Capitol Region Council of Governments (CRCOG)
Cybersecurity Model Policies and Consulting Services RFP ADDENDUM 3: Responses to Submitted Questions

Below are all of the questions that have been submitted. Many of the submitted questions inquire about similar sections of the RFP. For ease of all involved, these questions have been grouped and will be addressed in order of the section they reference. Please sign at the bottom and attach to your proposal to confirm that you have read this addendum in full.

Section II: Introduction/Background Information

1. How many members are currently a part of the IT Services Cooperative?

   The Capitol Region Council of Governments (CRCOG) is a voluntary Council of Governments formed to initiate and implement regional programs of benefit to the towns and the region. The cybersecurity program will become part of the IT Services Cooperative offerings. More information about CRCOG and the IT Services Cooperative can be found on the CRCOG website.

   Through CRCOG's member towns, the Capitol Region Purchasing Council (CRPC), and the Connecticut Council of Small Towns (COST), 154 of Connecticut's 169 municipalities have access to the IT Services Cooperative Programs. Membership in the IT Services Cooperative does not ensure that any or all of these municipalities will be interested or involved in this RFP or the proposed cybersecurity program.

Section III. Consultant Scope of Services

Policy List and Groupings

1. *Company* recommends differentiating between policies and procedures. Policies are higher-level guiding principles established by upper-management to set the direction within the organization, whereas procedures are specific steps required to meet the policy requirements. Is CRCOG seeking to develop policies, procedures, or a combination of both in a single document for each topic?

   The model policies and procedures listed in Section III are able to be altered and changed by the respondent as they see fit. CRCOG is seeking to provide a combination of policies and procedures that will be the starting point for municipalities to customize. The respondent should attempt to make both policies and procedures as relevant to all CRCOG municipalities as possible. The final deliverable will include all policies and procedures, listed or unlisted, that conform to applicable laws/mandates and the respondent determines as adequate to protect municipal networks and data. From the final deliverable, municipalities will have the option to customize the model policies to fit their own policies/procedures in place.

2. How does CRCOG define ‘policy,’ ‘standard,’ ‘procedure?

   In the RFP, ‘policy’, ‘standard’, and ‘procedure’ are used interchangeably to describe the model policies that our municipalities have requested. In the answers above, we have detailed that these polices/procedures can be altered if the respondent see fit. The respondent should define ‘policy’, ‘procedure’, ‘standard’, or any other necessary verbiage in their proposal.

3. Are the Model Cybersecurity Policies required to be separated into the four groups included in the RFP (I.e., are you married to these specific policy/procedure groupings)? For example: We noticed that the development of the "Recover Time and Recovery Point Policy" is listed under the "Ongoing Cybersecurity Policies and Procedures" group. However, we typically complete this through our standard process for developing a Disaster Recovery Plan. Are the four groups of Model Cybersecurity Policies subject to change?

   The respondent may alter the policy groupings as they see fit.

4. We also recommend including the development of the following policies, in order to ensure CRCOG comprehensively meets the principles set forth in the Connecticut’s Cybersecurity Action Plan, may we propose pricing as it relates to these as well?
   a. Vulnerability Management
   b. Third Party Risk Management
   c. Security Awareness
   d. Asset Management
   e. Change Control
   f. Risk Management
   g. Technology Disposal
   h. Standard Hardening

   If there are polices that are not listed that the respondent feels are necessary to adequately conform to applicable laws/procedures and protect CRCOG municipalities, those policies should be listed and defined in your proposal.

5. RFP page 3 refers to “On-going Cybersecurity Policies & Procedures” but only lists policies. Does the CRCOG want corresponding procedures authored for each policy listed?

   See answers above.

6. *Company* understands the RFP requirements to be outlined below, please confirm these are the requirements:
    - 27 policies and documents, divided into 4 categories
        - Each policy should include
            - Purpose
            - Scope
            - Policy
            - Exceptions
            - Expected Impact
            - Approval
    - 3 plans
        - IRP
        - BCP
        - DRP
    - 0 procedures

    See answers above.

7. Please confirm of the (3) plans requested, CRCOG is seeking a single document for each plan based on industry best practices and not a tailored plan for each.

    The format in which CRCOG is requesting the model policies/procedures/plans is listed in Section III. The respondent is free to alter the format in which the model policies/procedures/plans are delivered if they see fit. The proposal should include examples of the suggested format.

8. Several documents requested are titled “policy” but the description states that it is a “procedure”. Generally, these two terms are not interchangeable. Do you wish to have a combined policy and procedure in one document?

