāts, ņemot vērā Ministru prezidenta 2018. gada 31. maija rezolūciju Nr. 45/SAN-752 (turpmāk – rezolūcija) un Finanšu ministrijas 2018. gada 27. jūnija vēstuli Nr. 3.2-4/2-3/3019 "Par Ministru prezidenta 2018. gada 31. maija rezolūciju Nr. 45/SAN-752" (turpmāk – FM vēstule). Rezolūcijā tika lūgts Vides aizsardzības un reģionālās attīstības ministrijai (turpmāk – VARAM) izvērtēt e-pakalpojuma "2018. gada Saeimas vēlēšanu organizēšana" (turpmāk – vēlēšanu e-pakalpojums) nodrošināšanai paredzētos papildu drošības pakalpojumu risinājumus un provizoriskās izmaksas.

1. Esošā situācija

2017. gada 13. septembrī Centrālā vēlēšanu komisija (turpmāk – CVK) izsludināja aptauju par paredzamo līgumcenu atklātam konkursam "E-pakalpojums: Saeimas un Eiropas Parlamenta vēlēšanu organizēšana" ar piedāvājumu iesniegšanas termiņu līdz 2017. gada 6. oktobrim. 2017. gada 6. oktobrī SIA "SOAAR" iesniedza piedāvājumu ar līgumcenu 207 000 – 352 000 *euro* bez PVN (250 470 – 425 920 *euro* ar 21% PVN). Šī līgumcena tika aprēķināta, balstoties uz cenu aptaujā izvirzītajām prasībām un nosacījumiem. Papildus tika pievienota norāde, ka šī līgumcena ir atkarīga no tehniskajām, organizatoriskajām, drošības un citām izvirzītajām prasībām.

2017. gada 16. novembrī tika izsludināts CVK iepirkums "E-pakalpojums: 2018. gada Saeimas vēlēšanu organizēšana", iepirkuma ID Nr. CVK2017/02, ar piedāvājumu iesniegšanas termiņu līdz 2017. gada 20. decembrim. SIA "SOAAR" sagatavoja un iesniedza piedāvājumu ar minimālo iespējamo līgumcenu 208 585 *euro* bez PVN (252 387,85 *euro* ar 21% PVN). Šī līgumcena tika aprēķināta, balstoties uz iepirkumā izvirzītajām konkrētajām prasībām un nosacījumiem. Saskaņā ar iepirkuma dokumentāciju iepirkuma priekšmets ir vēlēšanu e-pakalpojums, kura ietvaros pretendents, izmantojot informācijas sistēmu, atbilstošu tehnisko infrastruktūru un kompetentus speciālistus, jānodrošina sekojoši vēlēšanu procesi 2018. gada Saeimas vēlēšanām:

1. Kandidātu sarakstu iesniegšana.
2. Vēlēšanu zīmju maketu sagatavošana.
3. Elektronisks vēlēšanu gaitas žurnāls.
4. Vēlētāju aktivitātes un nobalsojušo konstatēšana, publicēšana.
5. Vēlēšanu rezultātu konstatēšana, publicēšana.
6. Operatīvie un statistiskie vēlēšanu procesu pārskati.
7. Elektroniska vēlēšanu datu arhivēšana.
8. Vēlēšanu procesu tehniskā pavadīšana.
9. Tehniskās infrastruktūras nodrošināšana.

Iepirkuma rezultātā tika saņemts tikai viens piedāvājums no SIA "SOAAR". 2018. gada 5. janvārī tika noslēgts līgums Nr. CVK/01-2018 starp CVK un SIA "SOAAR" par vēlēšanu e-pakalpojuma nodrošināšanu. Lai nodrošinātu vēlēšanu e-pakalpojumu, atbilstoši SIA "SOAAR" sniegtajai informācijai tiek izmantota SIA "SOAAR" izstrādātā vēlēšanu organizēšanas un pārvaldības informācijas sistēma Balsis (turpmāk – Vēlēšanu sistēma). Ar Ministru kabineta 2018. gada 26. marta rīkojumu Nr.119k "Par kritiskās infrastruktūras kopumu" tika pieņemts lēmums Vēlēšanu sistēmai piešķirt kritiskās infrastruktūras (turpmāk – KI) statusu, kā rezultātā atbilstoši Ministru kabineta 2015. gada 28. jūlija noteikumiem Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" (turpmāk – MKN 442), Ministru kabineta 2010. gada 1. jūnija noteikumiem Nr. 496 "Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un

Rekomendāciju pamatojums: VARAM

08.03.2018. vēstule

Nr. 1-13/1573

1. Stafecka

05.02.2018.

