



**CITY OF CORONA
DEPARTMENT OF WATER & POWER**

September 25, 2009

SUBJECT: Request For Proposals (RFP) No. DWP 10-103CA

**Network Infrastructure Assessment and
SCADA Security Management Review**

ADDENDUM No. 1

To All RFP Recipients:

This Addendum No. 1 to the subject RFP **provides answers to participants' questions.**

By this reference, all provisions of and attachments to this Addendum No. 1 are hereby incorporated into the subject RFP. Participants shall account for all provisions pursuant to this Addendum No. 1 in submitting their proposals. Each participant shall acknowledge receipt of this Addendum in their Proposal in the spaces provided therein.

A. Questions & Answers

1. **Question:** "Network Infrastructure Assessment - 14 servers:
 - a) OS type(s)?
 - b) Number and type of servers in DMZ?
 - c) Number of type of DB servers?
 - d) Number of web application servers?"

Answer: a) Windows NT 4.0 Server, 2000 Server and 2003 Server; b) There is no SCADA DMZ; c) the SCADA network has no database servers; and d) there is only one web server, and it hosts terminal web server.

2. **Question:** “Network Infrastructure Assessment - 30 workstations:

- a) OS Type?
- b) Number of domains?”

Answer: a) Mainly Windows XP Pro, and b) one single SCADA NT 4.0 domain. This will be upgraded to Windows 2003 AD domain before the end of October 2009.

3. **Question:** “Network Infrastructure Assessment - 12 networking devices:

- a) Number and type of firewalls?
- b) Number and type of routers?
- c) Number and type of switches?”

Answer: a) The SCADA network has only one firewall; b) none; and c) 20 - 30.

4. **Question:** “Network Infrastructure Assessment - Wireless access?

- a) Number of SSIDs?
- b) Number and type of WAPs?
- c) Number of and approx. square footage of locations?
- d) Centralized administration?”

Answer: a) None; b) none; c) not applicable; and d) not applicable.

5. **Question:** “Network Infrastructure Assessment - Externally facing web applications to be assessed?

- a) Number of applications?
- b) Hosting platform?
- c) Commercial or custom-developed?
- d) Language or framework?
- e) Unauthenticated & authenticated roles to be tested?”

Answer: a) Two, Terminal Services and TS over Web (IIS); b) currently Windows 2000, soon to be upgraded to Windows 2003 (by the end of October 2009); c) commercial (Terminal Services); d) not applicable; and e) the only thing to test would be Windows Terminal Services, its exploits and patches should be thoroughly documented, therefore, testing would not be necessary.

6. **Question:** “Network Infrastructure Assessment - Number of systems accessible from the Internet?”

Answer: One

7. **Question:** “Network Infrastructure Assessment - Vulnerability scanning only, or penetration / exploit testing also?”

Answer: Vulnerability testing is required, and penetration testing should be included if it is not too intrusive.

8. **Question:** “SCADA Security Management Review - Is the City of Corona’s Water and Power Department (City) seeking to achieve regulatory compliance through the implementation of a full ISO-standard based information security program? If so, what is the timeline for completion?”

Answer: The City is unsure how a full ISO security program fully relates to its SCADA system. This may be the City’s ultimate goal after the project has concluded.

9. **Question:** “SCADA Security Management Review - Has the City conducted a CIP-002 self certification and declared its critical cyber assets?”

Answer: The RFP is not WECC or NERC driven. The RFP is for water and water reclamation.

10. **Question:** “SCADA Security Management Review - Has the City conducted a SCADA assessment in the past?”

Answer: No

11. **Question:** “SCADA Security Management Review - What types of previous audits have been performed in the past that could provide relevant information? (ISO17799 Reviews, IT Security Controls Reviews, etc.) Will the selected vendor have access to these reports?”

