Section 17930 CCTV Systems

PART 1 – GENERAL

1.01 Scope. In some locations in or near campus buildings there is a need to monitor activities by use of video camera systems. This need may be for a wide variety of activities. Examples include enhancement of security of persons and/or physical assets, monitoring of research areas (e.g. an animal breeding facility), promotion of a campus service or project, use as an instructional tool, etc. Systems used for these purposes are generally known as Closed Circuit Television (CCTV) systems. These differ from higher-end video conferencing or instructional audio-visual systems in that they tend to provide lower quality video signals suitable for monitoring activities as opposed to communication/teaching functions. This section describes recommendations for how these systems should be connected to the campus telecommunications infrastructure only. It does not address the cameras themselves or any related support equipment.

1.02 Traditional (RF) Approach. There are a multitude of configuration options available on the market for CCTV systems of varying costs and sophistication. Most fall within one of two basic approaches. The more traditional approach is to install systems that are RF signal-based and consist of a set of cameras wired to a video controller with coaxial cables. Although used more and more infrequently, this type of system still remains viable, especially for applications requiring very high signal quality and image storage. Generally, these systems will have their own isolated infrastructure and will not co-locate with or intermingle with the telecommunications infrastructure in a building. The central controller hardware may (if capable) be connected to the campus network merely by plugging into a standard telecommunications outlet data jack. Signals can then be transported to other campus locations via the campus data network.

1.03 IP-Based Approach. The other approach for CCTV systems (and the one that utilizes emerging CCTV technologies) is to connect individual cameras to the IP-based campus data network and use that network to transport signals. Typically, a server is connected to the data network that operates the CCTV system. That server may be placed in the same building as the cameras or may be located elsewhere on campus. The cameras and server appear to the campus network as just additional typical hosts (PCs) that are connected to it. While there are some restrictions regarding the connectivity for this type of system, it generally can meet most CCTV needs without a lot of extra infrastructure installation required.

1.04 Interface with Telecommunications Infrastructure. Regardless of the CCTV system approach selected for a particular application, the interface with the building telecommunications infrastructure is the same. The demarcation point is the telecom outlet faceplate. In addition, no system electronics or components may be installed in the BDF/IDF rooms. System wiring for CCTV systems may not be installed in telecommunication wireways and conduits. NC State Comtech is responsible to provide and support the data network connection at the data jack on the telecom outlet faceplate. Support of the CCTV system itself is the responsibility of the purchaser of the system.

1.05 Coordination with Access Control Systems. In some campus facilities there may be a desire to have CCTV cameras coordinate with the access control system in the building. An example would be a scenario where opening a door would automatically trigger operation of a nearby camera. This coordination would be handled by software in the card access system and would use standard IP cameras connected as described above.

1.06 Grandfathered Systems. CCTV systems that were installed prior to January 1, 2005, but do not adhere to this standard may remain in service. However, they must comply with sections of the UWS 2.0 standard that govern physical layer infrastructure, and they must not negatively impact the campus wired or wireless data network as described in this section.
PART 2 – DESIGN GUIDELINES

2.01 System Options.

- Applicable Guidelines. The guidelines below pertain only to IP-based CCTV systems. Traditional RF-based CCTV systems should be designed in compliance with industry standards and manufacturer requirements. The designer should consult appropriate NCSU standards for design of CCTV systems that will be integrated into the access control system.

2.02 Camera Locations.

- Indoor locations. Cameras to be installed inside a building should be provisioned as follows. A University Wiring Standard (UWS) outlet should be installed adjacent to each IP camera and where the system server is to be located. The IP camera then is to be plugged directly into one of the data jacks. Another option is for analog cameras to be installed with small camera servers located at the camera site. The server is then plugged into one of the data jacks.

- Outdoor locations. Cameras may need to be mounted onto the outside of buildings or in outdoor areas. In these cases, the installer of the camera system should install cabling from the camera to a dry location inside the building. A UWS outlet should be installed at that location and used for data network access.

- Blue light telephone standions. A separate underground conduit is installed from each blue light unit to the nearest building for future CCTV cabling. See Section 17690 for more information.

2.03 Connectivity Requirements.

- Copper vs. fiber cabling. All IP cameras are to be connected to the campus network via Category 5 or 6 UTP cabling installed as part of UWS outlets. Fiber optic cable will not be used to connect cameras.

- Wireless cameras. Wireless cameras should not be installed within or on the exterior of campus buildings. Wired cameras should be used instead per above. Wireless IP cameras (utilizing 802.11a, b, or g standard connectivity) may be used in other areas ONLY after review and approval from Comtech. If during this review, Comtech believes that installation of wireless cameras could negatively impact the wireless LAN coverage in that part of campus, then their installation will not be allowed.

- Power. Electrical power for cameras may be accomplished by installation of an AC power receptacle at the site of the camera or by requesting that ComTech activate a power over Ethernet port.

2.04 Bandwidth Limitations.

- Network traffic. CCTV cameras systems vary widely in the amount of data network traffic load they create on the campus network. Comtech reserves the right to restrict their use if it is deemed that network bandwidth availability is negatively affected for other users and applications.

- Video standards. Comtech does not wish to recommend a particular CCTV camera system nor restrict what systems may be installed. However, based on network traffic concerns per above, there are some basic requirements. IP cameras connected to the NCSU campus data network may utilize MJPEG and MPEG-4 standard technology. Cameras using MPEG-1 and MPEG-2 may not be connected and should not be specified for CCTV applications at NC State.

- IP Multicast Systems. IP Multicast is a protocol for transmitting information from one source to many destinations in a local or wide-area network. Some CCTV systems use this protocol for
distributing video signals. Due to the potential impact on the normal day-to-day operations of the NCSU campus data network, Comtech reserves the right to restrict the use of any IP-based CCTV system that requires IP Multicast functionality or configuring a CCTV system to use IP Multicast. Such systems may be used only with the approval of Comtech, and may be disallowed if they are projected to interfere with the campus network.

- **Network Capability Requirements.** Generally, IP cameras may only be installed in locations where the UWS outlet installed is wired back to a BDF/IDF equipped with the following capabilities: available 100BaseT ports for all cameras (and system servers) and a Gigabit Ethernet uplink to the campus backbone. For locations with less than the above capabilities, cameras may only be installed after evaluation and approval from Comtech. The designer should contact Comtech to determine the network capability of particular sites. The goal of Comtech is to support the highest quality CCTV connectivity possible while still ensuring that data connectivity for all users also remains at the highest level.

2.05 Resources.

- **Consulting.** Comtech will be glad to advise campus departments as well as outside consultants on available connectivity options for video systems. While the above guideline should cover the vast majority of CCTV connectivity needs, there may be particular applications requiring more careful planning and thought. Comtech is willing to assist the campus community as needed to determine solutions to meet these needs.

End of Section