Details of Wireless Network

A. Deployment of Access-Points

If chosen for the project, CC will work with Court IT to finalize placement of access-points to achieve desired wireless coverage while keeping the environment intact. CC's site survey has allowed it to identify the number and location of each AP in both Sacramento and Fresno courthouses.

CC will utilize Cisco Aironet 1130 access-points with integrated antennas in all courtrooms. Although it is not expected, a Cisco Aironet 1230 can be used where there is a need to direct the wireless signal in a particular direction, such as down a long hallway. Both the 1130 and 1230 have a very attractive design, and will not detract from courthouse aesthetics. All APs will be mounted professionally and in accordance with rules, design principles and the aesthetics of the courthouse.

Cisco Aironet 1130

Cisco Aironet 1200

B. Configuration of Access-Points

CC utilizes the Cisco 1130 and 1230 series access-points, which have upgraded processors to handle the advanced AES encryption utilized in WPA2. WPA2 is the second generation of WPA security, providing enterprise Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard. The access-points are also backward compatible with WPA, which is supported by virtually all major Wi-Fi cards manufactured since 2001. The adoption of WPA2 should not cause concern for users who are only able to use WPA to connect to the Wi-Fi network. WPA is still considered secure by the managing bodies of the Wi-Fi standard.

CC uses multiple 802.1q VLANs to separate user classes or groups. These VLANs are tied to specific SSIDs within the access-point and are held to these associations by rule, allowing no exceptions even through configuration. All the 802.1q VLANs will be trunked through the switched infrastructure to independent virtual gateways on the LAN router, or even a different gateway router (i.e., if a particular user group/class required a dedicated Internet connection). The use of 802.1q VLANs prevents even the dedicated traffic sniffer from gaining access to any traffic outside of the SSID that they have been granted access to. Although all wireless traffic can be encrypted to protect against intercepting wireless transmissions, VLANs add extra protection to protect a user from another user across the wired backbone. Users engaged in VPN sessions with appropriate firewalling already handle this precaution, but VLANs create an additional barrier.

VLANs include open SSIDs for which authentication is conducted via a web page (managed by the Cisco Building Broadband Services device located at the CC datacenter) and closed VLANs for which EAP authentication using rotating WPA2 keys are used to authenticate users before connection is made. The BBSM authenticates users with accounts to one of two RADIUS servers located within the datacenter, ensuring that authentication traffic never leaves the private network domain, or via secure web connection to a credit card gateway. EAP authentication also relies on the user and AP communicating with the RADIUS servers located in the secure CC data center.

CC uses a unique SNMP community string to allow monitoring of network devices. CC will provide this string, at Court's request, to allow for Court IT to monitor these devices as well. In addition to this, access-lists placed on each device specifically list the network addresses that are allowed to access the devices. To further manage access, accounts will be created that allow any of 15 levels of access (as defined by the device), providing extreme levels of granularity with access control and administrative rights. Again, at the Court's request, CC can provide accounts on these devices to allow access for Court IT personnel, based on agreed upon levels of administrative control.

C. Network Compatibility

CC has substantial experience creating networks that fit into the court environment. The network will be designed and implemented to preserve the aesthetics of the courthouse while at the same time as ensuring the highest level of reliability and security available. CC will utilize Cisco wireless access-points that are very attractive in appearance, and CC will place access-points in the most aesthetically pleasing locations possible. CC will respect the property of the Courthouse and will take all reasonable precautions not to impair the Courthouse during any installation or upgrade.

Equipment will be placed in locations that do not obstruct other transmitting devices, and wireless transmissions will be configured to co-exist with other nearby Wi-Fi networks. A high-capacity deployment involves minimizing channel interference between access-points and an extensive site survey will be conducted to determine optimal placement of access-points and to assess coverage. However, with dual-band access-points, for most installations, this effort need only be done once under the channel constraints of the wireless network. The dual-band radios in the access-points support up to 19 access-points being set to unique channels before channel interference becomes an issue. In most cases, the wireless radios can be deployed at maximum transmit power without causing co-channel interference. If the deployment density is such that co-channel interference becomes relevant, then the transmit power of the access-points can be reduced to minimize interference. A careful process of pre-qualifying the access-point locations has not resulted in CC needing to do so at any of its existing sites. Furthermore, with the congestion algorithm that runs inherently within the 1130 and 1230 Access-Points, an addition of RF signals to the deployed environment rarely cause interference issues. The access-points are designed and configured to self-heal and reconverge after adaptation to the new RF sources. Wi-Fi operates at very low power levels, unlike cellular and broadcast radio -- therefore, there is no health concerns related to the radio transmissions. Access-point placement, power settings, and antenna selection will be used to limit wireless coverage to appropriate locations.