Answer: None

12. **Question:** “SCADA Security Management Review - Does the City desire an assessment of their program’s compliance with all of the NERC CIP 002 through CIP 009 control standards?”
- Answer:** The City is not bound by NERC standards, but they are excellent standards to follow.
13. **Question:** “SCADA Security Management Review - As part of this review, will Critical Assets and Critical Cyber Assets need to be identified?”
- Answer:** Yes
14. **Question:** “SCADA Security Management Review - Is the City also seeking to have the logical security of its SCADA infrastructure assessed?”
- Answer:** Yes
15. “SCADA Security Management Review - Approximately how many City personnel will be available for interview?”
- Answer:** As many as required for a proper assessment.
16. **Question:** “SCADA Security Management Review - Will the selected vendor need to assess access points to the SCADA electronic security perimeter(s) to determine the effectiveness of security controls? If so, approximately how many access points will need to be assessed?”
- Answer:** All internal nodes and one terminal server.
17. **Question:** “SCADA Security Management Review - Will IT Assets within the SCADA Electronic Security Perimeter be assessed to determine the effectiveness of security controls? If so, approximately how many IT assets (and what type) will need to be assessed?”
- Answer:** Yes
18. **Question:** “SCADA Security Management Review - What is the approximate page count for policies, standards, and procedures that will need to be reviewed?”
- Answer:** There is none. This is a beginning point for the City.

19. **Question:** “SCADA Security Management Review - Will the selected vendor need to conduct a review of physical security where the SCADA devices are located? If so, how many locations will need to be assessed and how far away from each other are they?”
- Answer:** Yes. There are 6 main facilities and 5 remote locations.
20. **Question:** “SCADA Security Management Review - Will a review of firewall rulesets need to be conducted? If so, how many firewalls and types will be in-scope?”
- Answer:** Yes. One firewall.
21. **Question:** “SCADA Security Management Review - Will network scanning and analysis of the SCADA LAN be required? If so, please identify the number/type of networks, systems, services, etc.”
- Answer:** Yes. If the City understands the question, there are 61 nodes detected on the network.
22. **Question:** “SCADA Security Management Review - Will a review of server configurations and other devices on or connected to the SCADA LAN be required? If so, approximately how many servers and devices (and what type) will need to be assessed for this portion?”
- Answer:** Yes. 16.
23. **Question:** “SCADA Security Management Review - Will a review of remote access devices be required? If so, what type of remote access devices are currently being utilized?”
- Answer:** Yes. Wired and wireless.
24. **Question:** “Is it Primarily the Power side of your business driving this RFP from the push for NERC standards and the Feds? I’m just trying to identify the primary driver.”
- Answer:** No this is not from a NERC standpoint. The primary driver is preventive action. DWP operates its utility everyday by remote monitoring and intends to step back every two years and audit the system. The last few years have seen significant growth in DWP’s system, and this action is to make sure there are no errors. DWP will also use this as an update for its current practices to avoid making the same mistakes.

25. **Question:** “The City expects the selected vendor to conduct the SCADA Security Management Review using a methodology incorporating, at a minimum, SCADA security guidance, industry standard frameworks such as ISO 27001, other information security standards such as the PCI Data Security Standard, as well as applicable Federal laws and regulations. The methodology is expected to be sufficiently robust to uncover SCADA security management weaknesses against standard threat profiles.

The review identifies ISO 27001 and the PCI Data Security Standard. Neither of these standards were developed for SCADA applications. Is the City willing to recognize those standards being developed (don’t exist yet) for electric and water SCADA?”

Answer: Yes

26. **Question:** “The purpose of the SCADA Security Management Review is to compare the City’s SCADA security management practices to SCADA security management standards of care, including: The City’s need to secure its SCADA systems. Is this for electric SCADA, water SCADA or both?”

Answer: Water and Water Reclamation only.

27. **Question:** “External Network Assessment - What is the size of the target address range(s) to be assessed (e.g. one class B network, three class C networks, etc)?”

Answer: Two 254 address IP networks

28. **Question:** “External Network Assessment - How many Internet accessible systems are in scope for testing?”

