DEPARTMENT OF INFORMATION TECHNOLOGY
INFRASTRUCTURE GUIDELINES
Table of Contents

1.0 INTRODUCTION
   1.1 Overview
   1.2 General
   1.3 Codes and Standards

2.0 TELECOMMUNICATION
   2.1 Overview
   2.2 Conduits and Jack Requirements
   2.3 Telecommunication Equipment Room
   2.4 Cabling
   2.5 Standard Numbering Plan for Cabling Systems
   2.6 Grounding
   2.7 Electrical
   2.8 HVAC
   2.9 Industry Standards and References

3.0 ENERGY MANAGEMENT AND CONTROL SYSTEMS (EMCS)
   3.1 Overview
   3.2 Industry Standards and References

4.0 LIGHTING CONTROL SYSTEMS (LCS)
   4.1 Overview
   4.2 Industry Standards and References

5.0 BUILDING ACCESS CONTROL SYSTEMS (BACS)
   5.1 Overview
   5.2 Industry Standards and References
   5.3 System Components
6.0 BUILDING SECURITY SURVEILLANCE CAMERA SYSTEM (BSSCS)
   6.1 Overview
   6.2 Industry Standards and References

7.0 GENERAL GUIDELINES FOR EMCS, LCS, BACS AND BSSCS SYSTEMS
   7.1 Overview
   7.2 Remote Access to Systems
   7.3 County Standards & References
   7.4 Procedures – Process Outline
   7.5 DIT Forms Required for Installation of Systems

8.0 RADIO SYSTEMS
   8.1 Overview
   8.2 Curb, Vault and Conduit
   8.3 Industry Standards and References
1.0 Introduction

1.1 Overview: Communications technologies are a critical element in the design of all new construction and renovation building projects. Whether it is voice, data, building automation systems (energy management, lighting), door access, security, camera, or other communications technologies. It is important that a team of experienced professionals be involved in the design of these complex systems from the onset.

1.2 General: For all construction projects for Fairfax County, construction budgets are required to fund all internal and external telecommunication assets. This includes all wiring, telecom rooms, connectivity products, electronics, etc. Department of Information Technology (DIT) shall have the responsibility of recommending the computer hardware and software required to operate these systems. This process will ensure that all computer hardware and software are in compliance with DIT standards and ensures the compatibility required for the County’s IT infrastructure.

1.3 Codes and Standards: Fairfax County communications systems shall follow all applicable codes and standards set forth in the following: National Electrical Code (NEC); National Fire Safety Council (NFSC); National Fire Protection Association (NFPA); American National Standards Institute (ANSI); Telecommunication Industries Association (TIA); Electronic Industries Alliance (EIA); Telecommunication Building Wiring Standards; Federal Communications Commission (FCC); Institute of Electrical and Electronic Engineers (IEEE); and Building Industry Consulting Service International (BICIS) - Telecommunication Distribution Methods Manual. These standards are to be used as reference when designing telecommunication systems.

These standards are not intended to be used as the final specification or bid document for any specific project. The standards are to be used as a starting point in a process of collaboration between the architect/designer, owners and DIT.
2.0 Telecommunication

2.1 Overview: The main telecommunication room provides demarcation between the per-floor horizontal service distribution cabling and the building voice, data, and video backbone cabling. Furthermore, it provides the connection point between the building backbone and horizontal distribution pathways. These securable room shall be dedicated to this purpose with no other building service sharing the space.

2.2 Conduit and Jack Requirements:

A. Minimum of four (4) 4" conduits must be provided from the Quazite pull boxes located near the property line to the telecommunications equipment room. Each conduit must have mule tape with footage markings.

B. Intra-building conduits (connecting communication rooms) shall have minimum of two (2) 4" empty conduits with mule tape identified with footages. Intra-building conduits must be provided vertically and horizontally between all communications rooms that are wired in a series. The number, locations and routing of these conduits are to be approved by the DIT Project Manager.

C. A one-inch conduit with drawstring must be provided to each communication device location and stubbed towards the telecommunications room. The 1" conduit must be stubbed to the nearest drop ceiling area. Cable trays may be required based on the overall density of the voice and data cabling. Only metallic conduit or PVC (schedule 40) smooth conduit are allowed.

D. Co-located voice and data communications cables may utilize the same 1" conduit into a single gang box.

E. Inaccessible or secure areas must have an entire conduit system from communication jack to the telecommunications equipment room.

