MASTER SERVICE AGREEMENT (MSA)
CALIFORNIA PRISON HEALTH CARE SERVICES
BUSINESS CONSULTING SERVICES

STATE OF CALIFORNIA
DEPARTMENT OF CORRECTIONS AND REHABILITATION

REQUEST FOR OFFER

INFORMATION TECHNOLOGY (IT) CONSULTING SERVICES
FEDERATED DATA CENTER – IT SERVICES
RFO #10-017-ITS

April 30, 2010

The California Department of Corrections and Rehabilitation (CDCR), California Prison Health Care Services (CPHCS), is requesting offers for Information Technology (IT) Consulting Services to evaluate, configure, and manage installation of all hardware, software, and related IT goods to a Tier III data center (a.k.a., Federated Data Center [FDC]). The FDC is located at the California Office of the State Chief Information Officer, Office of Technology Services (OTech), Gold Camp Data Center, Rancho Cordova, CA. Contractor will report to CPHCS' Chief Information Officer (CIO) or designee. In submitting an offer vendor must comply with the instructions found herein.

The term of the proposed Agreement is targeted for June 1, 2010 through August 15, 2011. CPHCS reserves the option to extend Agreement for two (2) additional one-year terms at the same rate of award and/or to add additional funds up to the maximum MSA threshold. The contract award is subject to availability of funds approved for this purpose.

All offers must be signed by an authorized officer of the company or firm who has legal and binding authority. By submitting an offer, Offeror agrees to the terms and conditions of this Request for Offer and in accordance with Offeror's Leveraged Procurement Agreement (i.e., Master Service Agreement [MSA]).

A walk-through of the proposed job site is required for all interested Offerors. The specific date, time, location, and CPHCS contact person will be provided by Addendum to RFO #10-017-ITS. CPHCS anticipates the mandatory one-day site review to occur week of May 3, 2010 through May 7, 2010.

Offers are due by **4:00 p.m., Monday, May 17, 2010**. **Responses and any required copies must be submitted by electronic mail (e-mail) and clearly labeled to the following departmental contact:**

Department Contact:
California Department of Corrections and Rehabilitation
Attention: CYNTHIA BASA-PINZON
P.O. Box 4038
Sacramento, CA 95812-4038
(916) 324-8045
Cynthia.Basa-Pinzon@cdcr.ca.gov

RESPONSE GUIDELINES

This RFO, Offeror's response, the State's General Provisions – Information Technology (GSPD 401IT, effective 04/12/2007), and applicable IT Personal Services Special Provisions will be made part of the ensuing Standard Agreement and contract file.

Offers must be submitted electronically to the departmental contact address noted on page 1. All pages of Offeror's response received prior to due date and time will be considered. CPHCS is not responsible for any e-mail loss and/or failure to receive an Offeror's response. CPHCS assumes no responsibility if Offeror cannot transmit their response electronically to the departmental e-mail address and/or if entire response is not received prior to RFO due date.

The delivery of any offer via U.S. mail, private delivery service, and/or by personal service will not be accepted by CPHCS. In the event of such delivery, CPHCS may consider the offer as non-responsive.

Offers submitted in response to this RFO must include all of the following information:

1. Cover letter signed by the authorized officer of the company or firm who has legal and binding authority;

2. Full legal name of Offeror's organization or firm, mailing address, telephone and facsimile numbers;

3. Name, telephone number, and electronic mail (i.e., e-mail) address of Offeror's contact person;

4. Submission date of Offer;

5. A copy of Offeror's MSA that includes the California Department of General Services (DGS) logo, MSA number, term and DGS' signature approval;

6. Copy of Liability Insurance Certificate;

   Offeror must provide CPHCS with a Certificate of Insurance showing that there is liability insurance currently in effect for Offeror of not less than $1,000,000, per occurrence, for bodily injury and property damage liability combined. The Certificate of Insurance must include the following provisions:

   a. The insurer will not cancel the insured's coverage without 30 days prior written notice to the State;[1] and

   b. The State of California is included as additional insured.

7. Proof of Worker's Compensation Insurance;

   Offeror shall provide CPHCS with a Certificate of Insurance showing that there is current workers' compensation insurance coverage for its employees who will be engaged in performance of the requested services. The Certificate of Insurance must include the provision that insurer will not cancel the insured's coverage without 30 days prior written notice to the State.

[1] "Days" means calendar days unless otherwise specified.

8. Completed Rate Sheet (Exhibit B-1);

   Exhibit B-1 (Rate Sheet) must provide: 1) quantity of commodity/product; 2) description of commodity/product; 3) service description/deliverable; 5) personnel classification; 6) estimated hours per service/deliverable; 7) price [per service/deliverable]; 8) annual maintenance and support (e.g., training) cost; and 9) total cost. The ensuing Agreement will be invoiced and reimbursed on a deliverable (i.e., fixed cost) basis.

   a. An example of Offeror's proposed Rate Sheet (Exhibit B-1) has been included within RFO (page 21).

   Any modifications to SOW of the ensuing Agreement will be defined, documented and mutually agreed upon by Contractor and CIO, or designee, and will be paid based on a time and materials rate or fixed-cost as proposed on Exhibit B-1 (Rate Sheet).

9. Offeror Declaration Form (GSPD-05-105);

   Not applicable. For purposes of this RFO, subcontracting of proposed services will not be permitted.

10. Contractor's Small Business and/or Disabled Veteran's Business Enterprise Certification, if applicable;

11. Completed Payee Data Record (STD 204) - (Attachment A);

12. A detailed description of Contractor's approach for completing the services requested in Exhibit A (Statement of Work), Section C (Scope of Services) including, but not limited to, the functions, roles, and responsibilities of vendor personnel;

13. A description of Offeror's expertise and experience (e.g., type of services rendered, manufacturer relationship(s), industry-related certifications, etc.) performing IT consulting services as requested in Exhibit A (Statement of Work).

    Offeror's description of expertise and professional experience(s) must include all of the following:

    a. A description of at least one project that involved use of Nexus VDC's (maximum three pages);

    b. A description of at least one project that involved use of Cisco ASA contexts, preferably for a MSSP (maximum two pages);

    c. A description of at least two projects that involved use of Cisco Security Manager with a deployment of ASA's (maximum of two pages);

    d. A description of at least one project that involved use of Cisco Access Control Server in a multi-vendor environment (maximum one page); and

    e. A description of at least two projects that used Tipping Point Controllers and stacked 2500N or 5100N IPS, preferably in a 10Gbps environment and active-active mode (maximum two pages).

14. Three (3) customer references for Offeror to verify engagement(s) similar in scope as requested in Exhibit A (Statement of Work);[2]

    a. Include a brief narrative of customer projects and Offeror's role for each reference provided; and

    b. Include a reference from Cisco indicating Offeror's (i.e., company or firm) "Partner" level (e.g., Gold or Platinum) and performance history with similar projects.

15. Resumes of Contractor personnel must include all of the following:

    a. All relevant work experience;

    b. A start and end date for each job cited;

    c. Three (3) customer references to verify engagements similar in scope to FDC; and

    d. Consultant qualifications and experience(s) in performing network installation and configuration services.

16. Copies of pertinent IT certifications acknowledging skills and competency in project development; or network installation and configuration; or system analysis, design, and implementation.

17. Other Requirements:

    Contractor will be required to complete the following documents prior to award.

    Do not submit the following with your response.

    a. Contractor Confidentiality Statement (Attachment B):

       The Political Reform Act of 1974 (Government Code Sections 81000-91015) requires consultants to file a Contractor Confidentiality Statement certifying no personal or financial interest with the UHRC Project and agreeing to keep all information concerning the project confidential.

    b. Non-Disclosure Agreement (Attachment C)

    c. Statement of Economic Interests (Form 700) - (Attachment D)

Interested vendors may submit questions and/or requests for clarification, via e-mail, to Cynthia.Basa-Pinzon@cdcr.ca.gov. CPHCS responses to Offeror questions that provide new or additional information will be provided to all Offerors.

[2]Customer references will be used to verify information provided by Offeror for selection purposes.