    See answers above.

9. The document specifies many policies however it is said that they are to be "included but not limited to". Would the proposer be expected to submit any additional policies that they feel should be included?

    See answers above.

10. Is the “Post-Breach Investigation Policy” intended to be an actionable and detailed incident/breach response plan, or a policy that sets requirements for an incident response program, team, etc.?

    See answers above.

11. Usually a Business Continuity Plan and Disaster Recovery Plan encompass much more than managing cybersecurity attacks (e.g. natural disasters and man-made threats). Will we only be focusing on cybersecurity attacks for both of these policies?

    See answers above.

12. What will the desired update cycle be? Will we provide that service? Or will we provide feedback and comments to CT on a scheduled basis? Annual review and subsequent updates? Do they need a policy update schedule (January, do this, February, do that...) as a deliverable?

    A desired review/update schedule for the model policies has not been specified. If a respondent recommends a review/update cycle they should detail it in their proposal.

Security Framework/Applicable Laws

1. Are the CRCOG / counties subject to any specific (security and privacy-related) regulatory or industry standard requirements? Please indicate: (e.g. HIPAA, SOX, PCI, State Breach, Other)

   Municipalities collect and access data that is governed by FERPA, HIPPA, and PCI and various other state and federal laws. Respondents should be familiar with these laws and mandates that are relevant to municipalities and err on the side of caution when omitting requirements. The intent of this RFP is not only to comply with applicable laws and mandates but to adequately protect municipal networks and data.

2. Are there industry standards that the CRCOG/ counties want use as basis for policy development (outside of regulatory requirements, e.g. ISO, NIST)? Upon which standards and regulatory requirements would you like the policy development to be based? Should policies align to a security framework? If yes, what is the preferred security framework?

   There is no preferred security framework for the model policies at this point. Individual municipalities may have a preference for a security framework, but the model policies are intended to be useful for all CRCOG municipalities. If the respondent recommends a security framework for all CRCOG municipalities, they should detail it in their proposal. It will be at the discretion of the pilot group to accept that recommendation, after the RFP process.

3. Which Connecticut state laws do these policies need to comply with, specifically?

   See answers above.

4. Do any current policies align to a security framework (NIST, ISO etc.)?

   See answers above and answers regarding Policies in Place.

5. Is there a preferred framework or regulation that needs to be considered/incorporated? (We will recommend derivative of Cybersecurity Framework and others that must be observed, including CT SB 949).

   See answers above.

6. Should policies align to a security framework? If yes, what is the preferred security framework?

   See answers above.

7. Are there any specific laws that CRCOG is concerned about?

   See answers above.

8. Is there a security framework CRCOG would like to be used for the basis of developing the policies?

   See answers above.

9. Are there any compliance or regulatory guidelines that would need to be considered when developing the policies?

   See answers above.

10. Do the policies need to be based off any particular framework, such as National Institute of Standards and Technology (NIST)?

    See answers above.

11. Has a security control framework been adopted? If yes, which one?

    See answers above and answers regrading Policies in Place.

12. What are the types of data handled by CRCOG/ counties or that these organizations are particularly concerned about? (e.g. Personable Identifiable Information (PII), Credit Card Data)

    There will be more clarity to exactly the type of the data handled by the broad spectrum of municipalities during the pilot process. Also, reference answers above.

13. Is a formal policy framework in place that includes policies, standards, guidelines, procedures etc.?

    See answers above and answers regarding Policies in Place.

Policies in Place

1. Are there currently any internal municipality documents referred to as basis for requirements or policy?

   The intent of this RFP is to provide model polices that will be of value to all CRCOG municipalities. Any existing cybersecurity policies in place by individual municipalities or at CRCOG are irrelevant to the process of creating model policies. The existing policies in place at individual municipalities may be relevant if/when municipalities contract with the respondent to customize and adopt the model policies and during the pilot process.

2. Have CRCOG / counties implemented a formal information security program leading up to this RFP?

   Access to model policies through this RFP is one part of a voluntary information technology security program that CRCOG intends and is in the process of creating.

3. Have any of the counties which are part of the CRCOG conducted an information security assessment or audit of the environment within the past twelve months? If yes, please describe the scope.

   CRCOG does not represent any formal county government agency. This RFP is for model policies that can be used for the municipalities that we represent. A security assessment or audit of the environment has not been conducted for the CRCOG region. Any security assessment conducted at the municipal level is not relevant to the creation of the model policies.