F. Provide a conduit for all plenum and/or hard ceiling areas.

G. Empty conduits and boxes in concrete slabs or an under-slab duct /conduit distribution system, are required for systems furniture and/or freestanding furniture requiring communications outlets. Provide sleeves through floors and ceilings as required for cable pathways.

H. Provide a pull box every 200 feet and at each 90-degree bend.

I. Turn up under floor duct (UFD) three inches from the wall and at least three inches above the finished floor.
J. Accessible pull boxes which can be used as a junction point for several one-inch conduit runs, and which provide an empty three-inch conduit with mule tape having footage markings home run to the nearest Telecommunications Equipment room must be identified and detailed.

K. Provisions for dedicated voice and data jacks at mechanical EMCS stations and the direct dialer in the Telecommunications Equipment room for remote emergency monitoring must be made.

L. All voice and data jacks, wiring and cover plates will be furnished and installed by Fairfax County or its authorized vendors and contractors. Empty conduits with pull strings, pull boxes, junction boxes and fit-up of Telecommunications Equipment room with plywood, ground wire and buss bar, and electrical outlets as described in these guidelines, shall be included in the design and provided to the contractor.

2.3 Telecommunication Equipment Room: For telephone, data, video (CATV), etc., must be separate from electrical room.

A. Telecommunications Equipment rooms must be of adequate size to accommodate requirements for County telephone, data and CATV, but in no instance shall they be smaller than 10’ X 12’.

B. All four walls shall be covered with 4’x 8’x ¾” fire retardant plywood for County telephone, data and cable television equipment. Plywood shall have two coats of white paint and installed from floor to ceiling. (8ft x 4ft.). Additional backboards may be required for telephone or CATV equipment. Fire retardant stamp on the plywood must be in full view for inspection.

C. Provide anti-static VCT flooring in the room.

D. Door shall be minimum of 36” wide, opening outward. The door shall be secured by lock and key or access card reader.

E. Minimum of one Telecommunications Equipment room must be provided at each floor of a facility with additional rooms as required to accommodate the communications equipment and wiring requirements. The Telecommunication Rooms should be located above each other on the different floors. If the Telecommunications Rooms are not stacked, they shall have a means of access on the floor above and below via metal conduits or sleeves.
F. Adequate floor space for two (2) 19" wide by 26" deep by 84" high Cable Talk racks. Maintain minimum of three feet of clear space on all sides of electrical/communications equipment.

2.4 Cabling: Interior wiring on all new building shall be CAT-6 or better. Any deviation must be pre-approved by DIT.

A. Station Jacks Standard
   1. CAT 6 Siemon 1-CT-6-A4-A4-02 Dual Jacks with a white icon for voice and a red icon for data, 568B 8-pin, RJ45’s.

   2. CAT 6 Siemon 1-CT-6-A4-A4-02 Dual Jacks with white icon for voice and a red icon for data, 568B 8-pin, RJ45’s to be used upon request only.

B. Station Cabling Standard
   1. Data – Mohawk MegaLAN 400 CAT 6 24 AWG 4PR (blue in color). All cables should be plenum rated.
2. Voice – Mohawk CAT 6, 24 AWG 4PR, Yellow in color and plenum rated.

C. Connecting Blocks Standard
1. 110 Type CAT 6 Siemon # 100PR Voice Termination 110 Type CAT 6 Siemon# 300PR.
2. 110 Type CAT 6 Siemon # 100PR Data Termination.
3. 110 Type CAT 6 Siemon # 300PR.
4. 66 Type CAT 6 Siemon # S66M1-50 Data Termination.
5. 66 Type CAT 6 Siemon # S66M1-50 Voice Termination.

D. Patch Panels Standard
1. Siemon CAT 6 24-port-Blank #CT-PNL-24 48-port-Blank #CT-PNL-48 Inserts. Dual RJ45 #CTS-A4-A4-02 (red icons for data).

E. Patch Cords Standard
1. RJ45 to RJ45 8-pin-to-8-pin 568B CAT 6 (voice patch cables to be yellow in color).
2. RJ45 to RJ45 8-pin to 8-pin 568B CAT 6 (data patch cables to be grey in color).

F. Racks Standard
1. All new/future facilities.
2. Cable Talk rack 84” by 19” rack with minimum 5” cable management on both sides, electrical power strip and top panels.