KEY DATES

Event	Date	Time
Release of Request for Offer	04/30/2010	
Federated Data Center Site Walkthrough	05/03/2010 - 05/07/2010	
Questions or Clarifications Submittal (latest date)	05/10/2010	4:00 p.m.
Offer Response Submission Due Date	05/17/2010	4:00 p.m.
Comparison of Offers and Interview(s), if warranted	5/19/2010 – 05/21/2010	
Best Value Determination – Selection of Vendor	05/24/2010	4:00 p.m.
Proposed Contract Start Date[3]	06/01/2010	

[3] Dates subject to change

SELECTION PROCESS

All offers will be reviewed for responsiveness to requirements of this RFO. If a response is missing required information, it may be deemed non-responsive. Responsive offers will be scored on the "Best Value" criteria listed below. Further review is subject to CPHCS' discretion.

Best Value Criteria	
Technical Experience:	40 Points
• Certified Cisco Gold Partner;	0-5
• Experience with network installation and configuration of Cisco Nexus products;	0-5
• Experience with network installation and configuration of Tipping Point IPS products;	0-5
• Experience with network installation and configuration of Cisco CSM and ACS products;	0-5
• IT career certification acknowledging skills and competency in a specialized area;	0-5
• At least five (5) years experience performing network configuration, installation, and project management consulting services; and	0-10
• Knowledge of state IT policy and governance processes.	0-5
Administrative Criteria:	20 Points
• Completeness of response package;	0-5
• Detailed resumes for contractor personnel describing qualifications and work experience(s) that support Statement of Work (Exhibit A) requirements;	0-5
• Three (3) references for Offeror and/or company or firm;[4] and	0-5
• Offices with engineering resources located in the greater Sacramento region.	0-5
Cost:	40 Points
• Lowest cost proposal will receive full cost points and each proposal with higher cost will receive a percentage of total points.	0-40

CPHCS reserves the sole right to reject any and all offers, and reissue this RFO. In the event CPHCS determines that services would be best served by awarding multiple agreements for this RFO, CPHCS reserves the right to make this determination and negotiate with Offerors having "best value" to award more than one company and/or firm. Awarded Contractor(s) will be obligated to provide services at the cost offered in the Rate Sheet (Exhibit B-1), which under no circumstances may exceed their authorized MSA rate(s).

[4] Customer references must support consultative services offered.

EXHIBITS AND ATTACHMENTS:

Exhibit A	Statement of Work
Exhibit B	Budget Detail and Payment Provisions
Exhibit B-1	Rate Sheet
Exhibit C	CPHCS Special Provisions
Attachment A	Payee Data Record (STD 204)
Attachment B	Contractor Confidentiality Statement
Attachment C	Non-Disclosure Agreement
Attachment D	Statement of Economic Interests (Form 700)
Attachment E	Glossary of Acronyms
Attachment F	Multi-Tenant Environment
Attachment G	Standard POD

EXHIBIT A
STATEMENT OF WORK

A) BACKGROUND AND PURPOSE

The California Prison Health Care Receivership Corporation is a non-profit organization created to house activities of the Federal Receiver. United States District Court Judge, Thelton E. Henderson, established the Receivership as the result of a 2001 class action lawsuit (Plata v. Schwarzenegger) brought against the State of California over the quality of medical care in the State's prison system.

On June 6, 2008, federal Receiver, J. Clark Kelso, issued a plan called "Achieving a Constitutional Level of Medical Care in California's Prisons" (Plan), available at http://www.cphcs.ca.gov/docs/court/ReceiverTurnaroundPlan_060608.pdf. This Plan calls for numerous actions to be performed over the next three-to-five years by California Prison Health Care Services (CPHCS) program to meet constitutionally acceptable and sustainable levels of patient-inmate medical care.

All activities of the Receivership have one common purpose: to create a collaborative environment where custody and health care staff improve upon the quality of medical services in California prisons to meet constitutional standards while reducing avoidable morbidity and mortality. The Receiver has also adopted organizational change strategies suggested by the Institute of Medicine (Crossing the Quality Chasm, A New Health System for the 21st Century, Washington D.C., National Academy Press, 2001). One strategy is to improve CDCR's information technologies for clinical information and decision support.

To increase government efficiency through improvements to California's IT systems, the Receiver has dedicated resources to adhere to objectives the Governor has communicated in Executive Order (EO) S-03-10, dated February 9, 2010. The EO requires a standardization of IT governance, increased transparency in spending for cost savings, and reduced energy usage from IT operations. Specific improvements include, but are not limited to: 1) a reduction of total data center square footage by 25 percent before July 2010; and 2) transition of all mission critical and public-facing applications to a Tier III data center (i.e., Federated Data Center). The FDC is intended to be the gateway or transition environment from a discreet, standalone server environment to a virtualized environment sharing storage, network, and ultimately computing resources. .

To establish the FDC, CPHCS seeks a qualified Contractor with four (4) Senior Technical Leads to evaluate, configure, and manage installation of all hardware, software, and related IT equipment for back-up of all mission critical and public-facing applications to a Tier III data center.

B) CONSULTANT QUALIFICATIONS

Contractor must meet the following Mandatory Qualifications to be considered for award. Offerors will be evaluated on expertise and experience stated in the resume against the Mandatory Qualifications. At discretion of CPHCS, interviews may be a part of the selection process.

Mandatory Qualifications:

1. Certified Cisco Gold Partner;
2. Experience with network installation and configuration of Cisco Nexus products;
3. Experience with network installation and configuration of Tipping Point IPS products;

4. Experience with network installation and configuration of Cisco CSM and ACS products;
5. IT career certification acknowledging skills and competency in a specialized area;
6. At least five (5) years experience performing network configuration, installation, and project management consulting services; and
7. Knowledge of state IT policy and governance processes.

In addition to the above Mandatory Qualifications, Contractor personnel must meet the following requirements to be considered for award:

Senior Technical Leads (Network Engineers):

CPHCS seeks two (2) network engineers. One Network Engineer will focus on Nexus 7000 configurations while the second engineer deploys Nexus 5020/2248 switches.

The following are requirements for the Nexus 7000 Network Engineer (i.e., Senior Technical Lead).

1. Ten (10) years or more of IT networking experience;
2. A minimum of two (2) deployments as Lead Network Engineer, or equivalent, where Nexus 7010 switches were implemented;
3. Ability to translate Cisco IOS based router and switch templates to NX-OS based router and switch templates;
4. Experience working with Cisco MPLS VRF's including VRF Lite and Multi VRF;[5] and
5. Current Cisco Routing/Switching CCIE or Service OTech CCIE certification (or above).

CPHCS seeks one (1) Nexus 5020/2248 Network Engineer for the access portion of the network.

The following are requirements for the Nexus 5020/2248 Network Engineer (i.e., Senior Technical Lead):

1. Ten (10) years or more of IT networking experience;
2. A minimum of two (2) deployments as Senior Network Engineer, or equivalent, where Nexus 5020/2248 switches were implemented;
3. Experience working with Cisco MPLS VRF's including VRF Lite and Multi VRF;[5] and
4. Current Cisco Routing/Switching CCIE or Service OTech CCIE certification (or above).

Senior Technical Lead (Network Security Engineer):

CPHCS seeks a Network Security Engineer with extensive multi-vendor experience. Experience must include a blend of Cisco router and switch security, and two-to-three non-Cisco firewall vendor technologies.

The following are requirements for the Network Security Engineer (i.e., Senior Technical Lead):

1. Ten (10) years or more of network security experience;
2. Firewall experience using Cisco PIX, Cisco ASA, and Juniper Netscreen;
3. SSL VPN experience using Cisco ASA;
4. Experience working with Cisco Security Manager and Cisco Secure ACS software;
5. Current CISSP certification (or above); and

[5] This requirement can be satisfied by either Network Engineer.

6. Knowledge and experience with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) relating to network security.

Senior Technical Lead (IPS Security Engineer):

CPHCS seeks an IPS Security Engineer with extensive Tipping Point IPS and multi-vendor IPS experiences.

The following are the requirements for the IPS Security Engineer (i.e., Senior Technical Lead):

1. Ten (10) years or more of network security experience;
2. Experience with Tipping Point Controllers, N Series IPS, and Security Management System;
3. Experience building Managed Security Service OTech (MSSP) environments;
4. Current CISSP certification (or above); and
5. Knowledge and experience with HIPAA relating to network security.

