

# **UNIFIED FACILITIES CRITERIA (UFC)**

---

## **ELECTRONIC SECURITY SYSTEMS**



**APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED**

*This Page Intentionally Left Blank*

## UNIFIED FACILITIES CRITERIA (UFC)

### ELECTRONIC SECURITY SYSTEMS

Any copyrighted material included in this UFC is identified at its point of use.  
Use of the copyrighted material apart from this UFC must have the permission of the copyright holder.

Indicate the Military Department Preparing Activity responsible for the document.

U.S. ARMY CORPS OF ENGINEERS

NAVAL FACILITIES ENGINEERING SYSTEMS COMMAND (Preparing Activity)

AIR FORCE CIVIL ENGINEER CENTER

Record of Changes (changes are indicated by \1\ ... /1/)

Change No.	Date	Location

---

This UFC supersedes UFC 4-021-02, *Electronic Security Systems*, dated 1 October 2013.

*This Page Intentionally Left Blank*

## FOREWORD

The Unified Facilities Criteria (UFC) system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria, and applies to the Military Departments, the Defense Agencies, and the DoD Field Activities in accordance with [USD \(AT&L\) Memorandum](#) dated 29 May 2002. UFC will be used for all DoD projects and work for other customers where appropriate. All construction outside of the United States, its territories, and possessions is also governed by Status of Forces Agreements (SOFA), Host Nation Funded Construction Agreements (HNFA), and, in some instances, Bilateral Infrastructure Agreements (BIA). Therefore, the acquisition team must ensure compliance with the most stringent of the UFC, the SOFA, the HNFA, and the BIA, as applicable.


UFC are living documents and will be periodically reviewed, updated, and made available to users as part of the Military Department's responsibility for providing technical criteria for military construction. Headquarters, U.S. Army Corps of Engineers (HQUSACE), Naval Facilities Engineering Systems Command (NAVFAC), and the Air Force Civil Engineer Center (AFCEC) are responsible for administration of the UFC system. Technical content of UFC is the responsibility of the cognizant DoD working group. Defense Agencies should contact the respective DoD Working Group for document interpretation and improvements. Recommended changes with supporting rationale may be sent to the respective DoD working group by submitting a Criteria Change Request (CCR) via the Internet site listed below.

UFC are effective upon issuance and are distributed only in electronic media from the following source:

- Whole Building Design Guide website <https://www.wbdg.org/dod>.

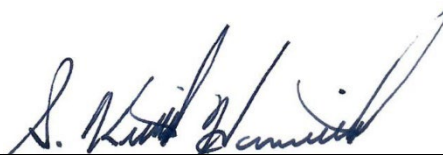
Refer to UFC 1-200-01, *DoD Building Code*, for implementation of new issuances on projects.

### AUTHORIZED BY:



---

THOMAS P. SMITH, P.E., SES  
Chief, Engineering and Construction  
U.S. Army Corps of Engineers



---

S. KEITH HAMILTON, P.E., SES  
Chief Engineer and Assistant Commander  
Planning, Design and Construction  
Naval Facilities Engineering Systems Command



---

THOMAS P. BROWN, SES  
Deputy Director of Civil Engineers  
DCS/Logistics, Engineering &  
Force Protection (HAF/A4C)  
HQ United States Air Force



---

MARK S. SINDER, SES  
Deputy Assistant Secretary of Defense  
(Infrastructure Modernization and Resilience)  
Office of the Secretary of Defense

*This Page Intentionally Left Blank*

## TABLE OF CONTENTS

<b>CHAPTER 1 INTRODUCTION .....</b>	<b>1</b>
<b>1-1 REISSUES AND CANCELS.....</b>	<b>1</b>
<b>1-2 PURPOSE AND SCOPE.....</b>	<b>1</b>
<b>1-3 APPLICABILITY.....</b>	<b>1</b>
<b>1-4 PROTECTION PROGRAM RISK ASSESSMENTS.....</b>	<b>1</b>
<b>1-5 REGULATORY OR FUNCTIONAL AUTHORITIES.....</b>	<b>1</b>
1-5.1 Military Authorities.....	1
<b>1-6 GENERAL BUILDING REQUIREMENTS.....</b>	<b>3</b>
<b>1-7 CYBERSECURITY.....</b>	<b>3</b>
<b>1-8 SECURITY ENGINEERING UFC SERIES.....</b>	<b>3</b>
1-8.1 DoD Minimum Antiterrorism Standards for Buildings.....	3
1-8.2 DoD Security Engineering Facilities Planning Manual.....	3
1-8.3 DoD Security Engineering Facilities Design Manual.....	4
1-8.4 Security Engineering Support Manuals.....	4
1-8.5 Security Engineering UFC Application.....	4
1-8.6 Compliance with Security Regulations.....	5
<b>1-9 GLOSSARY.....</b>	<b>6</b>
<b>1-10 REFERENCES.....</b>	<b>6</b>
<b>CHAPTER 2 ELECTRONIC SECURITY SYSTEM OVERVIEW.....</b>	<b>7</b>
<b>2-1 SYSTEM DEFINITION.....</b>	<b>7</b>
<b>2-2 PHYSICAL SECURITY AND ESS.....</b>	<b>8</b>
<b>2-3 PROJECT CATEGORIES AND ESS DESIGN RESPONSIBILITIES.....</b>	<b>9</b>
2-3.1 Construction.....	9
2-3.2 Equipment Installation.....	9
<b>2-4 PROJECT DESIGN REQUIREMENTS.....</b>	<b>10</b>
2-4.1 Regulatory Requirements.....	10
2-4.2 Risk Assessment Results.....	10
2-4.3 Standard Systems.....	10
2-4.4 Existing Systems.....	10
2-4.5 Approved Components and Systems.....	11
2-4.6 Alarm Monitoring.....	11