īstenošanas kārtība” un Ministru kabineta 2011. gada 1. februāra noteikumiem Nr. 100 “Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība” palielinājās drošības prasības vēlēšanu e-pakalpojuma nodrošināšanai. Jānorāda, ka tieša atbilstība MKN 442 neizriet, taču pēc būtības prasības, kuras ir noteiktas paaugstinātas drošības sistēmām ir izvirzāmas arī sistēmām, kurām ir piešķirts kritiskās infrastruktūras statuss. CVK sadarbībā ar SIA “SOAAR”, Informācijas tehnoloģiju drošības incidentu novēršanas institūciju (turpmāk - CERT.LV) un Satversmes aizsardzības biroju izvērtēja vēlēšanu e-pakalpojuma atbilstību jaunajām drošības prasībām, kā rezultātā tika secināts, ka:

1. Jāpilnveido Vēlēšanu sistēma un jānodrošina vēlēšanu e-pakalpojums atbilstoši drošības prasībām, kādas izvirzītas KI un pakalpojumiem.

2. Jāveic atbilstoši papildu drošības pasākumi un jāīsteno risinājumi, lai nodrošinātu Vēlēšanu sistēmas un vēlēšanu e-pakalpojuma kvalitatīvu aizsardzību pret potenciālajiem kiberuzbrukumiem.

Rezultātā SIA “SOAAR” nosūtīja CVK 2018. gada 23. aprīļa vēstuli Nr. 180423-1 “Par e-pakalpojuma “2018. gada Saeimas vēlēšanu organizēšana” nodrošināšanu”, kurā norādīja uz papildu nepieciešamajām pasākumiem saistībā ar izvirzītajām papildu drošības prasībām un atbilstošām papildu izmaksām. Ņemot vērā iesniegto informāciju, CVK nosūtīja Latvijas Republikas Ministru prezidentam 2018. gada 23. maija vēstuli Nr. 02-01.7/130e “Par Saeimas vēlēšanu nodrošināšanai nepieciešamo papildu finansējumu” ar lūgumu rast iespēju piešķirt papildu finansējumu Saeimas vēlēšanu nodrošināšanai 2018. gadā. Lai risinātu radušos problēmu, tika izdota rezolūcija, kurā tika lūgts VARAM izvērtēt vēlēšanu e-pakalpojuma nodrošināšanai paredzētos papildu drošības pakalpojumu risinājumus un provizoriskās izmaksas, bet Finanšu ministrijai sadarbībā ar VARAM sagatavot un noteiktā kārtībā kā Ministru kabineta lietu iesniegt attiecīgu tiesību akta projektu.

VARAM iepazīnās un izvērtēja informāciju, kura tika sniegta SIA “SOAAR” 2018. gada 23. aprīļa vēstulē Nr. 180423-1 “Par e-pakalpojuma “2018. gada Saeimas vēlēšanu organizēšana” nodrošināšanu”, CVK un SIA “SOAAR” 2018. gada 5. janvāra līgumā Nr. CVK/01-2018 un līguma 1. pielikumā “Tehniskā specifikācija “E – pakalpojums: 2018. gada Saeimas vēlēšanu organizēšana””. Izvērtējuma rezultātā VARAM 2018. gada 7. jūnija vēstulē Nr. 1-13/5175 “Par papildus informācijas sniegšanu” lūdza CVK precizēt nepieciešamo papildu drošības pasākumu sarakstu un pieprasīt papildu finansējuma apjomu. Ņemot vērā CVK 2018. gada 12. jūnija vēstulē Nr. 01-02.7/142e sniegto atbildi, VARAM savas kompetences ietvaros atbalstīja papildu drošības risinājumus un to provizoriskās izmaksas.