4. Are any of the policies currently in place that can be leveraged during the policy creation process?

   See answers above.

5. Are we are building from scratch or they have existing (old/obsolete) content that we can review?

   See answers above.

6. Are there existing procedures that need to be linked to updated policy content?

   See answers above.

7. Are there any established and documented security policies, standards, and supporting procedures? When? How often are they updated?

   See answers above.

8. Are there existing procedures that need to be linked to updated policy content?

   See answers above.

9. [Cyber Security Breach Process/Procedure] Are there contracts with (third party) breach response providers that will need to be examined/incorporated?

   In the creation of the model policies there are no specific contracts with third party breach response providers that need to be examined/incorporated. However, if the respondent recommends a policy to review contracts with third party breach responders, then it should be included in their proposal. During the customization process for individual municipalities, contracts with third party breach response providers may be relevant.

10. Has any existing breach process been audited/tested or are there state-managed post-mortem recommendations to be considered?

    The State of Connecticut has provided a Cybersecurity Action Plan that can be found in the link in Section II. However, respondents should rely on their own expertise in this area to create their proposals.

11. Does the state expect that municipalities have an accurate inventory of systems and/or sensitive data that needs to be incorporated in the breach response documentation?

    The State of Connecticut has not imposed any regulations or expectations on municipalities in regard to cybersecurity outside of the Cybersecurity Action Plan linked in Section II.

12. There's a difference between cyber breach and privacy breach, especially in terms of process and notifications. What is the current status and/or approach?

    See answers above.

13. Does a CIRT (cyber incident response team) exist? Is documentation and guidance to develop that capability required?

    See answers above and answers regarding Policy List and Groupings.

14. Are there existing guidelines, in addition to the Cybersecurity Action Plan enclosure, that should be considered for the various policy domains?

    See answers above and answers regarding Security Frameworks/Applicable Laws.

15. Does CRCOG anticipate utilizing any existing policies, or is the expectation that all requested policies will be created “anew”?

    See answers above.

16. Is it possible to access the current CRCOG cybersecurity policies?

    See answers above.

17. What are current industry best practices (if any) subscribed to by municipalities?

    See answers above.

Process for Creation/Acceptance

1. What are the plans/ process for policy review/execution (e.g. pilot)

   The process for model policy review will be at the discretion of the pilot group. The pilot group will consist of a small group of municipal employees from CRCOG towns that intend to use the template polices. Policy execution will be at the discretion of each municipality and will not start until after the model policies are finalized.

2. What is the estimated number of CRCOG-related contacts who will be involved in drafting of these policies? (Used for interview scheduling purposes)

   There has not been a decision relating the number of CRCOG-related contacts who will be involved in drafting these policies at this date. We intend for the pilot group to be diverse in terms of characteristics of the towns represented.

3. What is the approval process for draft policies?

   Approval for the draft model policies will be at the discretion of the pilot group.

4. Do proposed policies need to go through a union review?

   The model policies do not need to go through a union review. During the customization phase, individual municipalities may require union review before adoption if significant change is recommended.

5. Does CRCOG have a formal process for policy development? If so, can we obtain a copy?

   In regards to this RFP, CRCOG policy development processes are not relevant.

6. How many CRCOG professionals do you estimate will be needed to participate in interviews either in aggregate or per policy?

   See answers above.

7. Who from CRCOG will have authority to approve the content policies? Will there be a 1board that approves or will a single person have authority?

   See answers above.

8. What is the number of municipal leaders and relevant stakeholders that need to be consulted during the development of the cybersecurity policies?

   See answers above.

9. Please provide an estimate of the number of municipalities, teams, and individuals that will participate in the draft, review, and finalization process.

   See answers above.

10. Does a municipality cybersecurity oversight committee exist?

    A cyber security oversight committee does not exist at this point and any creation of a cyber security oversight committee will not influence the creation of the model policies.

11. Is there a policy oversight or governance committee?

    See answers above.

12. Who are the other stakeholders referred to ? (e.g. state, third party- page 2 and other)

    The stakeholders have not been defined but could be any person/staff who have a vested interest in the protection of municipal networks and data.

13. Can the Model Cybersecurity policies development be completed simultaneously, or must they be completed one-by-one? This is to inquire as to whether the same CRCOG stakeholders are required for all Model Cybersecurity policy drafting.

    It is expected that the model polices will be drafted simultaneously and accepted as a package.

14. Is there an approved template or preferred format for final policy deliverables?

    The preferred format for the model policies can be found in Section III. However, the respondent can make suggestions on alternate formats in their proposal, and during the drafting process.