IV. Security

A. Firewall

CC maintains a PIX firewall to protect users from others on the Internet. The PIX is configured to allow only traffic generated from inside the network to return -- no communication can be initiated from the outside. Users are protected from any malicious attacks or probing initiated from outside the network.

B. Wireless security

CC provides optional EAP-based encryption and 802.11i to provide authentication over the wireless LAN. 802.11i is an extension to the Wi-Fi standard using WPA/WPA2 keys, and provides security in place of less-secure methods such as local MAC Authentication and static WEP keys. The 802.11i standard uses the Extensible Authentication Protocol (EAP) and various authentication schemes to authenticate users to a RADIUS server and grant access to resources of the network. In addition to providing authentication, EAP manages the encryption of all wireless traffic. Developed by industry leaders Cisco, RSA and Microsoft, EAP has been called a quantum leap in network security and is rapidly being adopted as the de facto standard for wireless networking. To allow flexibility in client configurations, CC uses EAP for authentication in two major flavors: LEAP and PEAP. LEAP is provided for customers who use the Cisco Aironet PC card and PEAP is provided for customers who choose to use the built-in wireless functionality that is incorporated into Windows XP laptops. Both LEAP and PEAP are recognized as the gold standards for authentication of wireless clients and both provide security that is nearly transparent for the customer. CC can also support EAP-TTLS and shared WPA2 keys if desired for court users or individual private user VLANs.

C. Virtual Local Area Networks (VLANs)

Users can be segregated onto separate VLANs to provide added security. Users on a VLAN are not able to observe or communicate with users on another VLAN. One

VLAN will be shared by users who access the network through web authentication, which offers support for all types of Wi-Fi cards (called “cc”, this is CC’s basic VLAN). Other VLANs are reserved for trial teams, subscribers, and court reporters utilizing EAP-based authentication, which offers a higher level of security for users but requires more configuration and proprietary vendor or Windows XP extensions to standard Wi-Fi features. User can also have an individual VLAN set up to authenticate with EAP-TTLS, WPA2 shared keys, or other methods if desired. Also, although users within a secure VLAN can be permitted to share local access to others within the VLAN if desired, the open VLAN is restricted so that attempts to access the PCs of other users are not permitted.

D. User authentication

Access to CC’s network is controlled with users choosing to connect through either a Cisco BBSM SSL-encrypted web log-in page or EAP-based authentication. Users cannot get onto the Internet without logging in using one of these methods. This both prevents Internet abuses and allows for tracking/auditing of users. If alerted to an issue, CC can take measures to identify individual users, tying them to specific access-points and patterns of usage. CC recommends the Court to have authentication infrastructure reside within the CC datacenter for scalability, efficiency, security, and support purposes.

V. Testing and System Acceptance

CC has developed an intensive testing and system acceptance plan for all of its network components post-implementation. The following tests are performed by CC’s network team to accurately assess the health and operation of the network.

- Throughput Test
  - CC will conduct onsite testing by using over 6 of the most common industry sites to determine throughput speeds of the network.
  - CC certifies throughput at 80%
- Wireless Coverage
  - CC determines wireless coverage by testing onsite and utilizing Cisco Aironet Client Utility to determine signal strength quality. In addition, CC will also test using other consumer grade Wifi cards. Results must indicate good to excellent signal strength to pass coverage test.
- Network Monitoring/Alerts
  - CC will remotely monitor and check status of all network equipment to ensure proper configurations and latest firmware is installed.
- Security Checks
  - CC will conduct exercises designed to ensure security/encryption measures are intact.

All testing results are recorded and can be presented to the court.

VII. Network Monitoring and Maintenance[1]

A. Monitor Network for Quality and Security - Located in operations centers on each coasts, CC's monitoring software has visibility into all areas of CC's deployed network and can quickly spot the cause of any problems that may arise. The network is monitored 24X7, and automated alerts are sent to CC personnel when a

[1] Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this offer

problem is detected so that action can be taken immediately to resolve any anomalies. CC also keeps sign-in logs and can assist in tracking down a user that is suspect of foul play. CC does not actively monitor or filter outbound content, however, and considers the content of transmissions to be private.