G. Under Floor Duct Systems

H. Raised Floors
1. Twenty-four inch raised floor BICSI Telecommunications Distribution Methods Manual Volume I.

2.5 Standard Numbering Plan for Cabling Systems:

A. All vendors working on County IT projects shall maintain Fairfax County’s Numbering Plan for wiring. Station cables shall be labeled by the
communications room that they pull to, then by sequential numbering. For example, TC01-001 is station cable 001 connected to telephone room 01. The station end shall terminate in a dual jack with a white icon insert for voice and a red icon insert for data. The telephone room end shall terminate in wall-mounted blocks (AT&T 110 or Siemon 66 type) for voice cable, and directly to the CAT 6 patch panel for data cable.

B. Workstation cable runs cannot exceed 290 feet from the Telecommunications Equipment room. County buildings that exceed 290 feet from station set to the Telecommunications Room will require more than one Telecommunications Equipment Room.

C. All cables, circuits and facilities shall be clearly identified and labeled at all County sites. Cable shall be labeled at terminating points by use of durable self-laminating wire and cable markers. Patch panels, station jacks, terminal plates, etc., shall have typed labels. The AT&T 110/66 Siemon blocks shall be equipped with designation strips, which will be used to mark county cable and identify use. At the station jack, a label shall be placed at each cable, inside the outlet box, and on the jack faceplate.

2.6 Grounding:

A. All cabling systems and electronics-distribution equipment shall be grounded for both safety and minimization of electromagnetic interference. A 12-inch buss bar with an insulated number 6-ground wire shall be installed from the buss bar to the main building ground using a double lug nut, in accordance with the NEC guidelines. All building wiring, pathways and spaces, grounding and bonding shall meet or exceed the ANSI/EIA/TIA Telecommunications Infrastructure Standards as well as the NEC Electrical code (NFPA 70).
2.7 Electrical:

A. For every rack included in the design, there shall be one 120Vac/20A quadplex outlet at 90" AFF behind the proposed rack location(s) or installed on the rack. Each of these outlets shall be on a dedicated circuit connected to emergency power (UPS and generator).

B. Among all walls there should be one 120Vac/20A electrical duplex outlet every 6 feet at 18" AFF.

C. Minimum of two ceiling mounted, LED tube light fixtures with cover guard and a separate wall mounted switch to provide a minimum of 50-foot candles at 3’ above finish floor and connected to emergency power (UPS and generator).

2.8 HVAC: All Telecommunications Equipment rooms shall be provided with HVAC systems capable of maintaining the temperature of the room between 64 to 75 degrees F with the humidity being kept between 35 and 55 percent non-condensing. Separate split system units are acceptable.

2.9 Industry Standards and References: All building wiring, pathways, space grounding and bonding shall meet or exceed industry codes, Government Regulatory standards, and references current as of the time of the project design.


B. TIA/EIA-568-B.1-1 Commercial Building Telecommunications Cabling Standard Part 1: General Requirements - Addendum 1 – Minimum 4-Pair UTP and ScTP Patch Cable Bend Radius (May 2001)


E. TIA/EIA-568-B.1-4 Commercial Building Telecommunications Cabling Standard Part 1: General Requirements > Addendum 4 – Recognition of
DEPARTMENT OF INFORMATION TECHNOLOGY

APPENDIX B: INFRASTRUCTURE GUIDELINES

Category 6 and 850 nm Laser Optimized 50/125 Multimode Optical Fiber Cabling (February 2003)


J. TIA/EIA-568-B.2-2 Commercial Building Telecommunications Cabling Standard Part 2: Balanced Twisted-Pair Cabling Components – Addendum 2, Revision of Sub-clauses (December 2001)


L. TIA/EIA-568-B.2-4 Commercial Building Telecommunications Cabling Standard Part 2: Balanced Twisted-Pair Cabling Components – Addendum 4, Solderless Connection Reliability Requirements for Copper Connecting Hardware (June 2002)


P. TIA/EIA-568-3 Optical Fiber Cabling Components Standard (April 2002)


R. TIA-569-B Commercial Building Standard for Telecommunications Pathways and Spaces (October 2004)

S. TIA-570-B Residential Telecommunications Infrastructure Standard (April 2004)

T. TIA-598-C Optical Fiber Cable Color Coding (January 2005)

U. TIA/EIA-606-A Administration Standard for Commercial Telecommunications Infrastructure (May 2002)

V. J-STD-607-A Commercial Building Grounding (Earthling) and Bonding Requirements for Telecommunications (October 2002)

W. TIA-758-A Customer-owned Outside Plant Telecommunications Infrastructure Standard August 2004


3.0 Energy Management and Control Systems

3.1 Overview: Direct Digital Control (DDC) and Energy Management and Control System (EMCS) shall be installed on all new buildings. The control systems shall be based on Building Automation and Control (BACnet) protocol (ISO 16484-5) using County’s secured V-LAN network and approved Internet browser to remotely view system graphics, and monitor, control, and configure HVAC system and its properties. EMCS shall include Owner approved graphics including floor-level graphics with links to equipment for each building system.