Desirable Qualifications:

In addition to the above Mandatory Qualifications, the following are desirable Contractor qualifications:

1. Ability to plan, schedule, and/or manage workload to meet project deliverables involving network configuration, integration, and deployment of IT equipment;
2. Knowledge of installation, maintenance, operations and repair of IT equipment;
3. Experience installing IT equipment within a Tier III data center;
4. Knowledge of project management principles and techniques; and
5. Knowledge of CPHCS and/or CDCR operations.

Desirable Network Security Engineer qualifications:

1. Current JNCIA-FW certification;
2. Current Cisco Security CCIE certification; and
3. Current HIPAA certification.

Desirable IPS Security Engineer qualifications:

1. Tipping Point Trainer – Expert Level; and
2. Current HIPAA certification.

C) SCOPE OF SERVICES

The Scope of Services (Scope) includes the design evaluation, configuration, and implementation of the following Bill of Materials, and specific deliverables to be performed by Contractor.[6]

- For reference purposes, the following attachments have been included:
  - Attachment E – Glossary of Acronyms;
  - Attachment F – Multi-Tenant Environment; and
  - Attachment G – Standard POD.

[6] Diagrams of cabinets and cabinet layout will be provided to Offerors during mandatory walkthrough.

1. BILL OF MATERIALS

The following IT networking equipment is to be used in the FDC deployment:

A. Cisco LAN Equipment

a. Two (2) ASR1006 routers (for FDC/OTech border/edge) each have:
- Redundant power supply;
- Redundant processors;
- Four (4) 10GB MM Ports; and
- Ten (10) 1000-Base-SX Ports.

b. Eight (8) Nexus 5020 switches (two pairs for each POD) each have:
- Redundant power supply; and
- Fifty-two (52) 10Gig ports:
  - 36 for servers;
  - 4 for the HP VC connections;
  - 4 for links to the 7010s; and
  - 8 unallocated 10gig ports;

c. Six (6) Cisco Nexus 7010 switches (one pair for the Core, one pair for POD distribution with two PODs planned) each have:
- N+1 redundant power supply;
- Fabric;
- RPs;
- Sixty-four (64) 10Gig SR Ports (two [2] 32-Port 10Gig cards with sixty-four [64] 10Gig SFPs);
- Forty-eight (48) 1000Base-SX (1Gig) Ports (One [1] 48-Port 1Gig card with forty-eight [48] 1000BaseSX SFPs); and
- An option of four (4) 1000T SFPs for any copper needed in the Core or POD distribution.

d. Fifty-eight [58] Nexus 2000 fabric extenders (two for each server cabinet without blade chassis, twenty-four [24] standalone server cabinets) each have:
- Fifty-six (56) 100/1000 ports; and
- Two (2) 10GE ports with SR SPFs.

e. Two (2) Cisco ACS 5.1 VMWare installations with base license (for network device authentication).

f. Two (2) Cisco Security Manager 3.3 installations (for firewall and network security management)

B. CISCO Security Equipment (Firewall and VPN)

A. One (1) ASA5520 Cisco HA VPN pair with 50 VPN user licenses;
B. Three (3) ASA 5580-40 Cisco ASA HA Firewall pairs each have:
- Six (6) 10G MM ports;
- Eight (8) 1 Gig MM ports; and
- Fifty (50) Security Contexts (i.e., licenses).

C. Two (2) Cisco Security Manager installations for up to 150 devices.

C. Tipping Point Security Manager

3	Tipping Point 2500N – 3Gigabit Processing
3	Tipping Point Core Controller Base Chassis
18	Tipping Point 10 Gigabit XFP Short Range SFP

9	Tipping Point ZPHA Partner SR for 1-10Gigabit Segment Kit SR
1	Tipping Point SMS Security Management System

D. Western Telematic Inc.

6	Western Telematic Inc.	TSM-24	Console Server, 8 port, AC Power

E. HP – Out of Band

12	J8712A	ProCurve Switch zl 875W Power Supply
6	J8702A	24-port 10/100/1000 PoE module for 5400 switches
144	J4858C	ProCurve Gigabit SX-LC Mini-GBIC
6	J8706A	ProCurve Switch zl 24p Mini-GBIC Module
42	J9145#ABA	Lan Device, 24 Port Gig Ethernet
84	J4858C	ProCurve Gigabit SX-LC Mini-GBIC
6	J8994A	Premium Edge License for Switch 5400 Series

F. Brocade – SAN Fabric

2	DCX Directors

Note: Where products must be installed on or with a server, one will be provided by CPHCS with the requisite specification and OS.

2. SPECIFIC DELIVERABLES

Contractor will be required to perform specific deliverables that include, but are not limited to, upgrading to OS levels upon approval by the FDC Engineering Team, or designee(s), and creating and validating configurations based on the design document and existing IOS-based router and switch templates.

- Installation of network hardware is <u>not</u> included in the Scope.
- In the event Contractor fails to perform any of the following deliverables due to fault or negligence of Contractor, CPHCS may impose Section 1.a., of the State Model IT Purchase Special Provisions (Liquidated Damages), which will be incorporated by reference in the ensuing Agreement.

Contractor is required to perform all of the following:

A. NETWORK DESIGN REVIEW

The network design will be completed by the FDC Engineering Team prior to commencement of the ensuing Agreement. A period of three (3) weeks has been scheduled for design review.

Design review includes, but is not limited, to all of the following:

a. Review of FDC project design including goals and assumptions;
b. Review of existing IOS-based templates;
c. Questions and answers from contractor(s) to FDC design team;
d. Recommended changes from contractor(s); and
e. Final approval of design.

B. CISCO NEXUS 7010 SWITCHES

Contractor shall perform all of the following services to a pair of Cisco Nexus 7010 switches at the Core and each pair of 7010's located at each POD:

a. Create up to 4 VDCs per Nexus 7010 including administration VDC;
b. Set VDC resource allocation as directed by design document;
c. Configure VRFs at the Core Nexus 7010 as directed by design document;
d. Configure interfaces, routing and HA according to design document ;
e. Prevent the following attack types:
    - o DDoS attacks to the 7010 (Control Plane Policing);
    - o Spanning-tree loops (BPDU Guard);
    - o MAC floods (Port-Security); and
    - o Broadcast floods (Storm Control).
f. Configure SNMP v3 and Traps using settings provided by design document;
g. Configure QoS as directed by design document; and
h. Configure, test, and document availability:
    - o ISSU;
    - o GOLD;
    - o EE; and
    - o Call Home.

C. CISCO ASR 1006 ROUTERS

Two Cisco ASR 1006 routers will connect the FDC to Internet and WAN. This connection will be on a single cable and use VRF's to separate Internet to FDC tenant agencies. OTech will provide a primary and secondary connection, one connection to each router.

All of the following services will be performed for each of the Cisco ASR 1006 routers:

a. Physically connect OTech handoffs to ASR routers;
b. Configure primary and backup 10Gbps connections to OTech including Dot1q trunking;
c. VRF Lite to OTech router;
d. Configure BGP for each VRF and test connectivity to OTech:
    - o Test internet; and
    - o Test agency VRF connectivity as indicated in design document.
e. Customize, as necessary, and apply standard Internet Router security template as indicated in design document;
f. Configure SNMP v3 and Traps using settings provided by design document; and
g. Configure QoS as directed by design document.

D. CISCO NEXUS 5020/2248T SWITCHES

There will be four (4) Nexus 5020 switches in each of the two PODs, for a total of eight (8). There will also be up to fifty (58) Nexus 2248 Top of Rack switches in the FDC.

Contractor shall perform all of the following services:

a. Prevent the following attack types:
    - o Spanning-tree loops (BPDU Guard);
    - o MAC floods (Port-Security); and
    - o Broadcast floods (Storm Control);
b. Enable common error detection (errdisable) ;
c. Configure SNMP v3 and Traps using settings provided by design document;
d. Configure QoS as directed by design document; and

e. Configure miscellaneous management such as Syslog, NTP, etc., as directed by design document.

E. HP PROCURVE OUT-OF-BAND ACCESS SWITCHES

There will be six (6) HP Procurve 5400 for OOB access primarily used for ILO connectivity.

