

Реестровый номер закупки № 4-ОК/18
номер извещения на официальном сайте
Единой информационной системы
в сфере закупок № 0134200000117003903
ИКЗ 172380819740238080100103730017490244

РАЗЪЯСНЕНИЕ ПОЛОЖЕНИЙ КОНКУРСНОЙ ДОКУМЕНТАЦИИ ОТКРЫТОГО КОНКУРСА

на право заключения контракта, на выполнение работ по созданию и внедрению опытных участков аппаратно - программного комплекса "Безопасный город" на территории пилотных муниципальных образований Иркутской области

Рассмотрев запрос о разъяснении положений конкурсной документации, номер извещения на официальном сайте Единой информационной системы в сфере закупок № 0134200000117003903 (реестровый номер закупки № 4-ОК/18) на право заключения контракта на выполнение работ по созданию и внедрению опытных участков аппаратно - программного комплекса "Безопасный город" на территории пилотных муниципальных образований Иркутской области поступившего от участника закупки 06.12.2017 №1845 министерство по регулированию контрактной системы в сфере закупок Иркутской области на основании письма заказчика - ОГБУ «ПСС Иркутской области» сообщает:

Ссылка на раздел, подраздел, пункт либо форму конкурсной документации, требующие разъяснений	Содержание запроса на разъяснение положений конкурсной документации
Пункт 27 Части 2 «Информационная карта открытого конкурса»	Прошу разъяснить обоснованность требования о наличии следующих лицензий: <ul style="list-style-type: none">Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации;

- Лицензия ФСБ России на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- Лицензия ФСТЭК России на проведение работ, связанных с созданием средств защиты информации;
- Лицензия ФСТЭК России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части противодействия иностранным техническим разведкам);
- Лицензия ФСБ России на осуществление работ, связанных с использованием сведений, составляющих государственную тайну;
- Лицензия ФСБ России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны.

ОТВЕТ:

В соответствии с п.3 «Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности», утвержденным Постановлением Правительства Российской Федерации от 4 сентября 1995 г. № 870, сведения, утрата которых может нанести ущерб интересам предприятия, учреждения или организации (как правило, формируемые и используемые на муниципальном уровне), относятся к секретным сведениям.

В соответствии с ФЗ «О государственной тайне» от 21 июля 1993 г. № 5485-1 секретные сведения, как и любые другие, составляющие государственную тайну, подлежат защите (раздел VI Федерального закона), в том числе, от иностранных технических разведок.

В соответствии со ст. 27 Закона Российской Федерации № 5485-1 от 21.07.1993г. «О государственной тайне» допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

Согласно п. 3 ст.49 Гражданского кодекса Российской Федерации право юридического лица осуществлять деятельность, на занятие которой необходимо получение лицензии, возникает с момента получения такой лицензии или в указанный в ней срок и прекращается по истечении срока ее действия, если иное не установлено законом или иными правовыми актами.

В соответствии с пунктом 2 Положения о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны (утв. Постановлением Правительства Российской Федерации от 15.04.1995г. №333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а так же с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны») органами, уполномоченными на ведение лицензионной деятельности, являются:

А) на право проведения работ, связанных с созданием средств защиты информации - Федеральная служба по техническому и экспортному контролю (ФСТЭК).

Б) на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны - Федеральная служба безопасности Российской Федерации и ее территориальные органы (ФСБ), Федеральная служба по техническому и экспортному контролю (ФСТЭК).

Учитывая изложенное, а также концентрацию стратегических предприятий и объектов (Ангарский электролизный химический комбинат, Байкальский целлюлозно-бумажный комбинат, Восточно-Сибирское производственно-комплектовочное предприятие "Атомпромкомплекс", Братское авиапредприятие, Братская гидроэлектростанция), объектов оборонной промышленности на территории Иркутской области, при создании Системы должны быть реализованы мероприятия, направленные на исключение или существенное затруднение добывания иностранными разведками с помощью технических средств сведений, отнесенных к конфиденциальной информации и подлежащих защите.