3.2 Industry Standards and References: All systems shall meet or exceed industry codes, Government Regulatory standards, and references current as of the time of the project design.

A. American Institute of Architects (AIA).

B. ASHRAE—American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE).

C. Edison Electric Institute (EEI).

D. National Electronic Contractors Association (NECA).
4.0 Lighting Control Systems

4.1 Overview:

A. The following guidelines have been established for contractors to install and configure Lighting Control Systems (LCS). The standardization of LCS hardware, server, PC operating systems, databases, and networking will enable DIT to provide a controlled environment. This will ensure the LCS systems are well protected from cyber security threats and are physically secured, maintained and backed up. Secure access to these systems will be provided to the FMD staff and its contractors in order to manage and troubleshoot LCS issues and upgrade these systems.

B. The County has not standardized on a single Lighting Control System (LCS). There are several comprehensive lighting management software systems used in our buildings which provides intelligent control of the building’s lighting. The lights turn on and off automatically, brighten or dim to match different needs in different areas of a building or office. In addition, it turns on the outdoors lights when night falls, dim or brighten to meet light level requirements for spaces that have access to natural light through windows (daylighting). Lights should turn off when no one is in the area in order to save energy and reduce costs, respond to movement, and can come on in response to an alarm or emergency. Some spaces have multiple, preset scenes that offer staff the ability to quickly set lighting level in response to what activity is taking place.

C. Applications need to have a web interface that allows staff the ability to control, monitor, and schedule lights from a graphical floorplan. This building floorplan must include visual representation of the status of lights, indicate occupancy, and alarm on any fixtures that are failing. It must allow FMD staff the ability to easily set lighting levels, tune individual lights, and troubleshoot problems quickly by identifying fixtures that have raised alerts.

4.2 Industry Standards and References: All systems shall meet or exceed industry codes, Government Regulatory standards, and references current as of the time of the project design.

A. ASHRAE—American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE).

B. Illuminating Engineering Society (IES).

C. International Energy Conservation Codes (IECC).
5.0 Building Access Control Systems

5.1 Overview:

A. Scope and installation requirement for Building Access Control Systems (BACS) at each facility shall be evaluated with FMD during design phase. The County’s standard access control system for all facilities is Honeywell WIN-PAK PE software. All facilities must integrate with the County’s use of Honeywell WIN-PAK PE software.

B. Honeywell WinPak is an Integrated Security Management System (ISMS). The BAC system shall function as an electronic access control system and shall integrate the alarm monitoring, CCTV, digital video, ID badging and database management into a single platform. It shall function as a one-stop gateway for all the access control needs. A modular and network-enabled architecture shall allow maximum versatility for tailoring secure and dependable access and alarm monitoring solutions.

5.2 Industry Standards and References: All systems shall meet or exceed industry codes, Government Regulatory standards, and references current as of the time of the project design.

A. Federal Communications Commission (FCC):
   1. FCC Part 15 – Radio Frequency Device
   2. FCC Part 68 – Connection of Terminal Equipment to the Telephone Network

B. Underwriters Laboratories (UL):
   1. UL294 – Access Control System Units
   2. UL1076 – Proprietary Burglar Alarm Units and Systems

C. National Fire Protection Association (NFPA):
   1. NFPA70 – National Electrical Code

D. Electronic Industries Alliance (EIA):
   1. RS232C – Interface between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange
   2. RS485 – Electrical Characteristics of Generators and Receivers for use in Balanced Digital Multi-Point Systems
E. Federal Information Processing Standards (FIPS):
   1. Advanced Encryption Standard (AES) (FIPS 197)
   2. FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors

F. Homeland Security Presidential Directive 12 (HSPD-12)

5.3 System Components:

A. The Building Access Control System shall run on a single computer or on multiple computers, allowing flexibility in configuring a networked system. System components are divided into following six components:

1. Database Server: The database server is used for storing the database tables. This data is accessible to communication server and user interface for retrieving and generating the reports. The database server shall be installed on the client computer or any other computer connected to the network.