Lai nodrošinātu vēlēšanu e-pakalpojuma atbilstību papildu drošības prasībām pilnā apmērā, tika paredzēts nodrošināt sekojošus papildus pasākumus Vēlēšanu sistēmas un vēlēšanu e-pakalpojuma drošības paaugstināšanai, kuriem provizoriski bija nepieciešams papildu finansējums 343 701 *euro* ar 21% PVN:

1. Vēlēšanu sistēmas un tajā ietvertu visu apakšsistēmu drošības un informācijas aizsardzības audits pakalpojuma nodrošināšanas kontekstā, kā arī vēlēšanu e-pakalpojuma organizācijas drošības un informācijas aizsardzības audits atbilstoši aktuālajiem standartiem (piemēram, ISO 27002, 27001 vai līdzīgi).

2. Vēlēšanu sistēmas un tajā ietvertu visu apakšsistēmu drošības papildinājumi atbilstoši kritiskās infrastruktūras informācijas sistēmu drošības prasībām un vēlēšanu nodrošināšanai paaugstinātu kiberuzbrukuma risku apstākļos, t.sk.:

- MKN 442 8.2. - 8.5. apakšpunktos un 24. - 36. punktos noteikto prasību realizācija paaugstinātas drošības sistēmām.

- Sertifikātu izplatīšanas drošības paaugstināšana.
- Datu papildu šifrēšana.
- Kontrolsummu realizēšana vēlēšanu zīmju skenējumiem.
- Auditācijas pierakstu paplašināšana, atdalīšana no sistēmas.

- Audita rezultātā identificēto papildinājumu un drošības pasākumu realizācija.
- 3. Vēlēšanu e-pakalpojuma drošības un noturības paaugstināšanas pasākumi.
- 4. Vēlēšanu sistēmas un tajā ietverto visu apakšsistēmu ieviešanas un pārvaldības administrators.
- 5. Drošības incidentu speciālists visā vēlēšanu e-pakalpojuma periodā. Risku pārvaldība.
- 6. Krīzes komunikācijas plāna izstrāde, krīzes komunikācijas vadība.
- 7. Vēlēšanu sistēmas izstrādes vides un uzturēšanas vides drošības un informācijas aizsardzības audits atbilstoši aktuālajiem standartiem (piemēram, ISO 27002, 27001 vai līdzīgi), identificēto risku analīze, risku minimizēšanas pasākumu noteikšana.
- 8. Vēlēšanu sistēmas izstrādes un uzturēšanas vides tehniskās infrastruktūras ārējās ievainojamības skenēšana.
- 9. Vēlēšanu sistēmas izstrādes un uzturēšanas vides tehniskās infrastruktūras drošības paaugstināšana atbilstoši kritiskās infrastruktūras informācijas sistēmu drošības prasībām.
- 10. Vēlēšanu sistēmas izstrādes un uzturēšanas drošības politikas izstrāde un ieviešana atbilstoši kritiskās infrastruktūras informācijas sistēmu drošības prasībām.

Nemot vērā, ka līdz 2018. gada 6. oktobrī paredzētajām 13. Saeimas vēlēšanām ir atlicis ierobežots laiks, SIA "SOAAR" sadarbībā ar Latvijas valsts drošības iestādēm un CERT.LV ir identificējusi kritiskākos papildus pasākumus Vēlēšanu sistēmas un vēlēšanu e-pakalpojuma drošības paaugstināšanai, kuriem provizoriski nepieciešams papildu finansējums 225 786 euro ar 21% PVN:

Nr.	Pasākuma nosaukums	Izmaksas euro bez PVN
1.	Vēlēšanu sistēmas un tajā ietverto visu apakšsistēmu drošības papildinājumi (sistēmas izstrādes darbi) atbilstoši kritiskās infrastruktūras informācijas sistēmu drošības prasībām un vēlēšanu nodrošināšanai paaugstinātu kiberuzbrukuma risku apstākļos:	143 600
1.1.	Autentifikācijas drošības paaugstināšana:	85 100
1.1.1.	Servera bāzētas autentifikācijas realizācija, sistēmas lietotāju pārvaldības centralizēšana sistēmas blokiem.	25 000
1.1.2.	Sistēmas lietotāju divu faktoru autentifikācijas pastiprināšana, OTP (<i>one time password</i>) ieviešana.	17 000
1.1.3.	Lietotāju pārvaldības ķēdes minimizēšana, lietotāju pārvaldības deleģēšanas novadiem un pilsētām realizācija.	13 000
1.1.4.	Lokālās sesijas realizācija.	2 000
1.1.5.	Sertifikātu izplatīšanas drošības paaugstināšana.	17 000
1.1.6.	Iecirkņa, novada, pilsētas sistēmas droša izplatīšanas kanāla ieviešana.	5 500
1.1.7.	Sertifikāta obligāta lietošana visos posmos viesiem scenārijiem.	2 000
1.1.8.	Iecirkņa, novada, pilsētas izpildmoduļa parakstīšana.	2 600
1.1.9.	Viena lietotāja servera sesiju skaita ierobežošanas konfigurācija.	1 000
1.2.	Datu papildus šifrēšana:	34 000
1.2.1.	Iecirkņa, novada, pilsētas sistēmas lokālās datubāzes šifrēšana.	7 000
1.2.2.	Kontrolsummu ieviešana vēlēšanu procesu posmos, kontrolsummu pārbaudi intensificēšana.	5 500
1.2.3.	Slēpta taga ieviešana vēlēšanu zīmju skenējumos.	3 500

~~DIENESTA VAJADZĪBĀM~~

1.2.4.	Ārvalstu iecirkņiem jebkura skenera izmantošanai vēlēšanu zīmju skenējumu agrīna ievietošana lokālajā datubāzē.	2 000
1.2.5.	Vēlēšanu zīmju skenējumu šifrēšana lokālajā datu bāzē.	2 500
1.2.6.	Vēlēšanu zīmju skenējumu automātiska augšupielāde un centralizēta apkopošana.	13 500
1.3.	Auditācijas pierakstu paplašināšana, atdalīšana no sistēmas:	14 000
1.3.1.	Auditācijas pierakstu izvietošana uz atsevišķi izdalītas servera iekārtas.	2 700
1.3.2.	Rindas mehānisma realizēšana.	5 500
1.3.3.	Auditācijas pierakstu transformēšana analizējamā, vizuālā formātā ar rīkiem Elastic/Kibana.	5 800
1.4.	Datu, darbību monitorings:	8 500
1.4.1.	Sistēmas telemetrijas paplašināšana - ievietošana datubāzē reālā laikā.	3 500
1.4.2.	Sistēmas telemetrijas datu vizualizācija.	5 000
1.5.	Ārējās ievainojamības skenēšana (Vulnerability Assessment) (turpmāk – VA) rezultātā konstatēto ievainojamību novēršana.	2 000
2.	Vēlēšanu e-pakalpojuma drošības un noturības paaugstināšanas pasākumi:	8 300
2.1.	Sistēmas un datu rezerves kopiju nodrošināšanas pasākumi.	2 500
2.2.	Sistēmas un lietotāju monitorings.	2 800
2.3.	Papildus pasākumi, kas tiks identificēti VA skenēšanas rezultātā.	3 000
3.	Vēlēšanu sistēmas un tajā ietvertu visu apakšsistēmu ieviešanas un pārvaldības administrators.	3 200
4.	Drošības incidentu speciālists visā vēlēšanu e-pakalpojuma periodā. Risku pārvaldība.	23 500
4.1.	Risku analīze, pārvaldība drošības aspektos.	12 000
4.2.	Sistēmas un infrastruktūras papildinājumu, izmaiņu vērtēšana drošības aspektos.	1 500
4.3.	Papildus drošības testi.	10 000
5.	Krīzes komunikācijas plāna izstrāde, krīzes komunikācijas vadība.	4 500
6.	Vēlēšanu sistēmas pakalpojuma produkcijas vides, izstrādes un uzturēšanas vides tehniskās infrastruktūras ārējās ievainojamības skenēšana (VA), t.sk. atkārtota skenēšana.	3 500

Pozīcijām 1.5. un 2.3. papildus finansējums var tikt neizmantots, ja VA rezultātā netiks konstatētas ievainojamības.

CERT.LV savā 2018.gada 5.jūlija ziņojumā “Par CVK elektroniskās balsu skaitīšanas sistēmu” ir informējusi, ka ASV, Vācijas, Francijas un citu valstu pieredze pēdējo 3 gadu laikā rāda, ka ir identificēta mērķtiecīga Krievijas Federācijas kompleksu ofensīvu operāciju tendence ar mērķi ietekmēt vēlēšanu norisi, politisko apvienību vai atsevišķu kandidātu tēlus, veikt informācijas operācijas un citas ar IKT saistītas darbības, lai panāktu sev interesējošus rezultātus vai grautu sabiedrības uzticību vēlēšanu procesam.