2-4.7	End-User Requests. ....	11
2-4.8	Security-in-Depth .....	11
<b>2-5</b>	<b>PROJECT PHASES. ....</b>	<b>13</b>
2-5.1	Planning.....	13
2-5.2	Design.....	14
2-5.3	Procurement and Installation. ....	14
2-5.4	Testing and Training. ....	14
2-5.5	Final System Documentation. ....	14
2-5.6	Maintenance and Sustainment. ....	14
<b>CHAPTER 3</b>	<b>INTRUSION DETECTION SYSTEM.....</b>	<b>17</b>
<b>3-1</b>	<b>TECHNOLOGY OVERVIEW. ....</b>	<b>17</b>
<b>3-2</b>	<b>INTERIOR INTRUSION DETECTION. ....</b>	<b>17</b>
3-2.1	High Security Switch.....	18
3-2.2	Volumetric Sensor. ....	19
3-2.3	Beam-Break Sensor. ....	21
3-2.4	Scanning Laser Sensor.....	22
3-2.5	Vibration Sensor. ....	24
3-2.6	Glass-Break Sensor.....	25
3-2.7	Duress Switch.....	27
3-2.8	Local Annunciator. ....	28
3-2.9	Arm/Disarm Device with Zone Status Indicator.....	28
3-2.10	Intrusion Panel.....	29
<b>3-3</b>	<b>EXTERIOR PERIMETER INTRUSION DETECTION. ....</b>	<b>30</b>
3-3.1	Fence-Disturbance Sensor. ....	32
3-3.2	Taut-Wire Sensor.....	34
3-3.3	Bistatic Microwave Sensor.....	36
3-3.4	Monostatic Microwave Sensor. ....	38
3-3.5	Ported Coaxial Cable Sensor.....	39
3-3.6	Electrostatic Field Sensor. ....	40
3-3.7	Active Infrared Sensor. ....	43
3-3.8	Passive Infrared Sensor.....	44
3-3.9	Dual Technology Sensor.....	45

3-3.10	Scanning Laser Sensor.....	45
3-3.11	High Security Switch on Perimeter Gates.....	45
3-3.12	Field Distribution Box.....	47
<b>3-4</b>	<b>EXTERIOR WIDE AREA INTRUSION DETECTION.....</b>	<b>48</b>
3-4.1	Ground Surveillance Radar.....	49
3-4.2	Video Analytics.....	50
3-4.3	Electronic Harbor Security System (EHSS).....	51
<b>3-5</b>	<b>GENERAL DESIGN CONSIDERATIONS.....</b>	<b>52</b>
3-5.1	Compliance with Security Regulations.....	52
3-5.2	Alarm Monitoring Location.....	52
3-5.3	Zone Definition.....	52
3-5.4	Sensor Selection and Placement.....	53
3-5.5	Performance Metrics.....	54
3-5.6	Multi-Layered Detection.....	54
3-5.7	Supervision and Encryption.....	54
3-5.8	Tamper Switches.....	55
3-5.9	Alarm Annunciation.....	55
3-5.10	Alarm Assessment.....	55
3-5.11	Video Analytics for Intrusion Detection.....	55
3-5.12	Operational Availability.....	55
3-5.13	Latency.....	56
3-5.14	Backup Power.....	56
3-5.15	Wireless Sensors.....	56
3-5.16	UL 2050.....	56
<b>CHAPTER 4</b>	<b>ACCESS CONTROL SYSTEM.....</b>	<b>57</b>
<b>4-1</b>	<b>TECHNOLOGY OVERVIEW.....</b>	<b>57</b>
<b>4-2</b>	<b>SYSTEM CONFIGURATION.....</b>	<b>57</b>
<b>4-3</b>	<b>PRINCIPLE OF OPERATION.....</b>	<b>59</b>
<b>4-4</b>	<b>ACS ENTRY DEVICES.....</b>	<b>59</b>
4-4.1	Credential Devices.....	59
4-4.2	Coded Devices.....	60
4-4.3	Biometric Devices.....	60

4-4.4	Combining Entry Authorization Identifiers. ....	61
4-4.5	Selecting Entry Authorization Identifiers. ....	61
<b>4-5</b>	<b>OTHER ACS FEATURES. ....</b>	<b>61</b>
4-5.1	Anti-Passback. ....	61
4-5.2	Anti-Piggybacking/Anti-Tailgating. ....	62
4-5.3	Two-Man Rule. ....	62
4-5.5	Event Tracking/Event Logs. ....	62
<b>4-6</b>	<b>ACS EQUIPMENT. ....</b>	<b>63</b>
4-6.1	ACS Central Computer. ....	63
4-6.2	ACS Workstation. ....	63
4-6.3	Badging/Enrollment Equipment. ....	63
4-6.4	ACS Local Controller / Control Panel. ....	64
4-6.5	Entry Devices. ....	64
4-6.6	Card Types. ....	65
4-6.7	Keypads and PIN Codes. ....	66
4-6.8	Biometric Readers. ....	66
4-6.9	Mobile PIV Certificates. ....	68
4-6.10	Locking Devices. ....	68
4-6.11	Request-to-Exit (REX) Devices. ....	69
4-6.12	Door Position Monitoring Devices. ....	71
4-6.13	Access Controlled Door Configuration. ....	71
4-6.14	Typical Access Controlled Booth / Sally Port Configuration. ....	73
<b>4-7</b>	<b>ACS DESIGN CONSIDERATIONS. ....</b>	<b>74</b>
<b>CHAPTER 5 VIDEO SURVEILLANCE SYSTEM .....</b>		<b>77</b>
<b>5-1</b>	<b>OVERVIEW. ....</b>	<b>77</b>
5-1.1	Alarm Assessment. ....	77
5-1.2	Access Control. ....	77
5-1.3	Surveillance. ....	77
5-1.4	Evidentiary Archives. ....	77
<b>5-2</b>	<b>CAMERAS. ....</b>	<b>78</b>
5-2.1	Network Camera. ....	78
5-2.2	Indoor Cameras. ....	79