2. Archive Server: The archive server is used to obtain data from the archive database (the archive database consists of the backup details of the WINPAK main database).

3. Communication Server: The communication server routes user interface requests as well as the access transactions to the panel. The panel in-turn processes the transactions and sends the information to the database server as well as responses to the user interface through the communication server. When the communication server is sending information to the database server, it can also receive a request from the user interface. In this scenario, the communication server considers the user request as a higher priority and stops the panel-database server communication until the user request is processed. The communication server shall be installed on the client computer or any other computer connected to the network.

4. User Interface (Building Access Control System Client): The user interface helps Building Access Control System operators to communicate with the access control system. The user interface shall be installed on the computer where the database server or the communication server is installed, or any other computer connected to the network. Several client computers can be run simultaneously and can access the single database server simultaneously. The number of client computers varies based on the licensing information of Building Access Control System.
5. WIN-PAK API Server: The API server is used to obtain and set the details in the WIN-PAK database using the Application Programming Interface (API).

6. WIN-PAK Web: The WIN-PAK Web application is an extension of the WIN-PAK host application with limited operations. The operations such as Adding Cards and Adding Card Holders that are common to both WIN-PAK host and WIN-PAK Web application are saved on a common database server.

B. System Services: addition to above six components, the Building Access Control System includes the following four components, also called Building Access Control System services

1. Command File Server: A command file server provides text files containing device instructions that shall be stored in the command files database. The commands in the command files can be sent to the devices automatically on receiving, acknowledging, or clearing an alarm. Also, the command files can be manually executed.

2. Guard Tour server: A guard tour is a defined series of check points a guard must activate within a given amount of time. The check points are readers or input points where the guard presents the card or presses the button.

3. Tracking and Muster Server: A muster server is enabled in the event of an emergency and allows the card holders to swipe the readers. Muster areas are logical areas that contain readers to be used by the card holders, only if there is a call for muster (in the event of a disaster, for example).

4. Schedule Server: A schedule server schedules the list of events to be performed at a predetermined time and intervals such as hourly, daily, or monthly.
6.0 Building Security Surveillance Camera System


6.2 Industry Standards and References

A. The Security Industry Association (SIA)
   https://www.securityindustry.org/

B. The Physical Security Interoperability Alliance
   https://psialliance.org/

C. Open Network Video Interface Forum (ONVIF)
   https://www.onvif.org/

D. American Society for Industrial Security (ASIS International)
   https://www.asisonline.org/

E. Department of Homeland Security System Assessment and Validation for Emergency Responders (SAVER)—CCTV Technology Handbook
7.0 General Guidelines for EMCS, LCS and BAC Systems

7.1 Overview: All systems shall be isolated from the general County network and segmented on the FMD_VRF network. IT and FMD Energy Management staff shall access these systems only after Firewall Rules have been documented, approved, and set in place. FMD HVAC staff will have access through FairfaxNET’s FMD Department webpage under “FMD Internal – Employees Only” link.

7.2 Remote Access to Systems: Remote monitoring or remote-control access to any of the County’s systems is granted to the FMD staff and/or its contractors via the FFX Remote Portal to provide a gateway. The additional use of Symantec VIP Access is required to access Fairfax County network resources from outside the County network. This multifactor authentication (MFA) solution provides a more secure network environment, thus reducing the likelihood of a data breach via a compromised password.

7.3 County Standards and References:

A. Any computer hardware and software that is being provided must comply with the DIT Standards which are provided in Section 5 of the IT Plan—Section 5: Architecture and Infrastructure Foundation.

https://www.fairfaxcounty.gov/informationtechnology/it-plan

B. All proposed systems must comply with the County’s DIT Information Security Policy in order to be accepted by the County.

https://www.fairfaxcounty.gov/informationtechnology/sites/informationtechnology/files/assets/security/pm70-05_01.pdf

