OMB #0925-XXXX
EXP. XX/XXXX

Attachment 27:
Coordination & Evaluation Center (CEC) Tracker Security Overview

Physical Infrastructure: The Data Center and Informatics Systems (managed by Dr. Dennis) will be housed in the Computer Technology Research Lab on the sixth floor of the Center for Health Sciences at the University of California, Los Angeles. (Link: http://www.ctrl.ucla.edu). CTRL occupies 1175 square feet of office space that houses 12 full-time staff members. In addition to office space CTRL maintains 5 separate environmentally controlled server rooms across two different buildings in the south campus area of UCLA. The primary server room (300 square feet) is adjacent to the CTLR office suite in the Center for the Health Sciences (CHS). It has a dedicated chilled-water cooling system.

Data Centers Connectivity:
All server rooms are connect via 10 Gigabit fiber connections in a fault-tolerant, load-balanced ether channel configuration for TCP/IP communications and dual single-mode fiber channel connections to extend the facility's storage area network. For Internet access, CTRL is connected to the vBNS backbone of Internet2 via dual fiber optic 10 Gigabit lines using different route paths to the UCLA Campus backbone to ensure that the facility's external connectivity will be maintained in the case of a single path failure. All network switches and routers are Cisco. The main redundant routers are 6500 E series units. High-density server racks have Cisco 3750 switches. Smaller server rooms are connected by multi-mode fiber and use Cisco 3750 or 4000 service units.

Data Center Security:
The CTRL datacenters are secured by two levels of physical access to insure HIPAA compliance for data security. The main facility is secured 24/7 with Access-logging OmniLocks door sensor monitoring devices that photograph each entrance event. Only authorized personnel are allowed in server rooms, and guests are permitted in office space only after checking in and only during business hours. The datacenters are additionally secured by OmniLock access. Only authorized staff have access codes for the server room facilities. Individual racks containing HIPAA data are secured by lock and key to prevent cross access.

Relational Database Resources:
CTRL manages a licensed Oracle 11g database instances that is running in archive log mode where all transactions committed on a primary database are copied over to a fail-over instance running on separate hardware in another server room in a different building. All primary/fail-over database pairs and application servers are located in different buildings. Data from all production servers are backed up to a larger (40 terabyte) storage area network devices. All database servers reside on isolated private 10 IP spaces with host-based firewalls and router-level access control lists to limit connectivity to trusted application servers only.

Server Hardware:
CTRL manages over 85 separate rack mounted multi-core, multi-CPU servers. These systems are mostly 1U, 2U and 4U systems with dual power supplies and dual network interfaces. Most units have two dual or quad-core 2.5ghz or faster Xeon 5500Processors. The majority of these systems run Redhat Linux Advance Server 6.X. CTRL maintains several older dual-CPU 32-bit systems for older legacy applications.

Data Transmission:
Data are transmitted from the study sites on real-time basis over the Internet via a secure sockets layer (SSL) connection using SHA-256 bit with RSA Encryption over TLS 1.2.

Assuring Quality of Data Management System

Software systems developed as part of this project follow a standard set of development conventions and procedures. All coding is conducted on a development system and stable, internally tested code is committed to a subversion (SVN) repository. From the SVN repository, code is checked out to separate physical hardware designated as that staging server. The staging server is available to study staff for training and functional verification whereas the development systems are only accessible by programmers from within the CTRL firewall. When code is approved, it is checked out to the production servers which reside on robust physical hardware with redundant internal power supplies, RAID hard drives, ECC RAM, and external uninterruptible power supplies (UPS). In addition, system heartbeats are monitored using the open source administration software, *Big Brother*. The applications themselves are polled from an uptime monitor that resides on a separate computer (located on the east coast). If the uptime monitor fails to receive a response from the application server, alerts are sent to computer support staff via SMS text messages. The CTRL application servers are scanned quarterly using Accunetix web vulnerability scanner, and all systems are scanned quarterly for system-level vulnerabilities using the Nessus vulnerability scanner.