5-2.3	Outdoor Cameras.....	79
5-2.4	Fixed Position Cameras.....	80
5-2.5	Pan/Tilt/Zoom (PTZ) Cameras.....	80
5-2.6	Dome Cameras.....	81
<b>5-3</b>	<b>ILLUMINATION.....</b>	<b>82</b>
5-3.1	Illuminance.....	82
5-3.2	Uniformity.....	83
5-3.3	Glare Reduction.....	84
5-3.4	Dynamic Range.....	84
5-3.5	Interior Lighting.....	85
<b>5-4</b>	<b>VIEWING IN LOW-LIGHT CONDITIONS.....</b>	<b>85</b>
5-4.1	Black/White Switching.....	85
5-4.2	Infrared Illuminators.....	85
5-4.3	Thermal Imagers.....	86
<b>5-5</b>	<b>ANGLE OF VIEW AND FIELD OF VIEW.....</b>	<b>87</b>
5-5.1	Field of View.....	87
5-5.2	Angle of View.....	88
5-5.3	Field of View Calculations.....	89
<b>5-6</b>	<b>CAMERA RESOLUTION.....</b>	<b>90</b>
5-6.1	Object Discrimination.....	90
5-6.2	Maximum Effective Range.....	93
<b>5-7</b>	<b>VIDEO FRAME RATE.....</b>	<b>93</b>
<b>5-8</b>	<b>DIGITAL VIDEO BANDWIDTH.....</b>	<b>93</b>
5-8.1	Bandwidth Calculations.....	93
5-8.2	Example.....	94
<b>5-9</b>	<b>DIGITAL VIDEO STORAGE.....</b>	<b>95</b>
5-9.1	Edge Storage.....	95
5-9.2	Network Video Recorder.....	95
5-9.3	Required Storage Capacity.....	96
<b>5-10</b>	<b>VIDEO WORKSTATION.....</b>	<b>97</b>
<b>5-11</b>	<b>ANALYTICS.....</b>	<b>97</b>
5-11.1	Video Analytics.....	97

5-11.2	Audio Analytics. ....	98
<b>5-12</b>	<b>VSS DESIGN PROCESS SUMMARY. ....</b>	<b>98</b>
5-12.1	Define Security Objectives for VSS. ....	98
5-12.2	Develop Camera Layout to Meet Security Objectives. ....	98
5-12.3	Verify Illumination is Sufficient for Each Scene of Interest. ....	98
5-12.4	Specify Workstation Locations. ....	98
5-12.5	Specify Recording Locations and Capacity. ....	99
5-12.6	Define Network Architecture. ....	99
5-12.7	Define Power Requirements. ....	99
5-12.8	Describe Software and Integration Requirements. ....	99
<b>CHAPTER 6</b>	<b>DATA TRANSMISSION. ....</b>	<b>101</b>
<b>6-1</b>	<b>INTRODUCTION. ....</b>	<b>101</b>
<b>6-2</b>	<b>BANDWIDTH ANALYSIS. ....</b>	<b>101</b>
<b>6-3</b>	<b>SECURE COMMUNICATIONS. ....</b>	<b>101</b>
<b>6-4</b>	<b>NETWORK TOPOLOGY. ....</b>	<b>102</b>
6-4.1	General Network Topologies. ....	102
<b>6-5</b>	<b>COMMUNICATION REDUNDANCY. ....</b>	<b>107</b>
<b>6-6</b>	<b>TRANSMISSION MODES/PROTOCOLS. ....</b>	<b>107</b>
<b>6-7</b>	<b>TRANSMISSION MEDIA. ....</b>	<b>108</b>
6-7.1	Hardwired. ....	108
6-7.2	Direct Subscriber Lines (T1 Lines). ....	108
6-7.3	Wireless. ....	109
6-7.4	Free-Space Optics (FSO). ....	109
<b>6-8</b>	<b>NETWORK DEVICES. ....</b>	<b>111</b>
<b>6-9</b>	<b>TECHNOLOGY COMPARISON. ....</b>	<b>111</b>
<b>6-10</b>	<b>ENCRYPTION. ....</b>	<b>113</b>
<b>CHAPTER 7</b>	<b>COMMAND AND CONTROL DISPLAY EQUIPMENT. ....</b>	<b>115</b>
<b>7-1</b>	<b>INTRODUCTION. ....</b>	<b>115</b>
<b>7-2</b>	<b>WORKSTATION. ....</b>	<b>115</b>
7-2.1	Computer. ....	116
7-2.2	Keyboard and Pointing Device. ....	116
7-2.3	Joystick. ....	117

