Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Қазақстан Республикасының Ішкі істер министрлігі" мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Қазақстан Республикасының Ішкі істер министрлігі" мемлекеттік мекемесі
Конкурстың №:	№ 17835015-1
Конкурстың атауы:	2027 жылға арналған АҚ және АТ инфрақұрылымын техникалық сүйемелдеу қызметтерін сатып алуға арналған конкурс
Лоттың нөмірі:	№ 88110752-ОК1
Лоттың атауы	Ақпараттық жүйені қостау және техникалық қолдау көрсету бойынша қызмет көрсетулер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	620230.000.000001
Қызметтің атауы:	Ақпараттық жүйені қостау және техникалық қолдау көрсету бойынша қызмет көрсетулер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	17000000
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	17000000
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	2027 жылғы 31 желтоқсанға дейін
Аванстық төлем мөлшері:	0

Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Қызмет көрсету мерзімі – 2027 жылғы 1 қаңтардан бастап 2027 жылғы 31 желтоқсанға дейін. Қызмет көрсету орны – Қазақстан Республикасы, Астана қаласы, Тәуелсіздік даңғылы, 1. Қызметтер ақпараттық қауіпсіздік (бұдан әрі – киберқауіпсіздік) құралдарының тұрақты жұмыс істеуін қамтамасыз ету, оларға техникалық сүйемелдеу бойынша іс-шараларды орындау, киберқауіпсіздік талаптарын іске асыру және киберқауіпсіздік бөлінісінің цифрлық сервистерінің үздіксіз жұмыс істеуін қамтамасыз ету мақсатында көрсетіледі. Осы техникалық ерекшелікте мынадай негізгі терминдер пайдаланылады: Тапсырыс беруші – техникалық сүйемелдеу бойынша қызметтерді сатып алатын мемлекеттік мекеме. Жеткізуші – техникалық сүйемелдеу бойынша қызметтер көрсететін жеткізуші. Киберқауіпсіздік бөлінісі – киберқауіпсіздікті қамтамасыз ету жөніндегі қызметті ұйымдастыруды және үйлестіруді жүзеге асыратын Тапсырыс берушінің құрылымдық бөлінісі. Ақпаратты қорғау құралдары – киберқауіпсіздікті қамтамасыз етуге арналған бағдарламалық, бағдарламалық-аппараттық және аппараттық құралдар (антивирус, SIEM жүйесі, DLP жүйесі). Физикалық сервер – цифрлық жүйелер мен ақпаратты қорғау құралдарының жұмыс істеуін қамтамасыз ететін серверлік жабдық. Виртуалды сервер – цифрлық жүйелер мен ақпаратты қорғау құралдарының жұмыс істеуі үшін пайдаланылатын виртуалды есептеу ортасы. Киберқауіпсіздік инциденті – цифрлық деректердің немесе цифрлық жүйелердің құпиялылығының, тұтастығының немесе қолжетімділігінің бұзылуына әкеп соққан немесе әкеп соғуы мүмкін оқиға. Қызметтер шеңберінде Жеткізуші: 1) физикалық серверлерге, виртуалды серверлерге, ақпаратты қорғау құралдарына және киберқауіпсіздік бөлінісінің мамандандырылған бағдарламалық қамтамасыз етуіне техникалық сүйемелдеуді қамтамасыз етеді; 2) киберқауіпсіздік талаптарын іске асыруға бағытталған техникалық іс-шараларды орындайды; 3) берілген өкілеттіктер шегінде киберқауіпсіздік саясатын енгізуді және өзектендіруді жүзеге асырады; 4) цифрлық жүйелер мен желілік инфрақұрылымның қорғалу