City of Corona Police Department Network Overview

The City maintains a Public Safety Network ("PSN") which aides' in emergency services to be provided to its citizens using secure communication.

Network Environment: The Police Department network is segmented into three internal vlans. Our dispatch center operates on one of the three vlans and communicates with the CAD/RMS servers which reside on the City server vlan. All internal communication to the servers through the CAD/RMS program is encrypted using 128-bit Triple DES.

The City network infrastructure is Cisco. The switching hardware being used at the Police Department consists of a Catalyst 6509 switch; 4510 switch and multiple 3560G switches.

Our CAD system is virtualized and currently operating on Vmware 5.5 enterprise plus.

Network Access and Security:

All external access to and from the CAD system is secured using Netmotion, version 11 FIPS-140-2 Suite B AES 256-bit encryption and 2FA, two form factor authentication.

The PSN interconnects with the Riverside Sheriff's Office and the West Covina Service Group. The T1 circuit to West Covina is used for CLETS requests and for remote support provided by West Covina. The other T1 provides connectivity to Riverside County assets if needed. Typical uses are access to County agency assets for joint task teams operating from the Corona Police Department.

Users are authenticated on stationary desktop computers using Windows Active Directory. The user logs-in using the standard Windows login and upon successful authentication, the user arrives at the Windows desktop. In addition to logging into the network the user must log-in to the CAD application using different credentials and passwords. The passwords meet DOJ complexity requirements, frequency of changing passwords and the number of password changes made before reusing a password. All devices using the Radcom CAD application have a T-DEF (Terminal definition file) that is associated with the device IP address or machine name; furthermore, all devices that access the DOJ network have a pneumonic added to the T-DEF. The type of pneumonic associated determines the level of DOJ access the user has.

MDC users are authenticated using 2FA (two form factor authentication). The process begins with the user logging into the CF-31 Toughbook using their Windows credentials; then they present their employee badge to a RFID card reader followed by their CAD application credentials.

The MDC's use Windows 7 OS firewall and the traffic is encrypted by NetMotion using 256 AES encryption. Generated traffic is sent across the commercial wireless carriers (Verizon, AT&T and T-Mobile) to the PSN through our internet edge ASA 5525-X firewall to our Netmotion server. Access to all CAD resources is attained from the user connection to the Netmotion server. No CLETS data is stored on the MDC hard drives.

There is a tertiary authentication that occurs between the MDC, AD, Microsoft Certificate Authority ("CA"), and Microsoft RADIUS. This

authentication is called machine authentication. After the computer joins the Domain, the computer object in Active Directory is moved to the appropriate Organizational Unit ("OU"). The object then authenticates against RADIUS and the CA issues a valid certificate. This entrusts that the computer that has VPN access through NetMotion identifies as an authorized computer to then access network resources.

Time Synchronization: The City synchronizes system time through our Cisco 6509 switch, which gets time from an internet source and delivers it to the network using the NTP protocol. Windows utilizes a time service called 'Windows Time', which is automatically installed in the service list. The program executable is 'w32time.exe'. The service is installed and enabled by default during installation.

Windows Domain Networking is deployed, and only the Primary Domain Controller (PDC) synchronizes with the time reference. All other servers and workstations in the domain sync to the PDC using Windows proprietary protocol. The default installation procedure automatically configures workstations and servers to sync to the controlling PDC.

All servers, workstations, MDCs and Cisco network equipment are setup to sync with the City's PDC. Mobile devices like phones and tablets use the cellular provider network to sync their clocks.

Software Updates: Information Technology utilizes Microsoft's System Center Configuration Manager to deploy all software to each desktop computers once a month. The mobile computers are updated two times a year manually. When a threat is discovered between patch cycles staff deploys the patch using the Microsoft SCCM system or manually applying the patches as needed.

Desktop Hardware and Operating System Software: The City standardizes with Dell Optiplex desktops computers with Windows 7 Pro-64-bit. We are in the process of upgrading to Windows 10. The PC should have a minimum Intel Core i5 3.2GHz processor, 4 GB of RAM, and a 500 GB HDD. Each computer is equipped with Dell monitors varying from 17 inch to 24 inch models.

The City replaces desktop computers on a 6-year cycle and the monitors as needed.

Server Hardware and Operating System Software: The City has a Cisco UCS chassis with six B200 M3 blades in which VMWare 5.5 enterprise plus operates. The CAD servers run as virtual guests in the cluster using the Microsoft 2008 R2 -64 bit operating system. Our Cluster consists of Cent-OS, Red Hat Suse and Gentoo based Linux operating systems as well as, Microsoft 2008, 2008 R2, 2012 R2 operating systems.

Mobile Hardware and Operating System Software: The City deploys the same hardware for both police vehicles and fire apparatus. The standard hardware is Panasonic CF-31 Toughbooks, build CF-

3112149CM. The MDC's are configured to run Windows 7 Professional 64-bit.

The City replaces mobile computers on a 3-year cycle. For the purpose of the CAD, RMS and Mobile Replacement Project, the City requires the Vendor to ensure their mobile applications are capable of being installed and perform as designed without any degradation.

Mobile Smartphone's: The City uses Android and Apple phones.

Mobile Device Management ("MDM"): The City does not have a MDM solution. We use Microsoft Exchange to remotely wipe City email from user devices if necessary.

Back-Up and Recovery Software and Process: The City currently backs up the CAD and RMS system using Veeam software. The City backups the data from disk to disk. The backup storage SAN is remotely located in our Police Department with the datacenter being located at City Hall.

City Telephone System: The City has deployed a Voice over Internet Protocol ("VoIP") enterprise telephone system from Cisco. The phone system is virtual and consists of two call managers, a unity – voice mail server and a UCCX call center server. The Cisco phone system is an on premise system and utilizes PRI trunks. The system is SIP compatible and provides legacy analog functionality. The City phone system supports 750+ phones for the City, to include standard features such as voicemail, call forwarding, conference calling and other calling features.

Integration with Riverside Sherriff's Office Data Warehouse: The City of Corona shares specific data elements with Riverside County Sheriff's Office. We have a Database Server (RSODB) running SQL Server 2008 R2 on Windows Server 2008 R2. This database subscribes to specific tables which are published from the WCSG CAD database using SQL Server Replication. The Sherriff's Office has an automated nightly process that imports the changes to the data on RSODB into their Oracle based Data Warehouse. Since the data in the RSODB is near real time, there are various applications internal to the Corona Police Department which use this as the source of their data, as opposed to connecting to the CAD (OLTP) database directly.

Integration with Laserfiche: The Police Records Division uses Laserfiche to archive and track case records. The system utilizes quick forms to pull CAD information from the RSODB SQL server to populate case metadata. This data is used to catalog the data archived in Laserfiche.

Integration with FireRMS (Zoll): Zoll provides a listener application installed on a virtual workstation (FDAPPWS1). As fire related calls are input into the WCSG CAD system, there is a process that sends the call information to the listener. The listener then automatically writes the call information to the FireRMS system. The information recorded includes the units dispatched, the location of the incident, and the relevant times (dispatch times, on scene times, finish times).