7-2.4	Microphone. ....	117
7-2.5	Speaker. ....	117
7-2.6	Enrollment Equipment. ....	117
7-2.7	Monitors. ....	117
7-2.8	Printer. ....	117
7-2.9	Uninterruptible Power Supply. ....	117
<b>7-3</b>	<b>FILE SERVER. ....</b>	<b>118</b>
7-3.1	Hardware Requirements. ....	118
7-3.2	Physical Protection. ....	119
7-3.3	Backup Power. ....	120
<b>7-4</b>	<b>SOFTWARE. ....</b>	<b>120</b>
<b>CHAPTER 8</b>	<b>ESS SUBSYSTEM INTEGRATION. ....</b>	<b>121</b>
<b>8-1</b>	<b>OVERVIEW. ....</b>	<b>121</b>
<b>8-2</b>	<b>COMMUNICATION FROM THE IDS TO THE ACS. ....</b>	<b>121</b>
<b>8-3</b>	<b>COMMUNICATION FROM THE IDS (OR COMBINED ACS/IDS) TO THE VSS. ....</b>	<b>121</b>
8-3.1	Hardwired Conductors. ....	121
8-3.2	Serial Communications. ....	122
8-3.3	Software-Based Integration for Networked ESS. ....	122
<b>8-4</b>	<b>COMMUNICATION FROM THE VSS TO THE ACS. ....</b>	<b>122</b>
<b>8-5</b>	<b>COMMUNICATION FROM THE ACS TO THE CENTRAL MONITORING STATION. ....</b>	<b>122</b>
<b>8-6</b>	<b>DESIGN GUIDANCE ON IT SYSTEM COORDINATION. ....</b>	<b>123</b>
<b>8-7</b>	<b>INTEGRATING ESS AND OTHER SYSTEMS. ....</b>	<b>123</b>
<b>8-8</b>	<b>COMMON CONSIDERATIONS FOR ESS DESIGNERS. ....</b>	<b>123</b>
<b>CHAPTER 9</b>	<b>DESIGN PROCESS SUMMARY. ....</b>	<b>125</b>
<b>9-1</b>	<b>INTRODUCTION. ....</b>	<b>125</b>
<b>9-2</b>	<b>PROJECT PLANNING. ....</b>	<b>125</b>
9-2.1	Balance Project Funding and Project Scope. ....	125
9-2.2	Existing Site Plans and Building Plans. ....	125
9-2.3	Multi-Organizational Interfaces. ....	125
9-2.4	Space Planning. ....	127
9-2.5	ESS Site Surveys. ....	127

9-2.6	Central Monitoring Station. ....	127
<b>9-3</b>	<b>INITIAL DRAWING PREPARATION.....</b>	<b>128</b>
9-3.1	Cable Schedule. ....	128
9-3.2	Functional Matrix. ....	130
<b>9-4</b>	<b>BASIS OF DESIGN. ....</b>	<b>130</b>
<b>9-5</b>	<b>DESIGN DEVELOPMENT PHASES. ....</b>	<b>131</b>
9-5.1	Concept Design (35%).....	131
9-5.2	Intermediate Design (65%). ....	132
9-5.3	Pre-Final Design (95%).....	133
9-5.4	Final Design (100%). ....	135
<b>9-6</b>	<b>BIDDING.....</b>	<b>135</b>
<b>CHAPTER 10</b>	<b>CROSS-DISCIPLINE COORDINATION .....</b>	<b>137</b>
<b>10-1</b>	<b>GENERAL COORDINATION. ....</b>	<b>137</b>
<b>10-2</b>	<b>END-USER/CUSTOMER.....</b>	<b>137</b>
<b>10-3</b>	<b>HOST INSTALLATION/BASE.....</b>	<b>137</b>
<b>10-4</b>	<b>CIVIL COORDINATION.....</b>	<b>137</b>
10-4.1	Gate Control (Vehicle/Pedestrian Gates and Sally Ports).....	137
10-4.2	Underground Site Work. ....	138
10-4.3	Outdoor Perimeter Security Features. ....	138
<b>10-5</b>	<b>ARCHITECTURAL COORDINATION. ....</b>	<b>138</b>
10-5.1	Balance Security With Convenience.....	139
<b>10-6</b>	<b>ELECTRICAL COORDINATION. ....</b>	<b>139</b>
10-6.1	Power.....	139
10-6.2	Backup Power.....	139
10-6.3	Grounding, Bonding, and Lightning Protection. ....	140
10-6.4	Surge Protection. ....	140
10-6.5	Electromagnetic Interference (EMI). ....	140
10-6.6	Tamper Protection. ....	140
10-6.7	Cable Type. ....	141
10-6.8	Radio Frequencies (RF).....	142
10-6.9	Voltage Drop Considerations.....	142
10-6.10	Harmonics.....	143