Answer: One

29. **Question:** “External Network Assessment - Are there any timing limitations (e.g. night time or weekend only) limitations on the testing? If so, please specify.”

Answer: No

30. **Question:** “Internal Network Assessment – How many servers are in scope for testing?”
- Answer:** Two
31. **Question:** “Internal Network Assessment - How many workstations are in scope?”
- Answer:** 25
32. **Question:** “Internal Network Assessment - How many network devices (routers, firewalls, etc) are in scope?”
- Answer:** 20 – 30
33. **Question:** “Internal Network Assessment - Are there any timing limitations (e.g. night time or weekend only) limitations on the testing? If so, please specify.”
- Answer:** No
34. **Question:** “Network Architecture - What networks are in scope for the architecture review (e.g. internal network, DMZ, B2B connection, etc)?”
- Answer:** Internal
35. **Question:** “Network Architecture - What is the motivating factor for the architecture review (e.g. new network design, new systems added to the network, new connection to a partner or subsidiary, etc)?”
- Answer:** To set a guideline for future work and tighten security.
36. **Question:** “Network Architecture - Are firewall rule set reviews in scope? If so, please respond to the firewall configuration review questions.”
- Answer:** No
37. **Question:** “SCADA Specific - Could you briefly describe the purpose of this project?”

Answer: Analyze the current security posture, identify vulnerabilities that might result in significant security incidents, and provide the City with actionable recommendations for improving security.

38. **Question:** “SCADA Specific - Please list any previous or potential catalysts for this project? (Standards, Regulatory, Incident, Yearly Process, etc.)”

Answer: None

39. **Question:** “Site Information - Please provide the site information that is in scope for this project? Is the Water Source monitoring systems in scope? Are Waste Water Treatment Plants in Scope? Are Water Facility and Treatment Plants in scope?”

Answer: Yes to all.

40. **Question:** “Site Information - Could you briefly describe the network connectivity to all the sites that are in scope such as connectivity between the Alfred Merritt Smith Water Treatment Facility (AMSWTF) and the River Mountains Water Treatment Facility (RMWTF)?”

Answer: Not applicable. These are NOT City of Corona facilities.

41. **Question:** “Site Information - Are there any Energy or Electrical Generation facilities that are in scope that supply non-localized electricity to the BES? Please describe the site or any details.”

Answer: No

42. **Question:** “Architecture Information - Are wireless / radio / microwave in scope? If Microwave, are there any leased or shared Microwave capabilities?”

Answer: Yes. The City owns all radios. Various frequencies.

43. **Question:** “Architecture Information - Are pumping plants in scope? If so, how many?”

Answer: Yes. Six.

44. **Question:** “Architecture Information - Are there any Rate of Flow Control Stations (metering sites) ROFCS that are in scope?”

Answer: No

45. **Question:** “Architecture Information - Are there any elements of large diameter pipelines that require assessment (Such as touch points or RTUs that are monitoring the pipeline that is in scope)?”

Answer: No

46. **Question:** “Architecture Information - Can you provide network and/or security architectural diagrams that would help in scoping this project?”

Answer: No

47. **Question:** “Device and System Information - Which vendor SCADA system is used that are in scope? How many SCADA systems are in scope?”

Answer: Fix

48. **Question:** “Device and System Information - Are there any Data Historians that are in scope? If so what is the vendor and how many systems are in scope?”

Answer: Yes. Seven.

49. **Question:** “Device and System Information - Which vendor PLC/RTU systems are used that are in scope? How many PLC/RTU systems are in scope?”

Answer: Modicon and Allen-Bradley

50. **Question:** “Device and System Information - Are there any other servers within the SCADA environment that are in scope (In-house, legacy, etc.)? Please list and describe these servers.”

Answer: No

51. **Question:** “Project Timeline Information – Desired Start Date? Desired Completion Date?”