Contractor shall perform all of the following services on the HP Procurve switches:

a. Configure VLAN's and IP addresses for ILO subnet(s);
b. Apply standard security template as defined in design document; and
c. Test basic connectivity.

F. WTI TS-8 TERMINAL SERVER

The FDC will have six (6) WTI TS-8 terminal servers used solely for network device console access.

Contractor shall perform all of the following services for the terminal servers:

a. Connect to network with appropriate IP;
b. Cable all network devices to the TS-24; and
c. Test access to all consoles.

G. CISCO ASA 5580-40 FIREWALLS

The FDC has four (4) sets of firewalls. Each set is an HA pair. There is an external, public facing HA pair, two "POD" HA pairs, and an SSL VPN pair.

Contractor shall perform all of the following services for each firewall:

a. Configure three (3) HA clusters (one Internet facing edge and two PODs);
b. Configure five (5) contexts on each HA pair including a test agency VDOM on each pair;
c. Implement context CPU/Memory and other restrictions as indicated in design document;
d. Configure Cisco Security Manager to manage images, versions, role based access control, and reporting; and
e. Configure SSL VPN as an HA pair and ACS as the FDC user authentication server.
    - Specific access requirements will be provided in design document.

H. TIPPING POINT INTRUSION PREVENTION SYSTEM (IPS)

There will be four (4) TP Core Controllers, four (4) TP 2500N IPS, and one (1) Security Management System. These devices are expected to be placed inline.

Contractor shall perform all of the following services for each sensor:

a. Configure the Controllers in two separate HA pairs (one HA pair in each POD);
b. Configure the 2500Ns in two separate HA pairs set to an active-active state;
c. Enable full IPS for all inbound traffic to public facing servers on edge firewalls:
    - Obtain list of public facing servers including IPs/Networks, OS, and application types;
    - Enable signatures and actions per best practices; and
    - Tune according to types of OS's and applications for optimal security, and performance.

d. Enable signatures and actions at the POD level as directed by design document; and
e. Configure TP Security Management System (SMS) in a Managed Security Service Provider type environment to allow up to four (4) tenants to manage and maintain the IPS as it pertains to their networks.

I. CISCO ACCESS CONTROL SERVER (ACS)

The Cisco ACS will initially be used for network device access only. There will not be any external database integration.

Contractor shall perform all of the following services to the ACS:

a. Install and configure (2) Cisco ACS servers to specifications provided in design document;
b. ACS should be configured as an HA pair and synchronized;
c. Disable HTTP and enable HTTPS using self-signed cert;
d. Create and organize AAA clients based on tenants and their devices using device groups and user groups;
e. Configure tenant administrators with access only to specific device groups and user groups;
f. Add tenant user accounts with strong password enforcement and requirement to change password;
   - Password list to be provided to FDC engineering team.
g. Enable option to allow tenant users to change their password;
h. Patch ACS to latest patch levels;
i. Add all BOM devices that are TACACS+ or RADIUS capable including routers, switches, firewalls, security software, out-of-band management, terminal servers, etc.; and
j. Configure AAA on all network devices as directed by design document.

J. CISCO SECURITY MANAGER (CSM)

Contractor shall configure Cisco CSM deployment to manage the ASA firewalls per best practices including, but not limited to, all of the following:

a. Install and configure (2) Cisco Security Managers version 3.3 or, if available, version 4.0;
b. CSM should be configured as an HA pair, and synchronize if possible;
c. Patch CSM's up to latest patch levels;
d. Add all Cisco ASA contexts to CSM; and
e. Configure role-based access control to allow tenants to manage and monitor their ASA contexts, and integrate with Cisco ACS.

K. KNOWLEDGE TRANSFER

Contractor will provide CPHCS and CDCR personnel (e.g., Federated Engineer Team) with informal training and knowledge transfer as follows:

a. Conduct up to five (5) working days of training and knowledge transfer; and
b. Review all deliverables with Federated Engineer Team.

L. WARRANTY AND MAINTENANCE SERVICES

Contractor shall provide twelve (12) months of Warranty on all initial IT configuration services. The Warranty period will commence upon completion of all design

evaluation, configuration, and implementation deliverables as set forth in Exhibit A (Statement of Work) to the satisfaction of CPHCS representative(s).

Contractor shall also provide up to 760 hours of Maintenance services for twelve (12) months after CPHCS' final system acceptance including all of the following:

a. The first two weeks following CPHCS' final system acceptance will include 160-hours of on-site support and maintenance for CPHCS' FDC transition to maintenance and operations;
b. An additional two weeks of 160-hours off-site support and maintenance after completion of the initial on-site support;
c. Ongoing Maintenance services will be authorized through a Work Authorization process;
d. CPHCS will commit minimum of ten (10) hours per month, and a maximum of forty (40) hours per month, of Maintenance services on the condition that personnel of the initial Contractor are utilized for ongoing maintenance and support services; and
e. Any damage caused by Contractor to Gold Camp FDC shall be repaired by Contractor, at Contractor's expense, to the satisfaction of OTech and CPHCS representative(s).

M. WORK AUTHORIZATION

Either party may at any time propose a change to Scope. If Contractor believes that such change will increase Contractor's costs or delay completion, the parties will negotiate in good faith to try to accommodate such requests. Contractor will price any additional fees, at CPHCS' option, based on time and material rate(s) or fixed cost. Contractor will disclose and explain to CPHCS its method of pricing a change order. At CPHCS' request, the parties will use project estimation tools to aid in determining pricing and to ensure that it is competitive in the marketplace. No change will be effective unless and until set forth in a written amendment to the Agreement, which is approved and signed by the parties. Any agreed upon modifications will be performed by Contractor in accordance with the amendment and Agreement provisions. Any failure to agree to a proposed change will not impair the enforceability of other Agreement terms or in Scope.

D) PROJECT ASSUMPTIONS AND CONSTRAINTS

1. The work location will be the California Office of the State Chief Information Officer, Office of Technology Services (OTech), Gold Camp Data Center, Rancho Cordova, CA.
   a. Preliminary timeline for establishing FDC operations is from April 2010 through August 2010 (i.e., from procurement of goods/services, to network infrastructure, to implementation, to FDC readiness date).
2. Gold Camp data center has adequate power (i.e., terminals to electrical box are live), installed overhead cable raceway and ladder racking, and under floor power whips.
   a. Structured cabling design and/or installation are not included in this RFO.
   b. All equipment to be installed shall be new and the latest model in current production.
3. Work hours for this Agreement must be consistent with CPHCS normal business hours 8:00 a.m. to 5:00 p.m., Monday through Friday, excluding State holidays.

4. Contractor's performance of deliverables may occur during or outside normal business hours only upon prior written approval from CPHCS' CIO or designee.
    a. Contractor shall comply with OTech's and/or CPHCS' requirements that may require equipment deliveries are within defined time frames due to security policies.
5. Any modifications of the ensuing Agreement's Scope will be defined, documented and mutually agreed upon by Contractor and CIO or designee.
6. Services not specified in Scope may only be performed pursuant to a work authorization signed by CPHCS. In no event will the total amount paid for such work exceed ten percent (10%) of the value of IT consulting services required by the ensuing Agreement.
7. Contractor must submit, in advance, a resume of all personnel substitutions. All Contractor substitutions must be approved by CPHCS' CIO or designee prior to commencement of work.
8. CPHCS, in its sole discretion, reserves the right to require Contractor to substitute personnel.
9. CPHCS reserves the right to renegotiate services deemed necessary to meet FDC needs according to State priorities. CPHCS and Contractor shall mutually agree to all changes; and renegotiated services outside the Scope may require control agency approval prior to commencement of work.
10. CPHCS and Contractor are mutually obligated to keep open channels of communications to ensure successful performance of the awarded Agreement. Both parties will be responsible for communicating any potential problem(s) or issue(s) to CPHCS' CIO and the Contractor, respectively, within two (2) hours of becoming aware of said problem(s).
11. Contractor certifies that it has appropriate systems and controls in place to ensure that State funds will not be used in performance of this Agreement for the acquisition, operation, or maintenance of computer software in violation of copyright laws.