15. Is there an approved template or preferred format for final policy deliverables?

    See answer above.

16. How will these policies need to be presented to stake holders?

    See answer above.

Customization/Complimentary Services

1. What are the rules of engagement for municipalities? Clarification: how do municipalities contract with us and is there a conflict of interest if a municipality directly contracts with our company for further cyber security related work?

   If/when the model policies are accepted by the pilot group, municipalities will have the ability to contract with the selected respondent for policy customization services through this RFP and subsequent contract. Services outside of policy customization are outside of the scope of this RFP.

   Through CRCOG's partnership with Novus Insight, municipalities have access to precontracted cybersecurity services. Any technical cybersecurity services included in any proposal will not be considered.

2. Please confirm the member customization process is out of scope for this RFP and will be contracted separately.

   It is the intent of this RFP to provide pre-negotiated pricing for customization services at an hourly rate. This ensures that municipalities would satisfy their procurement requirements if/when contracting with the selected respondent for policy customization services.

3. In addition, in order to develop a comprehensive Disaster Recovery (DR) Plan, we would recommend completing a Business Impact Analysis (BIA) process. This would help us to more accurately evaluate the potential effects an interruption to critical municipal operations would have in the event of a disaster. It involves interviewing various contacts from the municipality operations to determine what systems are most critical to operations. The BIA is imperative to developing an effective DR Plan.

   The model policies are intended to cover a wide variety of towns. If/when the policies are accepted, the selected respondent can work with individual municipalities to cater the policies/plans to their individual procedures and networks. Any services that the respondent deems necessary to the policy customization process should be thoroughly detailed in their proposal with pricing.

   However, any technical cybersecurity services that are not directly related to policy customization are outside of the scope of this RFP. Any technical cybersecurity services included in any proposals will not be considered.

4. Does CRCOG anticipate site assessments as a requirement for Model Cybersecurity customizations? If so, can CRCOG provide the estimated number of site assessments that will need to be performed?

   See answer above.

5. Is the scope of this RFP to include individual member cities and towns' option for customization, or limited to providing the CRCOG with a model set of policies whereby the individual member cities and towns will contract subsequently?

   The scope of this RFP is to provide CRCOG member cities and towns with model cybersecurity policies and pre-negotiated pricing for customization of the policies.

6. Is the expectation that these policies will be customized to match specific organizations, business processes, and technology solutions, or provide as a general policy that could be customized on a case by case basis?

   See answers above.

7. Expectations of adoption: Will municipalities adopt this in its entirety or cherry pick policies as they need them?

   The model policies are intended to be customized. The relevance of certain policies will vary depending on the individual municipality.

8. Are the policies outlined in this RFP mandatory or optional by the municipalities? If optional, does the State currently conduct a review of the municipal policies that have been adopted independently?

   The policies outlined in this RFP are not mandatory. There is currently no State of Connecticut review process for cybersecurity policies.

9. How many members are in CRCOG? How many of these members are intended to be engaged with during the period of performance?

   The Capitol Region Council of Governments consists of 38-member municipalities. There is no estimate to how many members intend to be engaged in this process. See answers above regarding Policy Creation/Acceptance.

Location

1. How would the interviews for this engagement be conducted? On-site or remotely? If on-site, what location(s) are in scope?

   To solicit feedback from the pilot group, present project updates, and present the final deliverable, it is estimated that 3 on-site meetings will be mandatory. The costs for these meetings should be included and itemized in your fee proposal. Any additional on-site meetings requested can be billed separately. The location of the meetings will be the CRCOG offices in Hartford, CT.

   We will consider proposals that propose only remote meetings, however, on-site meetings are preferred.

   Weekly check-in meetings with CRCOG staff is expected of respondents. Those check-ins can be conducted remotely via conference call.

2. Can the engagement, aside from the interviews, be performed remotely from *Company* offices or does the team need to be onsite in Hartford, Connecticut?

   See answer above.

3. What will be the primary work location?

   See answer above.

4. Does the project require a presence in Connecticut?

   See answer above.

Deadline/Length of Project

1. How long is the project intended to take place?

   The project does not have a defined timeline. However, based on the information provided in this RFP and addendum, it is expected that the respondent includes a project schedule in their proposal. The project schedule should not assume a project start date.

2. What are the preferred dates for the engagement to start/ finish?

   See answers above.

3. What is the deadline for the delivery of the Model Cybersecurity policies? That bears directly on how *Company* will staff and therefore price the fixed fee portion of the engagement.