Answer: Anticipated start date is January 4, 2010; the work should be completed within four weeks of the start date.

52. **Question:** “Is this a security SCADA GAP analysis? A GAP analysis to where you are and where you should be (as conforming to NIST)?”

Answer: Yes

53. **Question:** “Is the SCADA system the same for power as for water? Are they separate?”

Answer: They are separate, and this RFP only includes water, wastewater and reclamation.

54. **Question:** “Are you considering all of field devices at the substations to be part of the SCADA system?”

Answer: Not all, but a handful of the larger locations that have intranets.

55. **Question:** “In the RFP “identify vulnerability points in a wide range of systems on the City’s network, including workstations, servers and network devices such as routers and switches—including wireless—that would allow an attacker to access the organization.” “including a description of vulnerabilities found during testing”--are you asking for a security penetration test against SCADA? It is generally not recommended. Are you asking for a security wireless scan?”

Answer: A wireless scan would be optimal as well as penetration testing so long as it does not affect the operation of the system.

56. **Question:** “Information security standards such as the PCI Data Security Standard”--are you asking for PCI compliance audit? This is completely different than a SCADA audit. If so, what is your transaction volume? Do you have PCI policies in place?”

Answer: The City is not aware of the difference but is looking for a comprehensive scan of its system that includes both SCADA and network reviews.

57. **Question:** “Do you have existing policies/procedures in place?”

Answer: For the SCADA network. It is unknown if policies exist for security.

58. **Question:** “Have you already had a NERC audit?”

Answer: Not applicable.

59. **Question:** “Do you have control system policies for SCADA? Do you have control policies for IT (they are different).”

Answer: For the SCADA network. It is unknown if policies exist for security.

60. **Question:** “In regards to providing references, due to the nature of our work (information security) we only provide this information should we be considered a viable candidate for the award of the engagement. Will it be acceptable to provided information about similar work experience, but only provide the actual company and contact information of our previous clients and references if we are considered a viable candidate to be awarded the engagement? Will points be deducted if specific reference information isn't provided?”

Answer: This is acceptable.

61. **Question:** “Is this project currently budgeted, or is The City of Corona Department of Water and Power issuing this RFP in order gathering information to obtain budget? If this project is budgeted, can you provide the budgeted amount?”

Answer: The project is budgeted.

62. **Question:** “Is there an incumbent vendor that The City of Corona Department of Water and Power prefers to work with?”

Answer: The City does not have an incumbent.

63. **Question:** “How many of each of the following types of devices in aggregate (external and internal) are to be considered to be in-scope of this assessment?”
- a. Routers
 - b. Firewalls
 - c. Switches
 - d. Wireless Access Points”

Answer: a) The City is not aware of any routers; b) there is one firewall; c) the City estimates there are 20-30 switches in the SCADA network (possibly unmanaged); and d) there are no computer wireless access points.

64. **Question:** “How many live IP's are in-scope of testing for this engagement? Please note that we are not seeking to know how much IP space you have, we are looking for an accurate representation of live systems that will be tested.”
- a. Internal
 - b. External”

Answer:

- a) Internal: 61 live IP addresses consisting of:
- iFix SCADA: 14 (mostly Windows XP and a few Windows 2000)
 - iFix VIEW: 7 (mostly Windows XP and a few Windows 2000)
 - Servers: 4 (two Windows NT 4.0 Server - Primary and Backup Domain Controllers; one Windows 2000 Server - Terminal Server; and one Windows 2003 Server - iHistorian)
 - Printers: 4
 - MDS Radios: 2
 - PLC: 17
 - Other HMI: 3
 - Other/Unknown: 10
- b) External: 1 Terminal Server

65. **Question:** “How many web based sites, portals or applications are considered in-scope for testing?”

- a. Internal
- b. External”

Answer: a) Internal: All SCADAs and VIEWs have VNC installed. There are no internal websites; b) External: There is only the terminal server.