E) <u>CPHCS ROLES AND RESPONSIBILITIES</u>

1. CPHCS will provide Contractor with a floor plan of the Gold Camp data center showing FDC location and each item of IT equipment to be installed.
2. CPHCS will be responsible for receiving, reviewing, and monitoring installation of FDC goods and services.
3. CPHCS will help resolve and escalate configuration issues as necessary.
4. CPHCS will be responsible for any delay, cost increase, or other consequence(s) caused by CPHCS' failure to fulfill its responsibilities as set forth herein.
    a. In the event of any claim for equitable adjustment to price, schedule, or both, the parties will negotiate in good faith regarding execution of an amendment; and
    b. If Contractor determines that a delay exists or is probable due to a failure of CPHCS, Contractor will promptly notify CPHCS in writing.

CPHCS will provide Contractor access to FDC for the IT consulting services described herein.

F) CONTRACTOR ROLES AND RESPONSIBILITIES

In addition to Scope of Services specified in Item C above, Contractor is required to do all of the following:

1. Comply with all applicable State and Agency policies and procedures, including those enumerated in Exhibit C (Special Provisions). By accepting an Agreement, Contractor acknowledges and agrees to provisions of Exhibit C;
2. Return all State property including security badges, computer laptop, work products, etc., prior to termination of the Agreement;
3. Complete an Application for Identification Card, and/or Emergency Notification form to gain entrance to the FDC; and
4. Perform any other duties as requested by CPHCS' CIO or designee.

G) PERIOD OF PERFORMANCE

The term of the proposed Agreement is targeted for June 1, 2010 through August 15, 2011. CPHCS reserves the option to extend Agreement for two additional one (1) year terms at the same rate of award, and/or to add additional funds up to the maximum MSA threshold. The contract award is subject to availability of funds approved for this purpose.

H) EVALUATION OF CONTRACTOR

The Chief Information Officer, or designee, will complete a written evaluation of Contractor's performance under the ensuing Agreement within sixty (60) days following the term end date. The evaluation shall be prepared on the Contract/Contractor Evaluation Form (STD 4) and maintained in the Agreement file for three (3) years. If Contractor's performance is deemed unsatisfactory, a copy of the evaluation shall be sent to the California Department of General Services (DGS), Office of Legal Services (OLS), within five (5) days, and to Contractor within fifteen (15) days, following completion of the evaluation.

"Days" means calendar days unless otherwise specified.

I. TERMINATION

The CPHCS reserves the right to terminate the ensuing Agreement if services are no longer required. Termination provisions in the ensuing Agreement will be subject to the State's General Provisions – IT (GSPD401-IT, effective 04/12/2007).

J. CPHCS CONTRACT MANAGER

CHIEF INFORMATION OFFICER
California Prison Health Care Services
P.O. Box 4038
Sacramento, California 95812-4038

EXHIBIT B
BUDGET DETAIL AND PAYMENT PROVISIONS

1. INVOICING AND PAYMENT

For services satisfactorily rendered, and upon receipt and approval of an invoice, CPHCS agrees to reimburse Contractor on a fixed-price deliverable basis in accordance with Exhibit B-1 (Rate Sheet).

Contractor shall submit an invoice in triplicate (with original signatures in blue-ink) specifying work delivered, number of hours performed, cost, and any outstanding issues and/or concerns that need to be addressed.

a. Invoices for reimbursement on a deliverable basis shall not be submitted more frequently than monthly in arrears and payments will not exceed ninety percent (90%) of the total price (i.e., deliverable cost). The ten percent (10%) withholding will be payable upon completion of all deliverables and final acceptance by CPHCS.

Invoices shall be submitted with all supporting documentation that properly details all charges. Contractor's invoices submitted to CPHCS must identify the Agreement number. Any invoice submitted without the above referenced information may be returned to Contractor for re-processing.

Upon completion of services to the satisfaction of CPHCS, Contactor shall address and submit invoice to the following:

CHIEF INFORMATION OFFICER
Information Technology Services Division
California Prison Health Care Services
P.O. Box 4038
Sacramento, California 95812-4038

2. BUDGET CONTINGENCY CLAUSE

a. It is mutually agreed that if the California State Budget Act for the current fiscal year and/or any subsequent fiscal years covered under this Agreement does not appropriate sufficient funds for the project, this Agreement shall be of no further force and effect. In this event, the State shall have no liability to pay any funds whatsoever to Contractor, or to furnish any other considerations under this Agreement and Contractor shall not be obligated to perform any provisions of the Agreement.

b. If funding for purposes of this project is reduced or deleted for any fiscal year by the California State Budget Act, the State shall have the option to either cancel the Agreement with no liability occurring to the State, or offer an Agreement amendment to Contractor to reflect the reduced amount.

3. PROMPT PAYMENT CLAUSE

Payment will be made in accordance with, and within the time specified in, Government Code Chapter 4.5, commencing with Section 927. Payment to small/micro businesses shall be made in accordance with and within the time specified in Chapter 4.5, Government Code 927 et seq.

4. TRAVEL AND MISCELLANEOUS EXPENSES

For purposes of this RFO, all travel related expenditures are the sole responsibility of bidders.

EXHIBIT B-1
RATE SHEET

Contractor hereby agrees to provide all labor and transportation necessary to perform installation services in accordance with the Statement of Work and the Terms and Conditions of the Agreement.

Upon completion of all deliverables to the satisfaction of CPHCS, Contractor services shall be billed and reimbursed on a deliverable basis (i.e., fixed-price) unless otherwise specified.

QTY	COMMODITY/PRODUCT CODE	SERVICE DESCRIPTION	PERSONNEL CLASSIFICATION	EST. # HOURS[7]	DELIVERABLE PRICE[8]
1	Cisco Nexus 7010 Switches				
2	Cisco ASR 1006 Routers				
8	Cisco Nexus 5020/2248T Switches				
6	HP Procure Out-of-Band Access Switches				

Subtotal $_____

Annual Maintenance and Support (480 hours)[9] +_____

Total Costs **$**_____

EXAMPLE

[7]Estimated number of hours and hourly-rate are for information and staffing purposes only, and will not be subject to evaluation.
[8]Offeror is required to submit pricing for consulting services of each commodity/product as listed in Exhibit A.
[9] Offeror may provide costing for annual maintenance and support either on a fixed-price basis or hourly basis.

EXHIBIT C
CDCR SPECIAL PROVISIONS

1. ACCOUNTING PRINCIPLES

The Contractor will adhere to generally accepted accounting principles as outlined by the American Institute of Certified Public Accountants. Dual compensation is not allowed; a Contractor cannot receive simultaneous compensation from two or more funding sources for the same services performed even though both funding sources could benefit.

2. SUBCONTRACTOR/CONSULTANT INFORMATION

Contractor is required to identify all subcontractors who will perform labor or render services in the performance of the Agreement. Additionally, the Contractor shall notify the CPHCS, DCIO, within ten (10) working days, of any changes to the subcontractor and/or consultant information.

3. EMPLOYMENT OF EX-OFFENDERS

a. Contractor cannot and will not either directly, or via a subcontracted consultant and/or firm, employ in connection with this Agreement:

   (1) Ex-Offenders on active parole or probation;

   (2) Ex-Offenders at any time if they are required to register as a sex offender pursuant to Penal Code Section 290 or if such ex-offender has an offense history involving a "violent felony" as defined in subparagraph (c) of Penal Code Section 667.5; or

   (3) Any ex-felon in a position which provides direct supervision of parolees.

b. Ex-Offenders who can provide written evidence of having satisfactorily completed parole or probation may be considered for employment by the Contractor subject to the following limitations:

   (1) Contractor shall obtain the prior written approval to employ any such ex-offender from the Authorized Administrator; and

   (2) Any ex-offender whose assigned duties are to involve administrative or policy decision-making; accounting, procurement, cashiering, auditing, or any other business-related administrative function shall be fully bonded to cover any potential loss to the State of California.

4. LICENSES AND PERMITS

The Contractor shall be an individual or firm licensed to do business in California and shall obtain at Contractor's expense all license(s) and permit(s) required by law for accomplishing any work required in connection with this Agreement.