10-6.11	Raceway.....	143
10-6.12	Labeling.....	143
10-6.13	Shielding.....	144
10-6.14	Intercom System.....	144
10-6.15	Lighting.....	144
<b>10-7</b>	<b>LIFE SAFETY AND FIRE PROTECTION COORDINATION.....</b>	<b>144</b>
10-7.1	Fire Alarm System.....	144
<b>10-8</b>	<b>MATERIAL ENTRY CONTROL.....</b>	<b>145</b>
<b>CHAPTER 11 SYSTEM TESTING, TRAINING, AND FINAL DOCUMENTATION.....</b>		<b>147</b>
<b>11-1</b>	<b>OVERVIEW.....</b>	<b>147</b>
<b>11-2</b>	<b>TRAINING.....</b>	<b>147</b>
11-2.1	Training Types.....	147
11-2.2	Training Plan.....	150
11-2.3	Training Content.....	150
11-2.4	Training Personnel Requirements.....	151
<b>11-3</b>	<b>SYSTEM ACCEPTANCE TESTING (SAT).....</b>	<b>151</b>
11-3.1	General.....	151
11-3.2	Test Plan.....	153
11-3.3	Pre-Acceptance Testing.....	157
11-3.4	System Acceptance Testing.....	158
11-3.5	Government Acceptance.....	162
11-3.6	System Turn-over.....	162
<b>11-4</b>	<b>FINAL DOCUMENTATION.....</b>	<b>162</b>
11-4.1	Final Test Report.....	162
11-4.2	Operations & Maintenance Manuals.....	163
11-4.3	Final As-built Drawings.....	163
11-4.4	Warranty Documentation.....	163
<b>APPENDIX A INTERIOR IDS ZONE EXAMPLES.....</b>		<b>165</b>
<b>A-1</b>	<b>SENSITIVE COMPARTMENTED INFORMATION FACILITY AND SPECIAL ACCESS PROGRAM FACILITY.....</b>	<b>165</b>
A-1.1	Coverage Based on Cognizant Security Authority Written Designation of Security-In-Depth.....	165
A-1.2	Coverage Based on No Written Designation of Security-In-Depth.....	166

A-1.3	DoD Criteria Document.....	166
A-1.4	Policy Baseline. ....	166
A-1.5	Baseline Intrusion Detection System Requirements. ....	167
A-1.6	Tamper Protection. ....	168
A-1.7	External Transmission Line Security.....	168
A-1.8	Emergency Backup Electrical Power. ....	168
A-1.9	Optional Equipment. ....	169
<b>A-2</b>	<b>SECURE ROOM (TOP SECRET OR SECRET OPEN STORAGE).....</b>	<b>169</b>
A-2.1	Coverage Based on Cognizant Security Authority Written Designation of Security-In-Depth .....	169
A-2.2	Coverage Based on No Written Designation of Security-In-Depth.....	170
A-2.3	Policy Baseline. ....	170
A-2.4	Baseline Intrusion Detection System Requirements. ....	170
A-2.5	Tamper Protection. ....	171
A-2.6	External Transmission Line Security.....	171
A-2.7	Emergency Backup Electrical Power. ....	171
<b>A-3</b>	<b>ARMS STORAGE AREA (ARMORY, ARMS ROOM, READY ISSUE ROOM). 172</b>	
A-3.1	Policy Baseline. ....	172
A-3.2	Baseline Intrusion Detection System Requirements. ....	173
A-3.3	Tamper Protection. ....	173
A-3.4	Emergency Backup Electrical Power. ....	174
<b>A-4</b>	<b>MAGAZINE (EARTH-COVERED MAGAZINE).....</b>	<b>174</b>
A-4.1	Policy Baseline. ....	175
A-4.2	Baseline Intrusion Detection System Requirements. ....	175
A-4.3	Tamper Protection. ....	175
A-4.4	Emergency Backup Electrical Power. ....	176
A-4.5	Hazards of Electromagnetic Radiation to Ordnance (HERO). ....	176
<b>APPENDIX B</b>	<b>SITE SURVEY CHECKLIST .....</b>	<b>177</b>
<b>B-1</b>	<b>ESS SITE SURVEY CHECKLIST. ....</b>	<b>177</b>
<b>APPENDIX C</b>	<b>EXAMPLE DRAWINGS .....</b>	<b>185</b>
<b>C-1</b>	<b>ESS EXAMPLE DRAWINGS. ....</b>	<b>185</b>
C-1.1	Symbols and Abbreviations. ....	186

C-1.2	Interior Sensor Details. ....	187
C-1.3	Exterior Sensor Details. ....	188
C-1.4	Access Control Details.....	191
<b>APPENDIX D GLOSSARY .....</b>		<b>193</b>
D-1	<b>ACRONYMS AND ABBREVIATIONS.....</b>	<b>193</b>
D-2	<b>DEFINITION OF TERMS.....</b>	<b>197</b>
<b>APPENDIX E REFERENCES .....</b>		<b>203</b>
<b>APPENDIX F ADDITIONAL REFERENCES .....</b>		<b>209</b>

## FIGURES

Figure 1-1	Security Engineering UFC Application .....	5
Figure 2-1	Conceptual System Diagram for an Integrated System .....	8
Figure 2-2	Security-in-Depth .....	13
Figure 3-1	IDS Technology Categories .....	17
Figure 3-2	Typical HSS Secure Side Door Configuration.....	19
Figure 3-3	Volumetric Sensor Coverage Patterns.....	21
Figure 3-4	Beam-Break Sensor Transmitter and Receiver .....	22
Figure 3-5	Scanning Laser Sensor Coverage Pattern .....	23
Figure 3-6	Vibration Sensors .....	25
Figure 3-7	Glass-Break Sensors.....	27
Figure 3-8	Duress Switch with Recessed Activation Button .....	28
Figure 3-9	Arm/Disarm Devices .....	29
Figure 3-10	Intrusion Panel.....	30
Figure 3-11	Single Line of Detection .....	31
Figure 3-12	Dual Lines of Detection .....	31
Figure 3-13	Fiber Optic Sensor Cable .....	33
Figure 3-14	Taut-Wire Sensor .....	35
Figure 3-15	Bistatic Microwave Sensor .....	37
Figure 3-16	“Double Stacked” Microwave Configuration.....	38
Figure 3-17	Monostatic Microwave Sensor .....	38
Figure 3-18	Ported Coaxial Cable Sensor.....	40
Figure 3-19	Electrostatic Field Sensor.....	42