66. **Question:** “How many physical locations will need to be visited in order to address the required services of this engagement?”

Answer: Estimated at 10.

67. **Question:** “What types of operating systems are in use and are in-scope for this engagement?”

Answer: Mainly Windows XP Professional, some Windows 2000 Professional and Server, there are a couple of Windows NT 4.0 Server, and a couple of Windows 2003 Server.

68. **Question:** “Are the City of Corona’s Safety Instrument Systems in scope for objective “B” (SCADA Security Management Review).”

Answer: The SCADA security management practices and standards of care have not been written, and the City intends to use this effort to develop these systems.

69. **Question:** “When were the SCADA security management practices and SCADA security management standards of care first written? When was the last review and update completed?”

Answer: The SCADA security management practices and standards of care have not been written, and the City intends to use this effort to develop these systems.

70. **Question:** “Network Infrastructure Assessment - What OS makeup the 14 servers?”

Answer: Mainly Windows XP Professional and a couple of Windows 2000 Professional.

71. **Question:** “Network Infrastructure Assessment - How large is the wireless infrastructure in terms of number of nodes and number of locations?”

Answer: It depends on what type of “wireless” you are referring to. The SCADA network has no wireless (802.11) WiFi access points. On the other hand, there are the wireless plant-to-plant radios, there are probably 8 locations and 14 nodes. There are Ethernet radios for communicating to the remote PLC sites. There are only a handful of these remote nodes and roughly 5 locations. It is important to point out that many of the locations overlap. For example, there are plant-to-plant radios and remote PLC radios at a treatment plant and at the desalter facility

72. **Question:** “SCADA Security Management Review - How big is the SCADA network in terms of number of nodes, size of network, and number of locations?”

Answer: There are 61 nodes.

73. **Question:** “SCADA Security Management Review - What controls and systems are being managed through the SCADA network?”

Answer: All water and wastewater operations.

74. **Question:** “SCADA Security Management Review - Can you further detail how the City expects ISO 27001 and PCI to be incorporated into the review?”

Answer: Through GAP analysis.

75. **Question:** “SCADA Security Management Review - How large is the internet presence in terms of total number of accessible IPs?”

Answer: The City is aware of only one external IP.

76. **Question:** “The RFP states that the final selection of consultants for interview and notification is expected to occur on or about October 7, 2009, and that the City anticipates making final selections and awards on or about October 8, 2009. Based on the short timeline, is the City planning to conduct finalist interviews?”

Answer: No.

77. **Question:** “Network Infrastructure Assessment - Based on the RFP Scope, is the Corona Department of Water and Power (CDWP) network separated from the other departments within the City of Corona networking environment? If so, how?”

Answer: The SCADA control network is separated by a single firewall from the remainder of the City’s network. The scope of this project will only affect what is within reach by the Department of Water and Power from the City’s intranet and the single terminal server connection.

78. **Question:** “Network Infrastructure Assessment - How many specific physical sites are included in the network assessment? How are these sites connected?”

Answer: There are approximately ten sites that are connected by wireless point-to-point radios. It is unknown whether there are other connections such as fiber.

79. **Question:** “Network Infrastructure Assessment - Has the CDWP completed a Risk Assessment of the network infrastructure and SCADA environment?”

Answer: No

80. **Question:** “Network Infrastructure Assessment - Does the internal network include a formal demilitarized zone (DMZ), application firewalls, or internal firewalls?”

Answer: The SCADA network does not have a DMZ, and there is only one firewall between SCADA and the City network.

81. **Question:** “Network Infrastructure Assessment - Does the network environment include intrusion detection, intrusion prevention, or digital loss prevention systems?”

Answer: No

82. **Question:** “Network Infrastructure Assessment - How many registered public IP addresses are utilized within the network environment?”

Answer: The SCADA network has only one public IP address for the terminal server.

83. **Question:** “Network Infrastructure Assessment - Does the CDWP use any hosted, managed service providers, etc.? If so, how are these services connected to the CDWP’s networking environment?”

