CALIFORNIA MULTIPLE AWARDS SCHEDULE
CALIFORNIA PRISON HEALTH CARE SERVICES
BUSINESS CONSULTING SERVICES

REQUEST FOR OFFER
INFORMATION TECHNOLOGY (IT) CONSULTING SERVICES
RFO-09-017-ITS

Addendum #2

Date: November 5, 2009

Department Contact:

California Prison Health Care Services
Attention: Alexander Thomson
501 J Street, Suite 225
P.O. Box 4038
Sacramento, CA 95812-4038
(916) 322-0529
Martin.Thomson@cdcr.ca.gov

The following questions have been received and are addressed herein for clarification purposes.

Question #1:

"What is the definition of 'Social Engineering'? For example, one of our attack processes during a wireless security audit is to place an access point within the local network to gain access. This is done as a proof of concept to show the need of a 24x7 dedicated wireless intrusion prevention system. Another example we use for social engineering is the need for the auditing team to get in range of CPHCS laptops to attack. Will we be able to talk our way into range of these devices or be given access?"

Answer:

Social Engineering is the act of manipulating people into performing actions or divulging confidential information. The scope of this engagement is a technical Black Box (i.e., using only information accessible to the public) assessment of wireless security architecture. The awarded contractor will focus on assessing the effectiveness of the wireless security design instead of finding ways to compromise the design through non-technical measures. The awarded contractor will be granted access to areas that are within range of the wireless signals.

Question #2:

"Point number six of section 'D' says: 'awarded Contractor shall attempt both external and internal security assessments.' Could you clarify this statement? Is it assumed that this is strictly wireless auditing or is there expectation for an internal wired assessment?"

Answer:

This statement means that the targets in scope for this assessment are protected by physical security controls to prevent unauthorized access. CPHCS will provide authorized physical access to the inside of target locations for simulation of attacks that might be launched from within the physical security access control boundaries. This is strictly a wireless security assessment engagement and there is no expectation that the awarded contractor would also conduct an internal wired security assessment or that there would be any direct physical contact with the wireless access points.

Question #3:

"What is 'demarcation' for the wireless side of the audit? For example, is it considered a 'successful' wireless compromise to gain a layer three IP address on the local network segment? "

Answer:

For security purposes, the technical details of a compromise will only be disclosed to the awarded contractor. In general, a successful compromise would require establishing a network connection via the wireless network to a system that is protected by the wireless network. CPHCS will work with awarded contractor to define the technical details of a successful compromise. CPHCS does not consider obtaining an IP address itself a successful compromise; the assessor would have to leverage that IP address to establish a network connection via the wireless network with a system that is protected by the wireless network to qualify as a successful compromise.

Question #4:

"Point number seven of section 'D' says: 'Wireless network activity may be provided.' Could you please expound on the meaning of this statement?"

Answer:

Some wireless attacks require a sufficient amount of “interesting” packets to exploit a vulnerability and complete a compromise. If the assessor requires a certain number of interesting packets to complete the assessment, CPHCS would ensure that sufficient interesting packets would be produced during a specified time frame.

Question #5:

"How deep into confidential data do you want us to go? For example, is it necessary to penetrate into the laptops, Microsoft AD, or database information?"'

Answer:

CPHCS would consider establishing a network connection via the wireless network with a system that is protected by the wireless network a successful compromise. It would not be necessary to compromise the system and/or the data it may contain.

Question #6:

How many authorized Wireless Networks (SSIDs) will be included in this engagement?

Answer:

The RFO's Exhibit A (Statement of Work), Section C (Contractor Roles and Responsibilities), Item #9, states in part:

"Conduct and assessment and prepare a written report on the security of CPHCS' wireless networks at two (2) designated sites."

Two SSIDs will be active. Awardees will be given the two SSIDs prior to conducting the security assessment.

Question #6:

"How many unique Wireless Access Point (WAPs) and/or Wireless LAN Controllers (WLCs) will be included in this engagement?"

Answer:

Answered in Question # 5.

Question #7:

"Which of the following Wireless specifications is utilized by your organization?

- 802.11a
- 802.11b
- 802.11g
- 802.11n"

Answer:

The RFO's Exhibit A (Statement of Work), Section A (Contract Purpose and Description), 2nd sentence, states:

> *"As Part of the WLAN deployment CPHCS as developed a wireless security architecture to secure the planned 802.11 A/B/G/N wireless networks."*

All four Wireless specifications may be utilized by CPHCS.

Question #8:

"Please provide the following information about each of the locations where Wireless testing will occur:

- # of locations in-scope for the assessment
- Approximate square footage of each location
- # of Floors of each location"

Answer:

Please refer to Question #6 for a partial answer. The approximate square footage of each location and the number of floors of each location may be available through public information. The locations will be given to the awarded contractor, and any further information about the location (e.g., square footage or number of floors) must be obtained through public information.

Question #9:

"Will the configuration of Wireless Clients (Notebooks, PDAs, etc.) be included in this engagement? If so, please list each device and how many of each device will be included in this engagement.
Examples:
Notebook Computers – 3 unique builds

PDAs – 2 unique devices (Blackberry & Windows Mobile)
Wireless Phones – 5 these resides at support employees' desks"

Answer:

Please refer to Question #8 for a partial answer. All information concerning configuration of Wireless Clients must be obtained through any public information.

A Bidders Conference for this RFO is scheduled for November 12, 2009, from 11:00 a.m. to 12:00 p.m. The response submission due date is 5:00 P.M. (PST), November 20, 2009.

Thank you for your inquiries.