In the event any license(s) and/or permit(s) expire at any time during the term of this Agreement, Contractor agrees to provide the CPHCS with a copy of the renewed license(s) and/or permit(s) within thirty (30) days following the expiration date. In the event the Contractor fails to keep in effect at all times all required license(s) and permit(s), the

State may, in addition to any other remedies it may have, terminate this Agreement upon occurrence of such event.

5. CONFLICT OF INTEREST

The Contractor and their employees shall abide by the provisions of Government Code (GC) Sections 1090, 81000 et seq., 82000 et seq., 87100 et seq., and 87300 et seq., Public Contract Code (PCC) Sections 10335 et seq. and 10410 et seq., California Code of Regulations (CCR), Title 2, Section 18700 et seq. and Title 15, Section 3409, and the Department Operations Manual (DOM) Section 31100 et seq. regarding conflicts of interest.

a. Contractors and Their Employees

Consultant Contractors shall file a Statement of Economic Interests, Fair Political Practices Commission (FPPC) Form 700 prior to commencing services under the Agreement, annually during the life of the Agreement, and within thirty (30) days after the expiration of the Agreement. Other service Contractors and/or certain of their employees may be required to file a Form 700 if so requested by the CDCR or whenever it appears that a conflict of interest may be at issue. Generally, service Contractors (other than consultant Contractors required to file as above) and their employees shall be required to file an FPPC Form 700 if one of the following exists:

(1) The Agreement service has been identified by the CDCR as one where there is a greater likelihood that a conflict of interest may occur;

(2) The Contractor and/or Contractor's employee(s), pursuant to the Agreement, makes or influences a governmental decision; or

(3) The Contractor and/or Contractor's employee(s) serves in a staff capacity with the CDCR and in that capacity participates in making a governmental decision or performs the same or substantially all the same duties for the CDCR that would otherwise be performed by an individual holding a position specified in the CDCR's Conflict of Interest Code.

b. Current State Employees

(1) No officer or employee shall engage in any employment, activity or enterprise from which the officer or employee receives compensation or has a financial interest and which is sponsored or funded by any state agency, unless the employment, activity or enterprise is required as a condition of regular state employment.

(2) No officer or employee shall contract on his or her own behalf as an independent Contractor with any state agency to provide goods or services.

(3) In addition to the above, CDCR officials and employees shall also avoid actions resulting in or creating an appearance of:

(a) Using an official position for private gain;

(b) Giving preferential treatment to any particular person;
(c) Losing independence or impartiality;

(d) Making a decision outside of official channels; and

(e) Affecting adversely the confidence of the public or local officials in the integrity of the program.

(4) Officers and employees of the Department must not solicit, accept or receive, directly or indirectly, any fee, commission, gratuity or gift from any person or business organization doing or seeking to do business with the State.

c. Former State Employees

(1) For the two year (2-year) period from the date he or she left state employment, no former state officer or employee may enter into an Agreement in which he or she engaged in any of the negotiations, transactions, planning, arrangements or any part of the decision-making process relevant to the Agreement while employed in any capacity by any state agency.

(2) For the twelve-month (12-month) period from the date he or she left state employment, no former state officer or employee may enter into an Agreement with any state agency if he or she was employed by that state agency in a policy-making position in the same general subject area as the proposed Agreement within the 12-month period prior to his or her leaving state service.

In addition to the above, the Contractor shall avoid any conflict of interest whatsoever with respect to any financial dealings, employment services, or opportunities offered to inmates or parolees. The Contractor shall not itself employ or offer to employ inmates or parolees either directly or indirectly through an affiliated company, person or business unless specifically authorized in writing by the CDCR. In addition, the Contractor shall not (either directly, or indirectly through an affiliated company, person or business) engage in financial dealings with inmates or parolees, except to the extent that such financial dealings create no actual or potential conflict of interest, are available on the same terms to the general public, and have been approved in advance in writing by the CDCR. For the purposes of this paragraph, "affiliated company, person or business" means any company, business, corporation, nonprofit corporation, partnership, limited partnership, sole proprietorship, or other person or business entity of any kind which has any ownership or control interest whatsoever in the Contractor, or which is wholly or partially owned (more than 5% ownership) or controlled (any percentage) by the Contractor or by the Contractor's owners, officers, principals, directors and/or shareholders, either directly or indirectly. "Affiliated companies, persons or businesses" include, but are not limited to, subsidiary, parent, or sister companies or corporations, and any company, corporation, nonprofit corporation, partnership, limited partnership, sole proprietorship, or other person or business entity of any kind that is wholly or partially owned or controlled, either directly or indirectly, by the Contractor or by the Contractor's owners, officers, principals, directors and/or shareholders.

The Contractor shall have a continuing duty to disclose to the State, in writing, all interests and activities that create an actual or potential conflict of interest in performance of the Agreement.

The Contractor shall have a continuing duty to keep the State timely and fully apprised in writing of any material changes in the Contractor's business structure and/or status. This

includes any changes in business form, such as a change from sole proprietorship or partnership into a corporation or vice-versa; any changes in company ownership; any dissolution of the business; any change of the name of the business; any filing in bankruptcy; any revocation of corporate status by the Secretary of State; and any other material changes in the Contractor's business status or structure that could affect the performance of the Contractor's duties under the Agreement.

If the Contractor violates any provision of the above paragraphs, such action by the Contractor shall render this Agreement void.

Members of boards and commissions are exempt from this section if they do not receive payment other than payment for each meeting of the board or commission, payment for preparatory time and payment for per diem.

6. DISCLOSURE

Neither the State nor any State employee will be liable to the Contractor or its staff for injuries inflicted by inmates or parolees of the State. The State agrees to disclose to the Contractor any statement(s) known to State staff made by any inmate or parolee which indicates violence may result in any specific situation, and the same responsibility will be shared by the Contractor in disclosing such statement(s) to the State.

7. SECURITY CLEARANCE/FINGERPRINTING

The State reserves the right to conduct fingerprinting and/or security clearance through the California Department of Justice, Bureau of Criminal Identification and Information (BCII), prior to award and at any time during the term of the Agreement, in order to permit Contractor and/or Contractor's employees' access to State premises. The State further reserves the right to terminate the Agreement should a threat to security be determined.

8. NOTIFICATION OF PERSONNEL CHANGES

Contractor must notify the State, in writing, of any changes of those personnel allowed access to State premises for the purpose of providing services under this Agreement. In addition, Contractor must recover and return any State-issued identification card provided to Contractor's employee(s) upon their departure or termination.

9. NON ELIGIBLE ALIEN CERTIFICATION

By signing this Agreement Contractor certifies, under penalty of perjury, that Contractor, if a sole proprietor, is not a nonqualified alien as that term is defined by the United States Code (U.S.C.) Title 8, Chapter 14, Section 1621 et seq.

The following provisions apply to services provided on departmental and/or institution grounds:

10. BLOODBORNE PATHOGENS

OTech shall adhere to California Division of Occupational Safety and Health (CAL-OSHA) regulations and guidelines pertaining to bloodborne pathogens.

11. TUBRCULOSIS (TB) TESTING

In the event that the services required under this Agreement will be performed within a CDCR institution/parole office/community based program, prior to the performance of contracted duties, Contractors and their employees who are assigned to work with inmates/parolees on a regular basis shall be required to be examined or tested or medically evaluated for TB in an infectious or contagious stage, and at least once a year thereafter or more often as directed by CDCR. Regular contact is defined as having contact with inmates/parolees in confined quarters more than once a week.

Contractors and their employees shall be required to furnish to CDCR, at no cost to CDCR, a form CDCR 7336, "Employee Tuberculin Skin Test (TST) and Evaluation," prior to assuming their contracted duties and annually thereafter, showing that the Contractor and their employees have been examined and found free of TB in an infectious stage. The form CDCR 7336 will be provided by CDCR upon Contractor's request.

12. PRIMARY LAWS, RULES, AND REGULATIONS REGARDING CONDUCT AND ASSOCIATION WITH STATE PRISON INMATES

Individuals who are not employees of the California Department of Corrections and Rehabilitation (CDCR), but who are working in and around inmates who are incarcerated within California's institutions/facilities or camps, are to be apprised of the laws, rules and regulations governing conduct in associating with prison inmates. The following is a summation of pertinent information when non-departmental employees come in contact with prison inmates.