жағдайына талдау жүргізеді; 5) цифрлық жүйелер мен желілік инфрақұрылымның техникалық осалдықтары мен конфигурациясындағы кемшіліктерді анықтайды; 6) анықталған осалдықтарды жою және қорғалу деңгейін арттыру бойынша ұсынымдар дайындайды; 7) киберқауіпсіздік инциденттерінің салдарын жоюға қатысады; 8) киберқауіпсіздік бөлінісінің тапсырмасы бойынша ақпаратты қорғау құралдарын, серверлер мен операциялық жүйелерді баптау жөніндегі техникалық іс-шараларды орындайды; 9) ақпаратты қорғау құралдары мен серверлік инфрақұрылымды пайдалану мәселелері бойынша киберқауіпсіздік бөлінісіне консультациялық қолдау көрсетеді. Жеткізуші берілген өкілеттіктер шегінде техникалық сүйемелдеуді жүзеге асырады және Тапсырыс берушімен келісусіз цифрлық инфрақұрылымның архитектурасын өзгертуге немесе жаңа цифрлық жүйелерді пайдалануға беруге байланысты дербес шешімдер қабылдамайды. Қызметтер киберқауіпсіздік бөлінісінің өтінімдері бойынша, сондай-ақ Тапсырыс берушімен келісілген тоқсан сайынғы

	профилактикалық іс-шаралар жоспарын іске асыру шеңберінде көрсетіледі. Тапсырыс беруші мен Жеткізуші арасындағы өзара іс-қимыл киберқауіпсіздік бөлімшесі немесе Тапсырыс берушінің уәкілетті лауазымды тұлғалары арқылы жүзеге асырылады. Киберқауіпсіздік инциденттері туындаған жағдайда Жеткізуші киберқауіпсіздік бөлінісін дереу хабардар етеді және берілген өкілеттіктер шегінде оларды оқшаулау және жою жөніндегі техникалық іс-шараларды орындауға кіріседі. Жұмыстарды орындау аяқталғаннан кейін Жеткізуші киберқауіпсіздік бөлінісін орындалған іс-шаралар туралы хабардар етеді және қажет болған жағдайда ұқсас инциденттердің туындауына жол бермеу бойынша ұсынымдар береді. Жеткізуші жұмыс күндері сағат 09:00-ден 18:30-ға дейінгі кезеңде Тапсырыс берушінің жұмыс орнында киберқауіпсіздік әкімшісінің болуын қамтамасыз етуге міндетті. Демалыс және мереке күндері, сондай-ақ белгіленген жұмыс уақытынан тыс уақытта әлеуетті өнім беруші осы техникалық ерекшелікте көзделген жағдайларда Тапсырыс берушінің өтінімі бойынша киберқауіпсіздік әкімшісін тартуды қамтамасыз етеді. Қызметтерді көрсету кезінде Жеткізуші Қазақстан Республикасының киберқауіпсіздік саласындағы заңнамасының талаптарын, сондай-ақ Тапсырыс берушінің ішкі құжаттарын сақтауға міндетті. Егер қызметтерді көрсету барысында Жеткізушіге таратылуы шектелген ақпаратқа, цифрлық жүйелерге немесе Тапсырыс берушінің техникалық мәліметтеріне қолжетімділік берілсе, Тапсырыс беруші мен Жеткізуші арасында құпиялылық туралы келісім жасалады. Техникалық сүйемдеу объектілерінің тізбесі: 1) Киберқауіпсіздік бөлінісінің физикалық серверлері – Dell, XFUSION; 2) Киберқауіпсіздік бөлінісінің виртуалды серверлері – VMware ESXi; 3) Киберқауіпсіздік бөлінісінің ақпаратты қорғау құралдары – желінің ішкі және сыртқы контурларына арналған DLP жүйесі, SIEM жүйесі, желінің ішкі және сыртқы контурларына арналған антивирус; 4) Киберқауіпсіздік бөлінісінің мамандандырылған бағдарламалық қамтамасыз етуі – Tenable Nessus осалдықтарды сканері.