C. The Policy defines the minimum security requirements necessary, based on the most up-to-date information available, to protect Fairfax County Government IT Assets, including the managerial, operational, and technical protection requirements and controls to ensure the confidentiality, integrity, and availability of County IT Assets; compliance with requirements of applicable federal, state, and local law and County's policies and regulations (e.g. FIIPAA, PCI-DSS, PII and other specific privacy regulations current or established later); and standards and guidelines established by the National Institute of Standards and Technology (NIST), US Department of Homeland Security Cyber security guidelines, US CERT, and any other in the future. The Policy applies to all existing and future implementations of technology.
D. The Policy defines the acceptable use and management of internal and remote systems, services and information, and technical controls and procedures that govern the design, acquisition, implementation, administration and use of County systems. The Policy also discusses steps to assist in mitigating risks due to evolving cyber threats and vulnerabilities caused through use of IT Assets, through the internet, or perpetrated by those with malicious intentions. This Policy applies to all County agencies, employees, volunteers, service providers, vendors, contractors, and commercial entities (may be referred to as 'users' in county IT policy and procedure documents) that develop, implement, administer, or use Fairfax County information and communications systems, data and information.

E. Policy provides for and shall enforce protective measures and compliance actions for the county technology eco-system. This includes all County information and internal/external communications systems, and supporting infrastructure that support government interactions, operations and transactions, and that transmit, receive, or store confidential, sensitive, internal use, or public use County data and/or information regardless of media format, processing method, mobility, or platform.

F. All agencies and persons that may develop, implement, or use Fairfax County information systems shall abide by the requirements and procedures established by the County's Information Technology Security Office as authorized by the County Executive. The County Executive grants authority to the Chief Information Security Officer (CISO) to immediately apply mitigation actions to shut off the source of a cyber-attack through penetration or unauthorized installation including terminating use privileges and/or confiscating suspicious source technology components, conduct cyber forensics on IT Assets, investigate breach and/or unauthorized use activities, and make recommendations related to appropriate disciplinary measures. The CISO may monitor systems and use, and conduct security scans and audits at its discretion. Further, the CISO is deemed the County's subject matter expert to support legal matters related to IT and cyber matters supporting the Office of the County Attorney.

G. Any information, data, or any other content that is in or transmitted through Fairfax County IT platforms, communications systems and infrastructure including through County external sources such as the Internet, County Social Media venues, subscription and 'Cloud' services are the property of Fairfax County. Therefore, users should not expect that personal information conducted through the county is private other than data explicitly covered by confidentiality and privacy laws.
H. All proposed computer hardware and software must be submitted to DIT for approval before it is purchased.

I. System’s architecture, configuration and network requirements must be submitted to DIT for approval before it can be installed in the County’s IT Infrastructure.

7.4 Procedures - Process Outline

A. Initial meeting with Capital Facilities (CAP), Facilities Management (FMD), Information Technology (DIT) and Contractor(s) to discuss new capital or renewal project to review/discuss the project.

- Review IT Standards required for system hardware and software.

- Discuss secure network requirements for County EMCS systems.

- DIT must review and approve all computer hardware and software recommended by Contractors to ensure compliance with the current version of IT standards at the time of installation.

- Discuss County IT environments during the implementation life cycle (Development, Test, Acceptance, and Production).

- Explain the DIT Services Provider Consultant/Contractor Agreement concerning access to and use of information systems and communications technology at Fairfax County, Virginia

- Explain process for obtaining Contractor User ID’s/Passwords.

- Contractor is responsible for conducting the required Background Checks of employees when the contractor is requesting a County User ID and Password. The contractor shall submit Employee Background checks to the hiring County agency.

- The County Agency who is hiring the contractors must have their Agency Information Security Coordinator (AISC) submit the necessary completed forms and Contractor Employee Background checks to INFOSEC so that the Contractor employees’ User ID’s and Passwords are created and issued. No sharing of user accounts is permitted.
• Explain onsite installation requirements and Remote Access for necessary support after installation.

• Agree on procurement method for buying new hardware and software for the EMCS system. Recommend CAP set aside the funding for hardware and software and let DIT purchase EMCS hardware and software to ensure all County IT standards are met.

B. Project Kick off meeting with CAP, FMD, DIT, Contractor(s) for the project.

• Discuss and review requirements for EMCS systems.

• Discuss and review EMCS hardware and software system configuration, storage disk space and database requirements. Ensure that the Systems Platform staff is involved in this process, reviews and approves what hardware to be purchased.

• Discuss and review supporting software required for the EMCS system (Java, Glassfish, etc.). Ensure that the INFOSEC staff is involved in this process and reviews and approves the required supporting software so that it can be installed on the new EMCS server(s) or workstation(s).