B. Network Maintenance and Recovery – Routine maintenance and network upgrades are performed monthly through remote support features defined on CC's network. These upgrades and maintenance are based on plans outlined by CC's Technology Group to maintain the latest firmware and software upgrades to all of CC's network equipment. All remote maintenance and upgrades are performed during non-business hours.

In the event of an issue with the network, CC personnel will begin working immediately (usually within 10 minutes and no later than 30 minutes) to resolve the problem. If there is a partial or total network equipment failure, and CC cannot fix remotely, a CC staff member will be sent on site to resolve the issue within a 4 hour period from the time the problem or network issue is reported and logged. CC staff person will notify Court personnel of the issues and make arrangements to come to Court in a response time of 4 hours or less during normal business hours of the Court (8:00AM-5:00PM, Monday through Friday). It is theoretically possible (though highly unlikely) to have ISP or manufacturer system failures that take longer than a single day to resolve. If that is the case, CC will apply persistent resources until the issue is resolved in as timely a fashion as possible.

C. Network Security, Broadcasting/Content Safeguards: CC will work with Court to devise exactly the framework that Court would like to have in place to prevent the open broadcast of proceedings as well as viewing of inappropriate content such as pornographic websites. We have a number of tools available, but no single tool covers everything. In addition, providing security to the user of their transmissions will in part need to be balanced against this prohibition -- a tradeoff we will leave up to Court to determine. CC is prepared to do the following to achieve the desired result of no broadcasts over the network:

1. Limited network to authorized users—Password Security will prevent an unauthorized user from using the network for any purposes, including broadcasting.
2. Clear communications to users - To avoid any unintentional misuse, CC will clearly communicate to all users the policy on "no broadcasting", as well as other user terms which include viewing of inappropriate content. The online user sign-in page will also contain this message.
3. Blocking ports/applications - CC uses Cisco's PIX firewall appliance and employs its associated Intrusion Detection (IDS) features. These features allow us to provide a powerful, highly flexible framework for defining flow- or class-based policies, enabling CC to identify a network flow or class based on different conditions, and then apply a set of customizable services to each flow or class. CC will proactively block streaming services from all VLANs. The PIX also provides inspection services to detect and optionally block instant messaging, peer-to-peer file sharing, and other "troublesome" applications, if the Court

deems them undesirable. In addition to the above policy-based security measures, CC is able to block specific traffic to and from the site based on source of traffic (user or location), destination of traffic (a known offending end-point located on Internet) or the type of traffic (a know application, or an unknown application) when that threat is brought to our attention.

4. Additional monitoring - While CC can attempt to block all attempts at streaming and/or accessing pornographic sites, there are ways for users to mask streaming as other applications or within secure tunnels. As an added security layer, the currently deployed version of the PIX firmware can identify users attempting to surreptitiously tunnel this traffic through Web application ports. Users who are identified as making such attempts can be checked out and removed from the network the same day.
5. Responding to violation - If CC becomes aware of any violation for any reason, the user will be immediately removed from the network and Court notified.
6. CC realizes that threats and technology evolve over time and to address this, CC maintains a strict program of testing and deploying updates to firmware on all devices to ensure that new threats are mitigated as they arise. Firmware on all deployed equipment is the most recent, fully tested version available. CC will continue to work with Court IT to make and revise user policies as needed to ensure the best possible security for the court and users.

D. Removing Users from Service

CC will remove any offending private user from the network immediately upon notice by the court, or if offensive behavior is observed by CC. Use is considered a privilege, and CC requires users to agree to terms of service specifying that they shall comply with all rules, regulations and security and operating procedures of CC and Court. Agreement is secured through click-through, e-mail, or signed document. For example, users agree that they will not use the services for chain letters, junk mail, "spamming", solicitations (commercial or non-commercial) or any use of distribution lists to any person who has not given specific permission to be included in such a process. They further agree not to use CC's services to send any message or material that is unlawful, harassing, libelous, abusive, threatening, harmful, vulgar, obscene or otherwise objectionable in any manner or nature or that encourages conduct that could constitute a criminal offense, give rise to civil liability or otherwise violate any applicable local, state, national or international law or regulation. CC will remove any user from the network who is believed to violate the terms in any way.

