Дата формирования: 17.04.2019

ПРОТОКОЛ ПРЕДВАРИТЕЛЬНОГО ОБСУЖДЕНИЯ ПРОЕКТА ТЕНДЕРНОЙ ДОКУМЕНТАЦИИ ПО ЗАКУПКЕ СПОСОБОМ ОТКРЫТЫЙ ТЕНДЕР НА ПОНИЖЕНИЕ № 271578

Акционерное общество "Национальная атомная компания "Казатомпром"

(наименование заказчика)

в соответствии с пунктом 54-1 Инструкции по проведению электронных закупок товаров, работ, услуг АО «Самрук-Қазына» и организациями пятьдесят и более процентов голосующих акций (долей участия) которых прямо или косвенно принадлежат АО «Самрук-Қазына» на праве собственности или доверительного управления (далее - Инструкция), в целях проведения процедуры предварительного обсуждения проекта тендерной документации с потенциальными поставщиками разместило 13.04.2019 09:43:00 проект тендерной документации по закупке:

Работы по разработке Стратегии развития информационной безопасности компании

(наименование закупки)

До истечения окончательного срока представления замечаний по проекту тендерной документации, установленного в соответствии с Инструкцией, поступили следующие замечания:

1. Наименование организации: Товарищество с ограниченной ответственностью "ПРАЙСУОТЕРХАУСКУПЕРС ТАКС ЭНД ЭДВАЙЗОРИ", ФИО инициатора: Ахэрн Майкл Роберт, Контактные данные: +7 (717) 255-0707

№	Дата и время поступления замечания/предложения	Номер лота	Требование по закупке	Замечания/предложения	Принятое решение	Обоснование решения
1	16.04.2019 11:21	858042	Техническая спецификация поставщика	Комментарий 1: Глава 5. Пункт 16b. Наличие в команде не менее трех членов, обладающих квалификациями в области информационной безопасности, подтверждаемых соответствующими международными сертификатами (CISM, CISSP, Security+). PwC полностью поддерживает АО "НАК "Казатомпром" в том, что наличие в команде членов, обладающих знаниями и навыками подтвержденными соответствующими квалификациями в области информационной безопасности является необходимым условием для успешного выполнения проекта. Разработка стратегии информационной безопасности требует большего внимания к системе управления информационной безопасностью (СУИБ) и ее дальнейшего развития. Для обеспечения высокого качества работ, мы предлагаем расширить список международных сертификатов квалификацией в области внедрения СУИБ ISO 27001 Lead Implementer. Комментарий 2: Глава 5. Пункт 16c. Наличие в команде не менее одного члена команды, обладающего квалификациями в области информационной безопасности, подтверждаемых соответствующими международными сертификатами (CompTIA CySA+, EC Council Certified Network Defender, Cisco CCNA Cyber Ops). PwC полностью поддерживает АО "НАК "Казатомпром" в том, что наличие в команде членов, обладающих знаниями и навыками подтвержденными соответствующими квалификациями в области информационной безопасности является необходимым условием для успешного выполнения проекта. Однако квалификации	принято	Принято

				перечисленные в Глава 5. Пункт 16с являются относительными новыми для рынка и были запущены чуть менее двух лет назад. Количество специалистов обладающих данными квалификациями является ограниченным. Для обеспечения большего доступа к конкурсу и увеличения количество участников открытого конкурса, мы предлагаем расширить список аналогичными квалификациями, более распространенными среди специалистов в РК (CCNA Security (CNSS-4011), CCNP Security (CNSS-4013) или аналогичными). Комментарий 3: PwC полностью поддерживает АО "НАК "Казатомпром" в том, что наличие в команде членов, обладающих знаниями и навыками подтвержденными соответствующими квалификациями в области информационной безопасности является необходимым условием для успешного выполнения проекта. АО "НАК "Казатомпром" является промышленной компанией, соответственно обеспечение безопасности промышленных активов (OT security, including SCADA, data security, и т.д.) является ключевым направлением стратегии ИБ. Для обеспечения высокого качества проработки стратегии мы предлагаем включить в главу 5, пункт 16, подпункт D квалификации в области информационной безопасности АСУ-ТП таких как Certified SCADA Security Architect (CSSA), GIAC ICS Security Professional (GICSP) или аналогичных.		

2. Наименование организации: Товарищество с ограниченной ответственностью "Делойт", ФИО инициатора: Жұмабек Жомарт Рахманбердіұлы, Контактные данные: +7 (707) 840-8700

№	Дата и время поступления замечания/предложения	Номер лота	Требование по закупке	Замечания/предложения	Принятое решение	Обоснование решения
1	15.04.2019 19:17	858042	Техническая спецификация поставщика	Комментарии к ТЕХНИЧЕСКОЙ СПЕЦИФИКАЦИИ. п. 2. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики. Глава 1. Общие положения. пп. 3. Основными целями разработки Стратегии является: 2)Актуализация процесса обеспечения ИБ в Компании для максимально эффективного снижения рисков целевых кибератак и их последствий; Комментарий: - что подразумевается под «актуализацией»; проект называется разработкой Стратегии; если актуализация подразумевает под собой внедрение процессов безопасности, то эта задача должна быть выполнена после разработки Стратегии и других документов; нам нужно уточнить, целью и	частично принято	Ответ на 1 вопрос: Под актуализацией политики Информационной безопасности подразумевается, обновление политики учитывая новых трендов в информационной безопасности, новых угроз и т.д. Актуализация НЕ предусматривает ВНЕДРЕНИЕ процессов безопасности, т.к эта задача будет выполнена после разработки Стратегии и других документов в рамках операционной деятельности. Ответ на 2 вопрос: 1) Исполнитель должен проанализировать возможные кибер атаки на предприятие с учётом специфики бизнеса. 2) Исполнитель должен перечислить риски реализации задачи для внедрения Стратегии. Ответ на 3 вопрос: Да, заказчик требует от подрядчика самостоятельного проведения оценки рисков экспертами; Ответ на 4 вопрос: "Актуализированная Политика ИБ" подразумевает под собой разработанный и представленный проект документа Заказчику.

				задачей проекта является разработка или разработка и внедрение в совокупности? Глава 1. Общие положения. пп. 4. Для достижения поставленной цели, Стратегия должна содержать: 2)Анализ возможных типов, векторов и целей кибератак; 7)Перечень возможных рисков реализации задач; Комментарий: - в чем заключается разница между этими двумя требованиями? Что подразумевается под “задачами”, проектные задачи для внедрения Стратегии? Глава 3. Требования по содержанию Стратегии. пп. 12. Стратегия должна обязательно содержать следующие разделы: 2)Анализ текущей ситуации по обеспечению ИБ в Компании: •Анализ угроз на основе процесса Kill Chain, •Перечень рисков, •Экспертная оценка из значимости; 3)Анализ возможных векторов кибератак: •Перечень и анализ реальных случаев целевых кибератак на промышленные объекты, •Перечень возможных векторов кибератак с учетом изменения технологического ландшафта Компании; Комментарий: - заказчик требует от подрядчика самостоятельного проведения оценки рисков экспертами? Глава 3. Требования по содержанию Стратегии. пп. 14. Комплект документов, который должен появиться по завершению разработки: 2) Актуализированная «Политика информационной безопасности». Комментарий: - "Актуализированная" подразумевает под собой подписанную или внедренную политику или что-то другое?		

Управляющий директор по комплексной безопасности Умербеков Жанат Жанбырбаевич