Answer: Outside applications run through a terminal server connection and two firewalls.

84. **Question:** “Network Infrastructure Assessment - Are any CDWP servers located in the DMZ? If so, how many?”

Answer: CDWP does not have a DMZ.

85. **Question:** “Network Infrastructure Assessment - What operating systems are used within the network (servers & workstations)?”

Answer: Windows XP Professional, Windows NT 4.0 Server, Windows 2000 Professional & Server, Windows 2003 Server.

86. **Question:** “Network Infrastructure Assessment - Outside of the SCADA application, are there other applications included in the security review? Are these applications included in the configuration assessment identified within the Network Security Assessment section of the engagement?”

Answer: No

87. **Question:** “Network Infrastructure Assessment - If there are other applications included in the network assessment, what DBMSs are utilized by these other applications?”

Answer: Not Applicable

88. **Question:** “Network Infrastructure Assessment - Within the included network to be reviewed, are there VoIP solutions in use, and are these areas included in the scope of the engagement?”

Answer: VOIP is not on the SCADA network.

89. **Question:** “Network Infrastructure Assessment - Does the included network process, store, or transmit credit card transactions?”
- Answer:** No for the SCADA network.
90. **Question:** “Network Infrastructure Assessment - How many wireless endpoints are in use?”
- Answer:** None
91. **Question:** “SCADA Security Management Review - How many sites are connected to the SCADA network?”
- Answer:** There are 10 to 20 Ethernet capable sites. If all SCADA sites are considered (including serial comms), there would be 80-100.
92. **Question:** “SCADA Security Management Review - Is radio used within the SCADA network? If so, is the radio system in the scope of the Review?”
- Answer:** The radio system should be included in the scope.
93. **Question:** “SCADA Security Management Review - Are other wireless systems (point-to-point or LAN) in use within the SCADA network?”
- Answer:** Yes
94. **Question:** “SCADA Security Management Review - Are security monitoring activities and tools in use within the SCADA environment today?”
- Answer:** Very little.
95. **Question:** “The RFP states that the expected duration of the SCADA assessment is four (4) weeks. Does this include the Network Infrastructure Assessment processes?”
- Answer:** The estimated four week duration is for both.

96. **Question:** “The RFP requests that the proposal not exceed 25 pages in length, excluding any appendices. Does this page count include the required forms (OSHA, Non-Collusion Affidavit, Costing and Price forms), or is it acceptable to include those forms in an appendix?”

Answer: The required forms are to be included as part of the maximum 25 page count.

97. **Question:** “Given that there is both “evaluation criteria” and “selection criteria” in the RFP, specifically how are these to be used in making a final selection? Which section weights more into the decision making process?”

Answer: The City is interested in overall quality of the final product and has not determined a weight criteria to the responses.

98. **Question:** “In Section IV, Subsection A indicates four areas of concern regarding current level of network security. Are these examples that show the minimum areas of analysis which the consultant should expand upon, or should the assessment be limited to these critical areas?”

Answer: This is the minimum.

99. **Question:** “In Section IV, Subsection A indicates the deliverable must include recommendations that are actionable. Does the City expect that the "ease of remediation" factor will include budget and personnel capacity estimations, or does the City expect that recommendations will be prioritized and triaged by those limiting factors during or after the summary briefing?”

Answer: The City expects the recommendations will be triaged by those limiting factors during or after the summary briefing.

100. **Question:** “What is the estimated or desired delivery schedule for the work in Section IV, Subsection A? Does the 4-week estimate in Subsection D include the Network Infrastructure Assessment (Subsection A), or only the SCADA Security Management Review (Subsection B) as stated?”

Answer: The estimate is for both.

Carol Appelt
Property and Contract Administrator
City of Corona
Department of Water & Power
755 Corporation Yard Way, 2nd Floor
Corona, CA 92880
951-279-3620
951-735-3786 Fax