

QUESTIONS AND ANSWERS TO THE REQUEST FOR PROPOSALS TO CONDUCT CYBERSECURITY EXAMINATIONS OF A SINGLE STATE (NON-CONNECTICUT BASED) HEALTH INSURER AND A MULTI-JURISDICTION HEALTH INSURER

Q. We have a question, on page 5 of the RFP, Section 1, Organization Support and Experience, item #3 indicates that applicants are to provide a “Statement that the Applicant firm has been issued the Certified Incident Response Assistance designation issued by the National Security Agency.” Is this a designation that MUST be held by the applicant, or its subcontracted firm, in order to be considered for selection?

Q. Page 5 – Section 1 – Organization Support and Experience. Item 3. Statement that the Applicant firm has been issued the Certified Incident Response Assistance designation issued by the National Security Agency. There are many other certifications that would appear to be more relevant to the requirements of this solicitation and which require more intensive study (and ongoing education) by the personnel holding them. These include the Certified Information Systems Security Professional, the Certified Information Security Manager, the Certified Ethical Hacker, and the Certified Information Systems Auditor. Will it suffice to propose staff who hold these cyber security assessment and examination-focused certifications?

Q. If we have applied for the CIRA designation, but have not yet received it, are we eligible for consideration?

A. We are requiring the CIRA designation to be considered for this assignment. Additional certifications should be identified, but the CIRA designation is a threshold requirement. The CIRA designation must have already been awarded.

Q. What is the geographic proximity of the two examination targets?

A. The main geographic locations will be Connecticut and Wisconsin.

Q. Is the expectation that the examinations will be conducted consecutively or concurrently?

A. It is expected that the examinations will be conducted concurrently.

Q. Is there an expectation, given the limited information provided in the RFP about the two examination targets, that an affirmative cost estimate to conduct the two examinations will be provided?

A. A cost estimate will not be provided. We certainly understand this is difficult to estimate but we are looking for a rough estimate.

Q. Page 5 – Proposal Format and Content, Section 3. In addition to the hourly rates, are you expecting a sample project plan that should be priced for a sample examination or should we just submit hourly rates? Also, so that we can estimate expenses, where is the single state provider and where is the multi-jurisdictional examination to take place?

A. As indicated in the “technical statement” of the RFP, a sample work plan is required. Additionally, as indicated in the cost statement we require rates by individual and expenses. The main locations will be in Connecticut and Wisconsin.

Q. What are the respective sizes (in premium volume and number of data centers and whether they are centralized or decentralized of the two insurers?

A. For the small non-CT insurer:

The two affiliated smaller single-state insurers have combined premium reported in 2014 within the range of \$750 million to \$1 billion. The insurers share a common IT platform. They have a Centralized Primary Data Center hosted by a third party. The third party also has a Disaster Recovery Data Center. In addition, the insurer group also has a backup data center at its home office. They have three outside service providers for administrative services for segments of their business.

A. For the multi-jurisdictional insurer:

Premium is in excess of \$10 billion dollars, there are multiple data centers and they are decentralized.