~~DIENESTA VAJADZĪBĀM~~

Ņemot vērā CERT.LV 2018.gada 5.jūlija ziņojumā "Par CVK elektroniskās balsu skaitīšanas sistēmu" sniegto informāciju, Latvijas valsts drošības iestādes un CERT.LV ir veikušas atkārtotu, virspusēju novērtējumu, kura rezultātā konstatētas sekojošas problēmas:

1. Elektroniskās balsu skaitīšanas procesos izmantotajām datorsistēmām vēlēšanu iecirkņos nav noteiktas prasības vai minimālie drošības nosacījumi. CERT.LV vērtējumā tas ir liels risks, kas apdraud elektroniskās balsu skaitīšanas rezultātu integritāti, un var apdraudēt arī konfidencialitāti un pieejamību. Šobrīd ir secināts, ka nav nekādu šķēršļu, lai potenciālais uzbrucējs savlaicīgi sagatavotos uzbrukumam, speciāli vēlēšanu balsu skaitīšanai aprīkojot portatīvo datoru, un šādā veidā jebkurā iecirknī sagādātu vēlēšanu procesam traucējošu, speciāli aprīkotu iekārtu. CERT.LV šobrīd ir piedāvājis vairākus tehnoloģiskos risinājumus dārgākais no kuriem provizoriski varētu izmaksāt aptuveni vienu miljonu *euro*.

2. Nepieciešams veikt neatkarīgus drošības un sistēmas biznesa procesu auditus, lai CVK un CERT.LV gūtu pārliecību, ka izstrādātās sistēmas un saistītie funkcionālie mezgli darbojas tā, kā to ir paredzējis pasūtītājs.

3. CERT.LV nodrošinās drošības rekomendācijas CVK darbinieku tīkla drošināšanai. Šajā procesā notiks sadarbība ar CVK tehnisko personālu. CVK darbinieku tīkla tiks izvietota arī CERT.LV agrās brīdināšanas sistēma, taču tas neatrisinās elektroniskās balsu skaitīšanas procesu riskus.

2. Turpmākās darbības

Papildu finansējuma piešķiršanas gadījumā:

1. Ņemot vērā, ka Vēlēšanu sistēma atbilstoši Ministru kabineta 2018. gada 26. marta rīkojumam Nr.119k "Par kritiskās infrastruktūras kopumu" ir atzīta par KI, tiks nodrošināta Vēlēšanu sistēmas un vēlēšanu e-pakalpojuma atbilstība prasībām, kuras noteiktas KI. Rezultātā tiks nodrošināta kvalitatīvāka informācijas sistēmas aizsardzība pret potenciāliem kiberuzbrukumiem, ievērojami mazinot risku, ka 13. Saeimas vēlēšanu norise tiks negatīvi ietekmēta.

2. Nepieciešams papildu finansējums no valsts budžeta provizoriski 225 786 *euro* ar 21% PVN, apmērā.

3. Ņemot vērā, ka līdz 2018. gada 6. oktobrī paredzētajām 13. Saeimas vēlēšanām ir atlicis ierobežots laiks, finansējuma piešķiršanas gadījumā jau šobrīd pastāv risks, ka visi nepieciešamie vēlēšanu e-pakalpojuma drošības uzlabošanas pasākumi netiek īstenoti nepieciešamajā apjomā un termiņā.

4. Ņemot vērā Publisko iepirkumu likuma 61.panta ceturtajā daļā noteikto ierobežojumu attiecībā uz līgumcenas pieaugumu, kas noteic, ka visu secīgi veikto grozījumu naudas vērtības summa nevar pārsniegt 50 procentus no sākotnējās iepirkuma līguma līgumcenas, CVK nepieciešams izvērtēt iespēju piemērot Publisko iepirkumu likuma 8.panta septītās daļas 3.punktu, atbilstoši kuram pasūtītājs ir tiesīgs piemērot sarunu procedūru, ja pasūtītājam neparedzamu ārkārtas apstākļu rezultātā objektīvi radusies situācija, kurā steidzamības dēļ nav iespējams piemērot atklātu konkursu, slēgtu konkursu vai konkursa procedūru ar sarunām.