By signing this contract, the Contractor agrees that if the provisions of the contract require the Contractor to enter an institution/facility or camp, the Contractor and any employee(s) and/or subcontractor(s) shall be made aware of and shall abide by the following laws, rules and regulations governing conduct in associating with prison inmates:

a. Persons who are not employed by CDCR, but are engaged in work at any institution/facility or camp must observe and abide by all laws, rules and regulations governing the conduct of their behavior in associating with prison inmates. Failure to comply with these guidelines may lead to expulsion from CDCR institutions/facilities or camps.

   SOURCE: California Penal Code (PC) Sections 5054 and 5058; California Code of Regulations (CCR), Title 15, Sections 3285 and 3415

b. CDCR does not recognize hostages for bargaining purposes. CDCR has a "NO HOSTAGE" policy and all prison inmates, visitors, and employees shall be made aware of this.
   SOURCE: PC Sections 5054 and 5058; CCR, Title 15, Section 3304

c. All persons entering onto institution/facility or camp grounds consent to search of their person, property or vehicle at any time. Refusal by individuals to submit to a search of their person, property, or vehicle may be cause for denial of access to the premises.

   SOURCE: PC Sections 2601, 5054 and 5058; CCR, Title 15, Sections 3173, 3177, and 3288

d. Persons normally permitted to enter an institution/facility or camp may be barred, for cause, by the CDCR Director, Warden, and/or Regional Parole Administrator.

SOURCE: PC Sections 5054 and 5058; CCR, Title 15, Section 3176 (a)

e. It is illegal for an individual who has been previously convicted of a felony offense to enter into CDCR institutions/facilities or camps without the prior approval of the Warden. It is also illegal for an individual to enter onto these premises for unauthorized purposes or to refuse to leave said premises when requested to do so. Failure to comply with this provision could lead to prosecution.

SOURCE: PC Sections 602, 4570.5 and 4571; CCR, Title 15, Sections 3173 and 3289

f. Encouraging and/or assisting prison inmates to escape are a crime. It is illegal to bring firearms, deadly weapons, explosives, tear gas, drugs or drug paraphernalia on CDCR institutions/facilities or camp premises. It is illegal to give prison inmates firearms, explosives, alcoholic beverages, narcotics, or any drug or drug paraphernalia, including cocaine or marijuana.

SOURCE: PC Sections 2772, 2790, 4533, 4535, 4550, 4573, 4573.5, 4573.6 and 4574

g. It is illegal to give or take letters from inmates without the authorization of the Warden. It is also illegal to give or receive any type of gift and/or gratuities from prison inmates.

SOURCE: PC Sections 2540, 2541 and 4570; CCR, Title 15, Sections 3010, 3399, 3401, 3424 and 3425

h. In an emergency situation the visiting program and other program activities may be suspended.

SOURCE: PC Section 2601; CCR, Title 15, Section 3383

i. For security reasons, visitors must not wear clothing that in any way resembles state issued prison inmate clothing (blue denim shirts, blue denim pants).

SOURCE: CCR, Title 15, Section 3171 (b) (3)

j. Interviews with SPECIFIC INMATES are not permitted. Conspiring with an inmate to circumvent policy and/or regulations constitutes a rule violation that may result in appropriate legal action.

SOURCE: CCR, Title 15, Sections 3261.5, 3315 (3) (W), and 3177

13. CLOTHING RESTRICTIONS

While on institution grounds, Contractor and all its agents, employees, and/or representatives shall be professionally and appropriately dressed in clothing distinct from that worn by inmates at the institution. Specifically, blue denim pants and blue chambray shirts, orange/red/yellow/white/chartreuse jumpsuits and/or yellow rainwear shall not be worn onto institution grounds, as this is inmate attire. The Contractor should contact the

institution regarding clothing restrictions prior to requiring access to the institution to assure the Contractor and their employees are in compliance.

14. TOBACCO-FREE ENVIRONMENT

Pursuant to Penal Code Section 5030.1, the use of tobacco products by any person on the grounds of any institution or facility under the jurisdiction of the Department of Corrections and Rehabilitation is prohibited.

15. SECURITY REGULATIONS

a. Unless otherwise directed by the entrance gate officer and/or Contract Manager, the Contractor, Contractor's employees and subcontractors shall enter the institution through the main entrance gate and park private and nonessential vehicles in the designated visitor's parking lot. Contractor, Contractor's employees and subcontractors shall remove the keys from the ignition when outside the vehicle and all unattended vehicles shall be locked and secured while on institution grounds.

b. Any State- and Contractor-owned equipment used by the Contractor for the provision of contract services, shall be rendered temporarily inoperative by the Contractor when not in use, by locking or other means unless specified otherwise.

c. In order to maintain institution safety and security, periodic fire prevention inspections and site searches may become necessary and Contractor must furnish keys to institutional authorities to access all locked areas on the worksite. The State shall in no way be responsible for Contractor's loss due to fire.

d. Due to security procedures, the Contractor, Contractor's employees and subcontractors may be delayed at the institution vehicle/pedestrian gates and sally ports. Any loss of time checking in and out of the institution gates and sally ports shall be borne by the Contractor.

e. Contractor, Contractor's employees and subcontractors shall observe all security rules and regulations and comply with all instructions given by institutional authorities.

f. Electronic and communicative devices such as pagers, cell phones and cameras/microcameras are not permitted on institution grounds.

g. Contractor, Contractor's employees and subcontractors shall not cause undue interference with the operations of the institution.

h. No picketing is allowed on State property.

16. GATE CLEARANCE

Contractor and Contractor's employee(s) and/or subcontractors(s) must be cleared prior to providing services. The Contractor will be required to complete a Request for Gate Clearance for all persons entering the facility a minimum of ten (10) working days prior to commencement of service. The Request for Gate Clearance must include the person's name, social security number, valid state driver's license number or state identification card number and date of birth. Information shall be submitted to the Contract Liaison or his/her designee. CDCR uses the Request for Gate Clearance to run a California Law Enforcement Telecommunications System (CLETS) check. The check will include a California Department of Motor Vehicles check, Wants and Warrants check, and Criminal History check.

Gate clearance may be denied for the following reasons: Individual's presence in the institution presents a serious threat to security, individual has been charged with a serious crime committed on institution property, inadequate information is available to establish positive identity of prospective individual, and/or individual has deliberately falsified his/her identity.

All persons entering the facilities must have a valid state driver's license or photo identification card on their person.

17. BUSINESS ASSOCIATE AGREEMENT

The awarded Contractor will be required meet provisions of the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 ("HIPAA") and the regulations promulgated thereunder. The Business Associate Agreement can be located at the link below:

http://www.cdcr.ca.gov/Divisions_Boards/Plata/HIPPA_ExhibitG.html.

ATTACHMENT A
PAYEE DATA RECORD (STD 204)

The Payee Data Record (STD 204) can be located at the link below:

http://www.documents.dgs.ca.gov/osp/pdf/std204.pdf

ATTACHMENT B
CONTRACTOR CONFIDENTIALITY STATEMENT

I understand that Consultant can be categorized as a public official for purposes of adherence to Conflict of Interest laws and the filing of a Statement of Economic Interests (Form 700). I certify that I have read and understand Conflict of Interest provisions identified in the online presentation "Ethics Orientation for State Officials" sponsored by the State of California Department of Justice, Office of the Attorney General and the Fair Political Practices Commission located at http://caag.state.ca.us/ethics/index.htm.

I certify that I have no personal or financial interest and no present or past employment or activity which would be incompatible with my participation in any activity related to the planning or procurement processes for the Federated Data Center (RFQ #10-017-ITS). For the duration of my involvement in this Project, I agree not to accept any gift, benefit, gratuity or consideration, or begin a personal or financial interest in a party who is offering, or associated with a business, on the Project.

I certify that I will keep confidential and secure and will not copy, give or otherwise disclose to any other party who has not signed a copy of this confidentiality Agreement, all information concerning the planning, processes, development or procedures of the Project and all bids, proposals, correspondence, etc. which I learn in the course of my duties on the Project. I understand that the information to be kept confidential includes, but is not limited to, specifications, administrative requirements, terms and conditions, any aspect of any supplier's response or potential response to the solicitation, and includes concepts and discussions as well as written or electronic materials. I understand that if I leave this Project before it ends, I must still keep all Project information confidential. I understand that following completion of this project that I must still maintain confidentiality should the Project and/or my organization be subject to follow-on contracting criteria per Public Contract Code §10365.5. I agree to follow any instructions provided related to the Project regarding the confidentiality of Project information.