In extreme cases, CC can turn off wireless transmitters that serve designated areas and make them "dark" if foul play was suspected or proactive protection desired by the Court for a particular region of the courthouse. CC can do this easily in a matter of minutes from a remote location (i.e., no physical intervention is required). While CC would hope that such precautions would rarely be required, it is an option that can be used to respond to localized issues.

E. Virus, Spam, and Network Intrusion – CC will keep firewall and router logs that it uses to monitor usage and network anomalies. Activity coming from internal equipment is tracked and traced to user accounts. Activity outside the firewall is analyzed to determine if steps need to be taken to further lock down the network to block specific addresses and/or protocols. CC does not look at the content of traffic, however, unless directed to do so by law enforcement.

In addition to CC's comprehensive network-wide monitoring system, CC will also be able to check for a variety of network maladies. This will be done by monitoring traffic inside, outside, and at the firewall, and using that information to take the necessary measures to ensure network integrity is preserved to the highest degree possible. CC employs a blended approach to security by utilizing Cisco PIX firewalls and routers employing Cisco's Intrusion Detection System, Access Control Lists (ACLs), flood guards, and SNMP traps. Additionally ACL logs on routers and PIX firewalls are monitored for spikes in the number of hits that ACL entries receive, and regular bandwidth trend analysis is performed and compared against 'normal' conditions to determine irregularities. Any significant deviations are treated as an attack on the network and its users by the CC network support staff, and responded to accordingly. DoS attacks, internet worms, abnormal traffic behavior, and congestion are issues which are fully addressed by this approach. CC's deployment of this monitoring system provides insurance that the network, and ultimately its users, are protected from network anomalies.

CC will provide reports to the Court's Technical Representative detailing security violations noted on the network. All reports will be accessible and viewable using Microsoft Office Bundled Software.

E. Traffic Report[2]

CC can provide traffic reports to Court. CC is able to run detailed reports from its RADIUS server for subscriber logins, as well as produce credit card and passcode login reports from the BBSM. CC will present weekly reports to the Technical representative of the Court as requested in this solicitation.

The weekly reports will detail total weekly usage by number of connections, access, and any other activity detail the Court representative wishes to review. CC can create additional network reports for Court IT including but not limited to the below:

- **Uptime Report** containing device up and down state changes AND service up and down state changes.
- **Statistics Report** containing return trip times and percentage of missed polls based on the accumulated polling statistics for each device.
- **Performance Graphs** showing devices by best performance or worst performance based on aggregated polling statistics.

CC will actively monitor for virus activity, spamming or malicious use of the Internet access, network intrusion, uptime of network equipment, and performance of Internet access. In addition, CC will investigate reports of any user issue by monitoring affected service.

F. Service Level Agreement

Proposed Service Level Agreement that includes but is not limited to:

--**Service Availability expressed as Percentage of Up-Time**

Up-time is in the 99.8th percentile. We maintain redundant equipment at each stage of the connection and install over-specified, internally redundant equipment at the facility.

--**End to End latency in milliseconds**

Round-trip time for coast to coast traffic is <100ms. Expressed as end to end, latency is a minimum of 50ms.

--**Minimum Packet Loss**

We do not tolerate any packet loss on the network. If faulty equipment or over-subscription of bandwidth is detected by our monitoring equipment, we will dispatch in accordance with below, "Minimum Time to Repair Outages" and repair, replace or upgrade facilities to support increased traffic.

--**Minimum Time to Repair outages**

We are notified of degradation in service or outages within one minute of a fault. We are fully staffed with helpdesk staff during east and west coast business hours and after hour alerts are sent via email and/or pager to on-call personnel. Problems associated with equipment failure are handled as soon as access to the facility is granted by the court. Problems dealing with capacity (additional traffic causing bandwidth bottlenecks) are handled proactively with capacity management strategies and upgrades to support addition traffic are handled in off-hours with remote administration of equipment or back-end systems.

--Plan for Monitoring User Satisfaction

User satisfaction is the most essential business principle for CC. As a result, CC employs various measures to monitor and ensure satisfaction by all of its users.

1) Initial Set Up: CC will make sure all users are properly equipped and trained to utilize service. CC will provide both onsite and remote support/set up options for users, if necessary. CC will also work with law firm IT departments if special configurations are needed for laptops while in court.
2) Ongoing check in: CC personnel will check in to make sure users are satisfied with service and to address any issues that may exist. If remote

monitoring software detects that certain users are not online, CC will check in with customers to make sure users are not encountering problems.