Ja papildu finansējums netiek piešķirts:

1. Neskatoties uz to, ka Vēlēšanu sistēma atbilstoši Ministru kabineta 2018. gada 26. marta rīkojumam Nr.119k "Par kritiskās infrastruktūras kopumu" ir atzīta par KI, Vēlēšanu sistēmai un vēlēšanu e-pakalpojumam netiks nodrošināta atbilstība drošības prasībām, kuras noteiktas KI.

2. Vēlēšanu e-pakalpojums tiks nodrošināts piešķirtā valsts budžeta ietvaros.

3. 13. Saeimas vēlēšanu norises laikā kiberuzbrukumu gadījumā pastāv paaugstināts risks, ka netiks nodrošinātas atsevišķas vēlēšanu e-pakalpojuma funkcionalitātes, kā rezultātā:

3.1. Tiks kavēta provizorisko vēlēšanu rezultātu paziņošana, līdz ar to var tikt radīts būtisks kaitējums Latvijas tēlam kā arī veicināta Latvijas vēlētāju neuzticēšanās vēlēšanu organizēšanas procesam.

3.2. Savlaicīgi netiks nodrošinātas Saeimas vēlēšanu likuma 23. panta piektajā daļā, 24. panta pirmajā un sestajā daļā, 28. pantā, 31. pantā, 35. panta otrajā daļā, 36. pantā, 45.³ panta septītajā daļā un 48. panta trešajā daļā noteiktās prasības.

- Atzīmes veikšana vēlēšanu gaitas žurnālā par atkārtotu vēlēšanu aploksnē saņemšanu.

- Vēlētāja, viņa pilnvarotas personas vai aizgādņa rakstveida iesnieguma reģistrēšana vēlēšanu gaitas žurnālā par vēlēšanu organizēšanu vēlētāja atrašanās vietā.

- Informācijas ierakstīšana vēlēšanu gaitas žurnālā par balsošanai vēlētāju atrašanās vietā izsniegtajām un pāri palikušajām, tai skaitā sabojātajām, vēlēšanu aploksnēm.

- Sūdzību reģistrēšana vēlēšanu gaitas žurnālā.

- Informācijas ierakstīšana vēlēšanu gaitas žurnālā par balsu skaitīšanas rezultātā iegūtajiem datiem.

- Ziņu ievadīšana vēlēšanu gaitas žurnālā par saņemtajām, izlietotajām un pāri palikušajām vēlēšanu aploksnēm, balsotāju skaitu iecirknī un vēlētāju atrašanās vietās.

- Nederīgo vēlēšanu aplokšņu kopskaita ierakstīšana vēlēšanu gaitas žurnālā.

- Katra kandidāta saņemto atzīmju skaita ierakstīšana vēlēšanu gaitas žurnālā.

- Atsauces veikšana vēlēšanu gaitas žurnālā par vēlēšanu materiālu iesaiņošanu un aizzīmogošanu.

- Detalizētas informācijas ierakstīšana vēlēšanu gaitas žurnālā par nederīgajām vēlēšanu aploksnēm.

3.3. Atkarībā no nodarījuma ko būs veicis potenciālais kiberuzbrukums, tiks aizkavēts (divas dienas – divas nedēļas) balsu saskaitīšanas un apkopošanas process. Šobrīd lielākā daļa vēlēšanu iecirkņu balsu skaitīšanai izmanto vēlēšanu e-pakalpojuma nodrošināto funkcionalitāti. Gadījumā, ja traucēts būs tikai sakaru kanāls, aizkavēšanās būs saistīta ar datu apkopošanas procesu. Savukārt, ja traucēta būs Vēlēšanu sistēma, balsis nāksies skaitīt un apkopot pilnībā manuāli, kā rezultātā process var ievērojami ieilgt.

Nemot vērā informatīvajā ziņojumā sniegto informāciju, nepieciešams pieņemt lēmumu par finansējuma piešķiršanu 225 786 euro apmērā vēlēšanu e-pakalpojuma drošības paaugstināšanai.

Vides aizsardzības un reģionālās attīstības ministrs



K. Gerhards

R.Guds, 67026525,
18.07.2018.
rihards.guds@varam.gov.lv