Figure 3-20	Active Infrared Sensor.....	43
Figure 3-21	Passive Infrared Sensor .....	45
Figure 3-22	Dual Technology Sensor.....	46
Figure 3-23	Field Distribution Boxes.....	48
Figure 3-24	Ground Surveillance Radar.....	50
Figure 3-25	Exterior Perimeter IDS Zone Layout.....	53
Figure 4-1	Example Access Control System .....	58
Figure 4-2	Sample Access Controlled Door Configuration (Single Door) .....	72
Figure 4-3	Sample Access Controlled Door Configuration (Double Door) .....	72
Figure 4-4	Sample Access Controlled Door Configuration (Exit-Only Double Door)	73
Figure 4-5	Sample Access Controlled Booth / Sally Port Configuration .....	74
Figure 5-1	Example Block Diagram for a VSS .....	78
Figure 5-2	Scene Illuminance and Faceplate Illuminance .....	83
Figure 5-3	Effect of Glare on Camera Image Quality .....	84
Figure 5-4	Angle of View and Field of View .....	87
Figure 6-1	Enclosures for Secure Communications.....	102
Figure 6-2	Star Topologies.....	104
Figure 6-3	Ring Topologies.....	105
Figure 6-4	Fully Meshed Topologies .....	106
Figure 6-5	Bus Topology.....	107
Figure 6-6	ESS Network .....	111
Figure 7-1	ESS Workstation and Lockable File Server Rack .....	115
Figure 7-2	Lockable Console Bay for ESS Workstation Computer .....	116
Figure 7-3	Monitor-Keyboards-Touchpad Console.....	118
Figure 7-4	Central Monitoring Station with Separate Equipment Room .....	119
Figure 9-1	Cable Counts on Riser Diagrams .....	128
Figure 9-2	Functional Matrix .....	130
Figure 11-1	SAT Process Flowchart.....	152
Figure 11-2	Sample Test Procedure .....	155
Figure 11-3	Example Test Log .....	156

## TABLES

Table 3-1	Imaging Technology for Video Analytics (Wide Area IDS).....	51
Table 5-1	Fixed Versus PTZ Cameras.....	81
Table 5-2	Reflectivity Factors for Various Surface Conditions .....	84
Table 5-3	Characteristics of Thermal Imagers .....	87
Table 5-4	Typical Faceplate Sizes.....	90
Table 5-5	Typical Camera Resolution Specifications.....	91
Table 5-6	Object Discrimination Levels Based on Johnson Criteria .....	91
Table 5-7	Single-frame File Size for Various Resolution Values and Compression Schemes.....	95
Table 6-1	Bandwidth Usage Values .....	101
Table 6-2	Data Transmission.....	110
Table 6-3	DTM Technologies for ESS. ....	112
Table 9-1	Agency Requirements for Electronic Security Systems .....	126
Table 9-2	Sample Cable Schedule .....	129

*This Page Intentionally Left Blank*

## CHAPTER 1 INTRODUCTION

### 1-1 REISSUES AND CANCELS.

This UFC reissues and cancels UFC 4-021-02, dated 1 October 2013.

### 1-2 PURPOSE AND SCOPE.

The purpose of this UFC is to provide requirements and guidance for designing Electronic Security Systems (ESS) in support of Department of Defense (DoD) physical security program requirements. An ESS is one of many physical security measures that must be considered when addressing the physical security posture of a facility. This UFC is intended to provide uniformity and consistency in the design of an ESS.

This UFC provides design requirements and guidance for the design of ESS. It is not intended to create the requirement for an ESS, but rather to assist in designing systems that meet an established requirement and give guidance to commanders, architects, and engineers on designing an ESS. Consult with headquarters, major command, and installation physical security personnel for DoD and Service directives outlining ESS requirements for asset protection. The ESS requirement may come from DoD policy, Service policy, installation requirements, or user requirements.

### 1-3 APPLICABILITY.

In addition to the applicability of UFC 1-200-01, paragraph 1-3 APPLICABILITY, this UFC applies to all construction, renovation, or repair projects that include an ESS. This UFC provides planning and design criteria for DoD components and participating organizations.

### 1-4 PROTECTION PROGRAM RISK ASSESSMENTS.

DoD facilities are regularly assessed in accordance with the Mission Assurance Program, Antiterrorism Program, and other protection programs. Results of these assessments may include recommendations that physical security measures such as ESS be deployed to reduce risk. This UFC assumes the pre-design phases, including any required risk assessments, are complete prior to beginning design, and that risk assessment results will be used to develop project-specific ESS requirements.

### 1-5 REGULATORY OR FUNCTIONAL AUTHORITIES.

The program regulatory authorities are included below.

#### 1-5.1 Military Authorities.

The following offices have authority over their respective Service's ESS as listed below.