I fully understand that any unauthorized disclosure I make may be grounds for civil or criminal penalties and/or contract termination. I agree to advise the Deputy Chief Information Officer (DCIO) immediately in the event that I either learn or have reason to believe that any person who has access to Project confidential information has or intends to disclose that information in violation of this Agreement. I also agree that any questions or inquiries from bidders, potential bidders or third parties shall not be answered by me and that I will direct them to CPHCS' DCIO.

Signature: _____ Date: _____

Printed Name: _____ Title: _____

Organization: _____ Telephone Number: _____

Fax Number: _____

Email Address: _____

ATTACHMENT C
NON-DISCLOSURE AGREEMENT

I certify that I will hold in confidence all discussions, bids, proposals, correspondence, memoranda, working papers, procurement of goods and services, or any other information on any media, which has any bearing on or discloses any aspect of the Technical Leader (TL). Based on my involvement with the FDC, where applicable, I certify that I have no personal or financial interest and no present employment or activity, which would be incompatible with my participation in the discussions, review and or participation in the procurement process for the PM and related initiative(s)/procurement(s) thereof.

At all times during and after the process by which the California Prison Health Care Services and/or the California Department of Corrections and Rehabilitation (CDCR) procures Subject Matter Experts, CPHCS' and/or CDCR's employees, CPHCS' prospective bidders, and/or CPHCS and/or CDCR's vendors will keep confidential, and will not disclose to any third party or use, such confidential information, except in the course of their employment by or contractual relationship with the Department, and for the benefit of CDCR. The parties will protect CPHCS' and/or CDCR's confidential information using the same degree of care, but no less than a reasonable degree of care, as such party uses to protect his/her/its own confidential information. The parties will carefully restrict access to CPHCS' confidential information, and they may disclose it only to their employees, contractors, and/or other State agencies that have a need to know it and are bound by obligations of confidentiality.

I certify that I am fully able to provide fair and impartial consideration and contribution to all aspects of this project in which I am directly involved. I fully understand that any such disclosure by an employee of the State of California may be considered as a basis for disciplinary action.

Signature: _____ Date: _____

Printed Name: _____

Title _____

Organization: _____

Telephone Number: _____

Fax Number: _____

Email Address: _____

ATTACHMENT D
STATEMENT OF ECONOMIC INTERESTS (FORM 700)

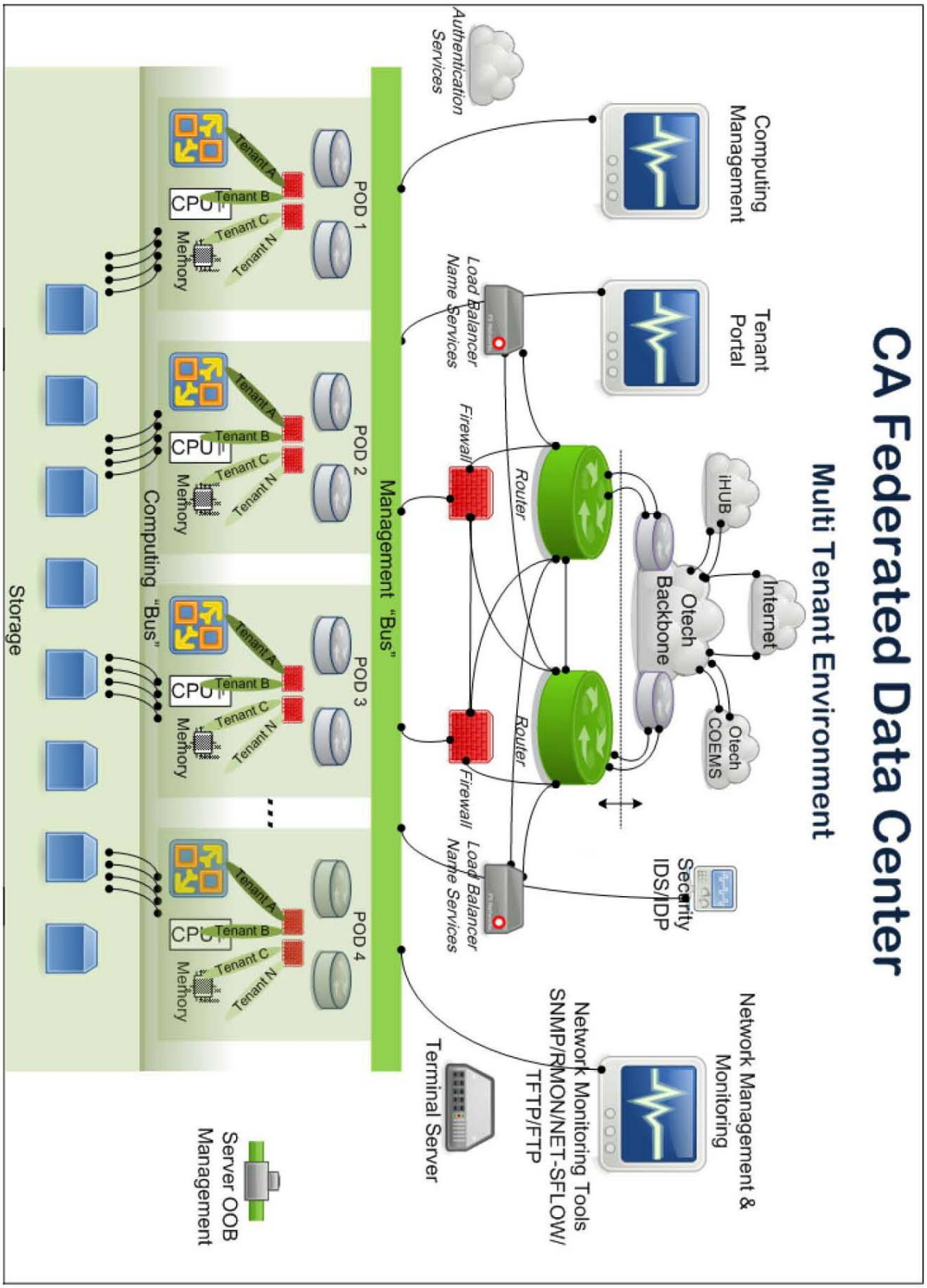
The Statement of Economic Interests (Form 700) can be located at the link below:

http://www.fppc.ca.gov/forms/700-09-10/Form700-09-10.pdf

ATTACHMENT E
GLOSSARY OF ACRONYMS

- FDC – Federated Data Center
- IPS – Intrusion Prevention System
- CSM – Cisco Security Manager
- ACS – Access Control Server
- MPLS – MultiProtocol Label Switching
- VRF – Virtual Routing and Forwarding
- IOS – Internetwork Operating System
- NX-OS – Nexus Operating System
- CCIE – Cisco Certified Internetwork Expert
- Cisco PIX – Private Internet Exchange
- Cisco ASA – Adaptive Security Appliance
- JNCIA-FW – Juniper Networks Certified Internet Associate – Firewall
- HIPAA – Health Insurance Portability and Accountability Act
- CISSP – Certified Information Systems Security Professional
- SSL – Security Sockets Layer
- VPN – Virtual Private Network
- MSSP – Managed Security Service Provider
- SP – Service Provider
- Cisco ASR – Aggregation Services Router
- MM – MultiMode
- SFP – Small form-factor pluggable
- GBIC – Gigabit Interface Converter
- SAN – Storage Area Network
- BPDU – Bridge Protocol Data Units
- DDoS – Distributed Denial of Service
- ISSU – In-Service Software Upgrade
- GOLD – Generic Online Diagnostics
- EEM – Embedded Event
- SNMP – Simple Network Management Protocol
- QoS – Quality of Service
- ILO – Integrated Lights Out
- VLAN – Virtual Local Area Network
- HA – High Availability
- OS – Operating System

ATTACHMENT F



ATTACHMENT G