Разработка требований на проведение анализа возможных каналов утечки охраняемых сведений должна быть осуществлена подрядчиком на этапе технического проектирования, с учетом возможных демаскирующих признаков, раскрывающих сведения в отношении информации, которая может циркулировать в Системе. Такими демаскирующими признаками могут быть: побочные электромагнитные излучения и наводки, создаваемые техническими средствами Системы; визуально-оптическая информация, составляющая государственную тайну, выводимая на устройства отображения, входящие в состав Системы; акустические и вибрационные сигналы, создаваемые в процессе обсуждения вопросов, содержащих охраняемые сведения на объектах автоматизации.

Исходя из вышеизложенного, в конкурсной документации установлены требования о наличии у участника закупки действующих лицензий:

- 1) ФСТЭК России на проведение работ, связанных с созданием средств защиты информации.
- 2) ФСТЭК России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части противодействия иностранным техническим разведкам).

Режимные меры по предотвращению утечки сведений из перечня охраняемых на различных этапах работы должны быть включены подрядчиком в единый план мероприятий по сохранению режима секретности. Контроль и оценку достаточности и эффективности принимаемых мер обеспечения секретности осуществляют режимно-секретные подразделения подрядчика. Ответственность за организацию выполнения требований по обеспечению сохранения государственной тайны при выполнении работ возлагается на подрядчика, а ответственность за непосредственный

допуск подрядчика к выполнению работ, связанных с сохранением сведений содержащих государственную тайну – на заказчика работ.

Таким образом, в конкурсной документации обоснованно установлены требования о наличии у участника закупки действующих лицензий:

- 1) ФСБ России на осуществление работ, связанных с использованием сведений, составляющих государственную тайну;
- 2) ФСБ России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны.

Следует отметить, что в соответствии с частью III конкурсной документации «Наименование и описание объекта закупки (техническое задание)», а также проектом контракта Подрядчик должен организовать сбор необходимых для выполнения работы исходных данных, содержащихся, в том числе на топографических, геодезических и ортофотографических материалах (имеющих соответствующий гриф) с последующим созданием на базе указанных выше материалов цифровой картографической основы (в части реализации «Интеграционной географической информационной подсистемы»), Подрядчик в силу закона обязан иметь необходимые лицензии на проведение работ с использованием сведений, составляющих государственную тайну. Соответственно, при отсутствии у Подрядчика упомянутых лицензий блокируется исполнение контракта, так как получение Подрядчиком основополагающих данных для создания цифровой картографической основы становится невозможным.

По вопросу установления требования о наличии лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации сообщаем следующее. В части III конкурсной документации «Наименование и описание объекта закупки (техническое задание)» установлено: «4.2.1.8 Требования к Подсистеме информационной безопасности КСА «Региональная платформа» «Подсистема информационной безопасности КСА «Региональная платформа» должна соответствовать требованиям действующего законодательства Российской Федерации и нормативных документов в области защиты информации, в том числе защиты персональных данных.

Информационная безопасность должна обеспечиваться комплексом средств и мер обеспечения информационной безопасности, состоящим из программно-аппаратных средств защиты информации и организационных мероприятий по противодействию потенциальным угрозам, которые направлены на объект защиты.

К объектам защиты Системы относятся:

- технические средства;

- программные средства;
- информация, содержащая охраняемые сведения;
- помещения, предназначенные для обработки и хранения информации. «

4.2.1.8.8 Компонента анализа защищенности

«Компонента анализа защищенности должна обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем выявления и анализа уязвимостей информационной системы.»

В рамках выполнения обязательств по контракту подрядчиком должна быть создана подсистема информационной безопасности, одной из основных функций которой является защита конфиденциальной информации (в том числе персональных) данных. Также подрядчик должен обеспечить соответствующий контроль защищенности объектов защиты и обрабатываемой информации.

В части III конкурсной документации «Наименование и описание объекта закупки (техническое задание)» установлено:

4.2.1.8.7 Компонента криптографической защиты передаваемых данных
«Компонента криптографической защиты передаваемых данных должна обеспечивать защиту информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны.»

4.2.4.1.1 Требования к компоненту сети передачи данных
«- обеспечить аутентификацию соединения, шифрование и сжатие данных;»

В рамках исполнения обязательств по контракту должен быть выполнен комплекс работ по монтажу и наладке и последующей передаче заказчику криптографических (шифровальных) средств передачи информации.

Таким образом, в конкурсной документации обоснованно установлено требование о наличии у участника закупки действующей лицензии ФСБ России на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств,

информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

Уполномоченный орган

(Подпись)

М.Н. Павлюк