Әлеуетті өнім берушіге оның жеңімпазы анықталған және онымен Мемлекеттік сатып алу туралы шарт жасалған жағдайда қойылатын талаптар (қажет болған кезде көрсетіледі) (әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін қабылдамауға жол берілмейді)	-

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Государственное учреждение "Министерство внутренних дел Республики Казахстан"
Наименование организатора	Государственное учреждение "Министерство внутренних дел Республики Казахстан"
№ конкурса:	№ 17835015-1
Наименование конкурса:	Конкурс по приобретению услуг по техническому сопровождению ИБ и ИТ инфраструктуры
Номер лота:	№ 88110752-ОК1
Наименование лота:	Услуги по сопровождению и технической поддержке информационной системы
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	620230.000.000001
Наименование услуги:	Услуги по сопровождению и технической поддержке информационной системы
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	17000000
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	17000000
Срок оказания услуги:	по 31 декабря 2027 года
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	Срок оказания услуг – с 1 января 2027 года по 31 декабря 2027 года. Место оказания услуг – Республика Казахстан, г. Астана, проспект Тәуелсіздік, 1. Услуги оказываются в целях обеспечения устойчивого функционирования средств информационной безопасности (далее – кибербезопасности), выполнения технических мероприятий по их сопровождению, реализации требований кибербезопасности и обеспечения непрерывной работы цифровых сервисов подразделения кибербезопасности. В настоящей технической спецификации используются следующие основные термины: Заказчик – государственное учреждение, приобретающее услуги по техническому сопровождению. Поставщик – поставщик, оказывающий услуги по техническому сопровождению. Подразделение кибербезопасности – структурное подразделение Заказчика, осуществляющее организацию и координацию деятельности по обеспечению кибербезопасности. Средства защиты информации – программные, программно-аппаратные и аппаратные средства, предназначенные для обеспечения кибербезопасности (антивирус, SIEM система, DLP система). Физический сервер – серверное оборудование, обеспечивающее функционирование цифровых систем и средств защиты информации. Виртуальный сервер – виртуальная вычислительная среда, используемая для функционирования цифровых систем и средств защиты информации. Инцидент кибербезопасности – событие, которое привело или может привести к нарушению конфиденциальности, целостности либо доступности цифровых данных или цифровых систем. В рамках услуги поставщик обеспечивает: 1) техническое сопровождение физических серверов, виртуальных серверов, средств защиты информации и специализированного программного обеспечения подразделения кибербезопасности; 2) выполнение технических мероприятий, направленных на реализацию требований кибербезопасности; 3) внедрение и актуализацию политик кибербезопасности в пределах предоставленных полномочий; 4) проведение анализа состояния защищенности цифровых систем и сетевой инфраструктуры; 5) выявление технических уязвимостей и недостатков конфигурации цифровых систем и сетевой инфраструктуры; 6) подготовку рекомендаций по устранению выявленных уязвимостей и повышению уровня защищенности; 7) участие в устранении последствий инцидентов кибербезопасности; 8) выполнение технических мероприятий по настройке средств защиты информации, серверов и операционных систем по поручению подразделения кибербезопасности; 9) консультационную поддержку подразделения кибербезопасности по вопросам эксплуатации средств защиты информации и серверной инфраструктуры. Поставщик осуществляет техническое сопровождение в пределах предоставленных полномочий и не принимает самостоятельных решений, связанных с изменением архитектуры цифровой инфраструктуры либо вводом в эксплуатацию новых цифровых систем без согласования с Заказчиком. Оказание услуг осуществляется по заявкам подразделения кибербезопасности, а также в рамках реализации

	плана ежеквартальных профилактических мероприятий, согласованного с Заказчиком Взаимодействие между Заказчиком и Поставщиком осуществляется через подразделение кибербезопасности либо уполномоченных должностных лиц Заказчика. При возникновении инцидентов кибербезопасности Поставщик незамедлительно информирует подразделение кибербезопасности и приступает к выполнению технических мероприятий по их локализации и устранению в пределах предоставленных полномочий. По завершении выполнения работ Поставщик информирует подразделение кибербезопасности о выполненных мероприятиях и, при необходимости, предоставляет рекомендации по предотвращению возникновения аналогичных инцидентов. Поставщик обязан обеспечить нахождение администратора кибербезопасности на рабочем месте Заказчика в рабочие дни в период с 09:00 до 18:30 часов. В выходные и праздничные дни, а также вне установленного рабочего времени, потенциальный поставщик обеспечивает привлечение администратора кибербезопасности по заявке Заказчика в случаях, предусмотренных настоящей технической спецификацией. При оказании услуг Поставщик обязан соблюдать требования законодательства Республики Казахстан в области кибербезопасности, а также внутренние документы Заказчика. Между Заказчиком и Поставщиком заключается соглашение о конфиденциальности, если в процессе оказания услуги Поставщику предоставляется доступ к информации ограниченного распространения, цифровым системам либо техническим сведениям Заказчика. Перечень объектов технического сопровождения: 1) Физические серверы подразделения кибербезопасности – Dell, XFUSION; 2) Виртуальные серверы подразделения кибербезопасности – VMware ESXi; 3) Средства защиты информации подразделения кибербезопасности – DLP система для внутреннего и внешнего контура сети, SIEM система, антивирус для внутреннего и внешнего контура сети; 4) Специализированное программное обеспечение подразделения кибербезопасности – Сканер уязвимости Tenable Nessus.
Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается)	-