   See answers above.

4. Please provide your estimation of the overall duration of the project for the initial development of the Model Cybersecurity Policies, excluding the customization by individual members cities and town.

   See answers above.

5. When will a decision be made on submitted proposals?

   Proposal evaluations will start after the proposal deadline. A decision will take place after the evaluation committee has had sufficient time to adequately evaluate all proposals and, if necessary, interview respondents.

6. What is time frame estimated for proposal decision?

   See answers above.

7. When will a decision be made on submitted proposals?

   See answer above.

8. What is the length of the contract? The document alludes to a non-specific 2-3 years. We would like to have a structured end date if possible.

   The length of the contract subject to negotiation.

Section IV. Fee Structure

1. Should the pricing be presented as cumulative in nature (one lump fee) or should we price out each of the policies separately?

   Pricing for the model cybersecurity policies should be cumulative. Please itemize direct and indirect costs as detailed as possible. This RFP also requests an hourly rate for policy customization.

2. Will CRCOG reimburse any travel expenses associated with the fixed fee portion of the engagement?

   All costs, direct and indirect, for the fixed fee portion of the engagement should be included and itemized in your cost proposal. See answers above regarding Location.

3. Has a budget been set for this project?

   The budget for this project is at the discretion of the CRCOG Executive Committee. Preliminary discussions have been held, but the budget for this project is subject to change depending on the recommendation of the evaluation committee.

4. Is there budget on this project? If so, what is it?

   See answer above.

Section V. Proposal Requirements

1. RFP page 7 refers to “Part 1- Consultant Overview and Plan”. Are there any additional parts?

   There are no additional parts. Proposals should include all items listed in Section V and include signed copies of the addenda.

General Questions

1. Does the State have an actual or perceived catalog of cybersecurity services (i.e. digital investigation and forensics, secure file archives, hosting facilities for RMV and other State of CT citizen services) that can be requested by the municipalities? If so, can you provide a list of such services and a description of each service?

   For the sake of this RFP, any state perceived catalog of cybersecurity services is not relevant. If a respondent feels that a resource is necessary to their proposal, they should supply it.

2. There is mention of a product to manage policies. We would like to gain more understanding of that request/idea.

   Refer to Section III and the answers in this addendum for more information regarding the scope of services.

3. How are they planning to communicate policies? Would they like us to provide awareness materials as well?

   Awareness materials are not in the scope of this RFP. If/when the draft policies are accepted, should the respondent decide to create any marketing or awareness materials, they do so on their own accord.

4. Is the current vendor, Novus Insight, excluded from this project?

   Novus Insight and CRCOG have a partnership for technological related services that includes cybersecurity services. Cybersecurity model policies and work related to the model polices are not being provided by Novus Insight.

5. We are making the observation that breach documentation is a different problem from policy development and an alternate approach might be that the policies be developed first and then clarify the breach documentation/crisis management issues. Would the State support a process where policies are developed first, and then, once approved, a second step would be to articulate those policies in operational processes and documentation?

   This is not a State program. See answers regarding Policy List and Groupings.

6. Is the IT organization centralized or decentralized?

   See answers regarding Policies in Place.

7. Are there remote locations or data centers involved?

   See answers regarding Policies in Place.

8. [Cyber Security Breach Process/Procedure] Does one exist at the State level?

   See answers regarding Policies in Place.

9. Will there be a centralized portal for review and final distribution? I see that their websites are being rewritten, where will policies reside when completed?

   This is not a State of Connecticut program. See Section II for more information.

10. When will responses to these questions be made available to bidding vendors?

    Due to procedure this is not a question that can be answered informally. When this addendum is posted, this question is moot.

11. Will the responses to questions be posted as addendums on the CRCOG website?

    Yes.

General Legal Questions

1. We cannot indemnify clients in an RFP. This conflicts with our firm's risk management policies. Any indemnities to be agreed between the parties would be negotiated in the Services Agreement, along with a cap on liability.

   That is correct. Any indemnities between the parties would be negotiated after the RFP process.

2. Proposals supplied by *Company* may contain confidential and/or proprietary methodologies, information and pricing of *Company*, and we do not assign entire ownership of our proposals to a potential client during an RFP process. We would request a carve out for our own intellectual property and confidential information contained in the proposal provided.

   Any proprietary methodologies or information should be specified as such. These areas specified can be redacted if information is requested by a third party.

Please sign below and attach to your proposal to confirm that you have read the addendum

Name:_____

Company:_____