#### **1-5.1.1 Army.**

For integrated commercial intrusion detection systems (ICIDS), the following authority must approve the acquisition methodology, design team composition, site selection, facility requirements, DD Form 1391, concept development, and final design-build request for proposal (RFP) or final design:

- Product Manager Force Protection System (PM FPS), Ft Belvoir, VA, Phone: 703-704-2413

For commercial intrusion detection systems (IDS), any ESS installed in construction projects, and USACE restricted area ESS, the following authority must review the facility requirements, DD Form 1391, concept development, and the final design-build RFP or final design:

- U.S. Army Corps of Engineers (USACE) Electronic Security Center (ESC) Electronic Security Systems Mandatory Center of Expertise (ESS-MCX), Huntsville, AL, [AskESSMCX@usace.army.mil](mailto:AskESSMCX@usace.army.mil)

#### **1-5.1.2 Air Force.**

Consult with the following authority for IDS and ESS site selection, facility requirements, concept development, and regulatory guidance:

- Air Force Security Forces Center, JBSA-Lackland, TX, [afsfsc.ibdss@us.af.mil](mailto:afsfsc.ibdss@us.af.mil)

#### **1-5.1.3 Marine Corps.**

For all ESS, the following authority must approve the acquisition methodology, design team composition, site selection, facility requirements, DD Form 1391, concept development, and the final design-build RFP or final design:

- Marine Corps Installations Command (MCICOM) G-3, Physical Security/MCESS, Phone: 703-571-1188

#### **1-5.1.4 Navy.**

For all Navy ESS questions, e-mail the following organizational account. Questions will be forwarded to the appropriate Navy point of contact (POC):

- Navy Electronic Public Protection Office (NEPPO), Washington Navy Yard, Washington DC:
  - [CNIC\\_N3\\_IDS.fct@navy.mil](mailto:CNIC_N3_IDS.fct@navy.mil) (Non-classified Internet Protocol Router Network [NIPR]) or
  - [CNIC\\_N3\\_IDS.fct@navy.smil.mil](mailto:CNIC_N3_IDS.fct@navy.smil.mil) (Secret Internet Protocol Router Network [SIPR])

## **1-6 GENERAL BUILDING REQUIREMENTS.**

Comply with UFC 1-200-01, *DoD Building Code*. UFC 1-200-01 provides applicability of model building codes and government unique criteria for typical design disciplines and building systems, as well as for accessibility, antiterrorism, security, high performance and sustainability requirements, and safety. Use this UFC in addition to UFC 1-200-01 and the UFCs and government criteria referenced therein.

## **1-7 CYBERSECURITY.**

All facility-related control systems (including systems separate from a utility monitoring and control system) must be planned, designed, acquired, executed, and maintained in accordance with UFC 4-010-06, *Cybersecurity of Facility-Related Control Systems (FRCS)*, and as required by individual Service implementation policy. UFC 4-010-06 defines ESS as a facility-related control system.

## **1-8 SECURITY ENGINEERING UFC SERIES.**

This UFC is one of a series of security engineering UFCs that cover minimum standards, planning, preliminary design, and detailed design for security and antiterrorism. Figure 1-1 illustrates the process from initial planning to the development of facility design requirements. The manuals in this series are designed to be used sequentially by a diverse audience to facilitate project development throughout the design cycle. The manuals in this series include the following.

### **1-8.1 DoD Minimum Antiterrorism Standards for Buildings.**

UFC 4-010-01 establishes standards that provide minimum protection against terrorist attacks for the occupants of all DoD inhabited buildings. This UFC is intended to be used by security and antiterrorism personnel and design teams to identify the minimum requirements that must be incorporated into the design of all new construction and major renovations of inhabited DoD buildings. It also includes recommendations that may be, but are not required to be, incorporated into all such buildings.

### **1-8.2 DoD Security Engineering Facilities Planning Manual.**

UFC 4-020-01, *DoD Security Engineering Facilities Planning Manual*, presents processes for developing the design criteria necessary to incorporate security and antiterrorism into DoD facilities and identifying the cost implications of applying those design criteria. Those design criteria may be limited to the requirements of the minimum standards, or they may include protection of assets other than those addressed in the minimum standards (people), aggressor tactics that are not addressed in the minimum standards, or levels of protection beyond those required by the minimum standards. The cost implications for security and antiterrorism are addressed as cost increases over conventional construction for common construction types. The changes in construction shown by those cost increases are tabulated for reference, but they represent only representative construction that will meet the requirements of the design criteria. The manual also addresses the tradeoffs between cost and risk. UFC 4-020-01 is intended

to be used by planners as well as security and antiterrorism personnel, with support from planning team members.

### **1-8.3 DoD Security Engineering Facilities Design Manual.**

UFC 4-020-02FA, *Security Engineering: Concept Design*, provides interdisciplinary design guidance for developing preliminary systems of protective measures to implement the design criteria established using UFC 4-020-01. Those protective measures include building and site elements, equipment, and the supporting manpower and procedures necessary to make them all work as a system. UFC 4-020-02FA is in the process of becoming a joint document. For the purpose and implementation of this UFC, UFC 4-020-02FA applies towards all three services regardless of the “FA” suffix. UFC 4-020-02FA contains sufficient detail to support concept-level project development, and as such can provide a good basis for a more detailed design. The UFC also provides a process for assessing the impact of protective measures on risk. The primary audience for UFC 4-020-02FA is the design team, but it can also be used by security and antiterrorism personnel.