• Discuss and review requirements for EMCS systems access for FMD staff and contractors.

• Complete the Purchase Orders for CAP or FMD so that the hardware and software of the EMCS system are ordered.

• Discuss and review EMCS networking requirements and network schematics, number of required IP addresses, required ports to be opened, and network protocol(s) to be used.

• Discuss and review the number of required network jacks.

• Setup a site visit to inspect network requirements.

• Submit request to Telecomm Help Desk for the required data jacks for the EMCS system.

• Submit necessary Firewall Ruleset Requests to INFOSEC to ensure that the EMCS devices can talk to each other.
When the hardware has arrived, submit the necessary Server forms to the DIT Systems Platforms staff so they install and configure all the hardware and software required for the EMCS system.

Have Capital Facilities or FMD submit the User ID/Password request for contractor staff along with the signed IT Services Provider Consultant/Contractor Agreements.

Once DIT Systems Platform staff notifies the General Business Applications Branch staff that the server(s), database, storage disk space and all other system components for the EMCS system are ready for the EMCS application to be installed, setup meetings with Contractor, DIT and FMD staff for the EMCS system installation.

Setup meetings with Contractor, FMD and DIT staff to ensure that EMCS systems meets FMD’s needs.

Setup system training for the FMD and DIT EMCS Administrators.

Setup systems training for the FMD EMCS users.

Setup commissioning meetings for the EMCS system.

Provide all the project documents (Design document, User manual, etc.) to System Administrators.

C. Post Installation requirements.

FMD to establish post warranty period Service Maintenance Contracts for EMCS system.

Review the need for EMCS system access for contractors to maintain and support the system and remove unneeded access. (Note: some contractors work on the project for the initial installation and configuration only and will not provide system maintenance and support after turning over the system to FMD).

7.5 DIT Forms Required for Installation of Systems

A. IT Services Provider Consultant/Contractor Agreement: Signed document by consultant/contractor and the company agreeing to the proper use concerning access to and use of Information Systems and Communications Technology at Fairfax County, VA
B. INFOSEC form for requesting County Userid and Password: This shall be completed by County agency.

https://infoweb.fairfaxcounty.gov/iprotect/

C. INFOSEC Firewall Ruleset Form is used to request access through County firewalls. Identify the IPs (or group of IPs) addresses that are needed to communicate to other areas on the network, what protocol, and what port(s) are being utilized for communication between the equipment.


D. INFOSEC Waiver/Exception to Policy Form outlines what software or hardware (not standard to Fairfax Count) is requiring an exception and why it is required. Must provide computer information you are installing on, documentation on the system and/or hardware, and be signed off by the agency director.

8.0 Radio System

8.1 Overview: Contractor shall provide and install roof curb, weather sealed aluminum vault with conduits on the roof close to the Telecommunication room. This shall be provided for all public safety buildings and/or as requested by DIT. The vault shall serve as the centralized entry point for the installation of conduits to house antenna wires for public safety radio system.

8.2 Curb, Vault and Conduits:

A. Roof Curb
   1. Provide a roof curb manufactured of 14 gage galvanized steel with continuously welded seams and mitered corners providing air and watertight construction. The curb shall be minimum of 8” high. Internally reinforced as needed for the installation of the vault.

B. Aluminum Vault
   1. The vault shall be minimum of 0.080-inch-thick aluminum with gaskets and stainless-steel hardware.
   
   2. It shall have a UV protected powder coating.
   
   3. Vault at minimum should be 12” (L) x 12” (H) x 20” (H).

C. Conduit
   1. Install two (2) 4” PVC conduits.
   
   2. Vault shall have tight exit seals with inserts for the three (3) 4” conduits. This shall be constructed of aluminum or stainless-steel flange.
   
   3. The conduits shall be installed from the vault to a pull box located to the closet restroom or wet area. From the pull box install two (2) 4” conduits and terminate them into the telecommunication room. Third exit seal will be a spare for future use.
   
   4. Each conduit must have mule tape with footage markings.
   
   5. Conduits shall be installed with minimum fitting consisting of 45- and 90-degree bends. All 45-degree bends shall be sweeping bends, and at each 90-degree bend install a pull box.
8.3 Industry Standards and References: All systems shall meet or exceed industry codes, Government Regulatory standards, and references current as of the time of the project design.

A. Construction Industry Specifications (CSI)
   a) Section 077200 – Roof Accessories