### **1-8.4 Security Engineering Support Manuals.**

In addition to the standards, planning, and design UFCs listed above, there is a series of additional UFCs that provide detailed design guidance for developing final designs based on the preliminary designs developed using UFC 4-020-02FA. These support manuals provide specialized, discipline-specific design guidance. Some address specific tactics such as direct fire weapons, vehicle-borne improvised explosive devices, or airborne contamination. Others address limited aspects of design, such as resistance to progressive collapse or design of portions of buildings such as mail rooms. Still others address details of designs for specific protective measures such as vehicle barriers or fences. The security engineering support manuals are listed in appendix E and are intended to be used by the design team during the development of final design packages.

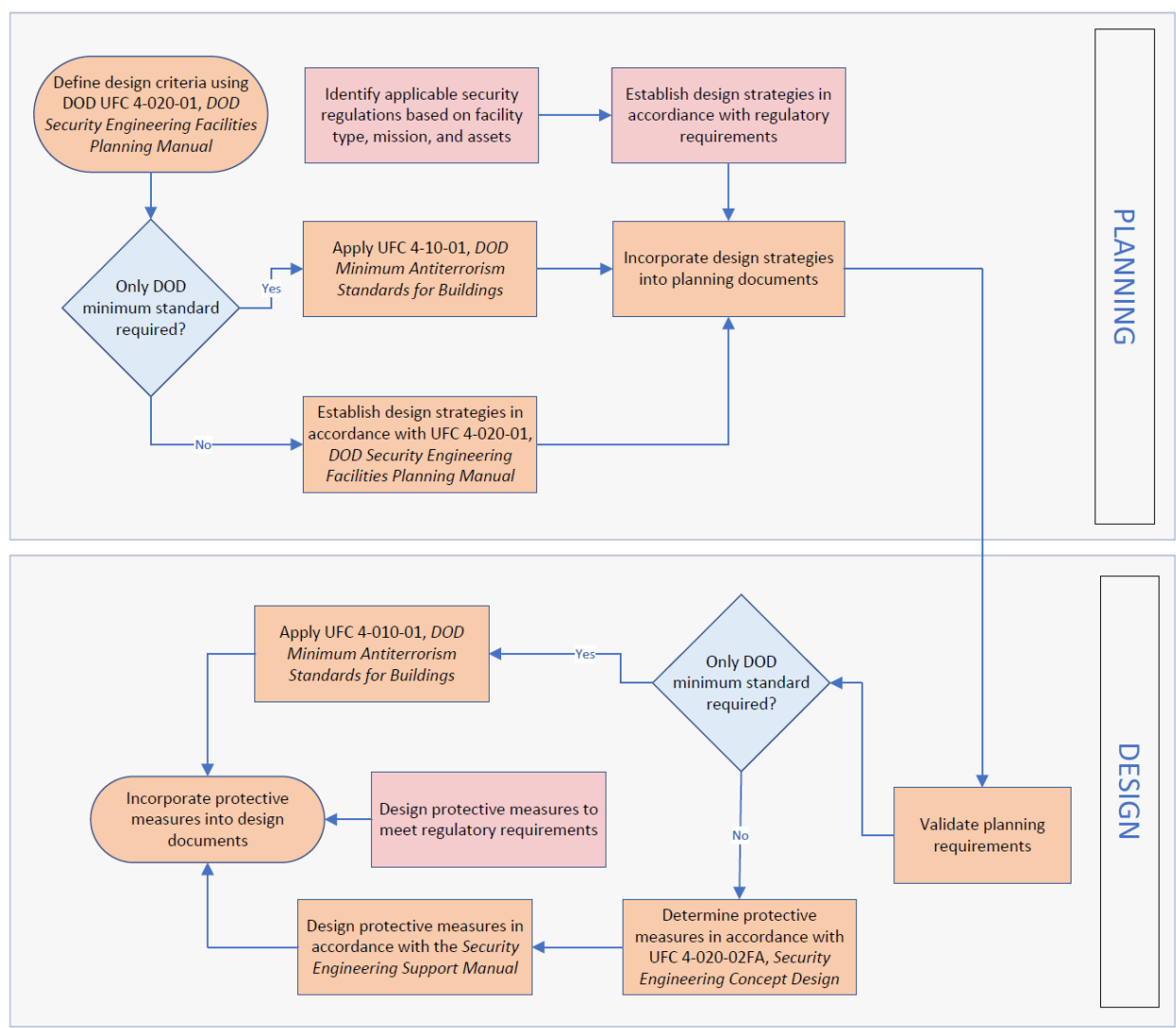
### **1-8.5 Security Engineering UFC Application.**

The application of the security engineering series of UFCs is illustrated in Figure 1-1. UFC 4-020-01 is intended to be the starting point for any project that is likely to have security or antiterrorism requirements. By beginning with UFC 4-020-01, the design criteria will be developed that establishes which of the other UFCs in the series will need to be applied. The design criteria may indicate that only the minimum standards need to be incorporated, or it may include additional requirements, resulting in the need for applying additional UFCs. Applying this series of UFCs as illustrated in Figure 1-1 will result in the most efficient use of resources for protecting assets against security- and antiterrorism-related threats.

## 1-8.6 Compliance with Security Regulations.

Security regulations specify protective measures based on the mission and assets associated with a particular facility. These protective measures may include site features, construction methods, building components, and security equipment. The security engineering series of UFCs is intended to complement security regulations, not contradict or supersede them. Regulatory requirements must be addressed as an integral part of the security engineering planning and design process, as illustrated in Figure 1-1.

**Figure 1-1 Security Engineering UFC Application**



**1-9 GLOSSARY.**

Appendix D contains acronyms, abbreviations, and terms.

**1-10 REFERENCES.**

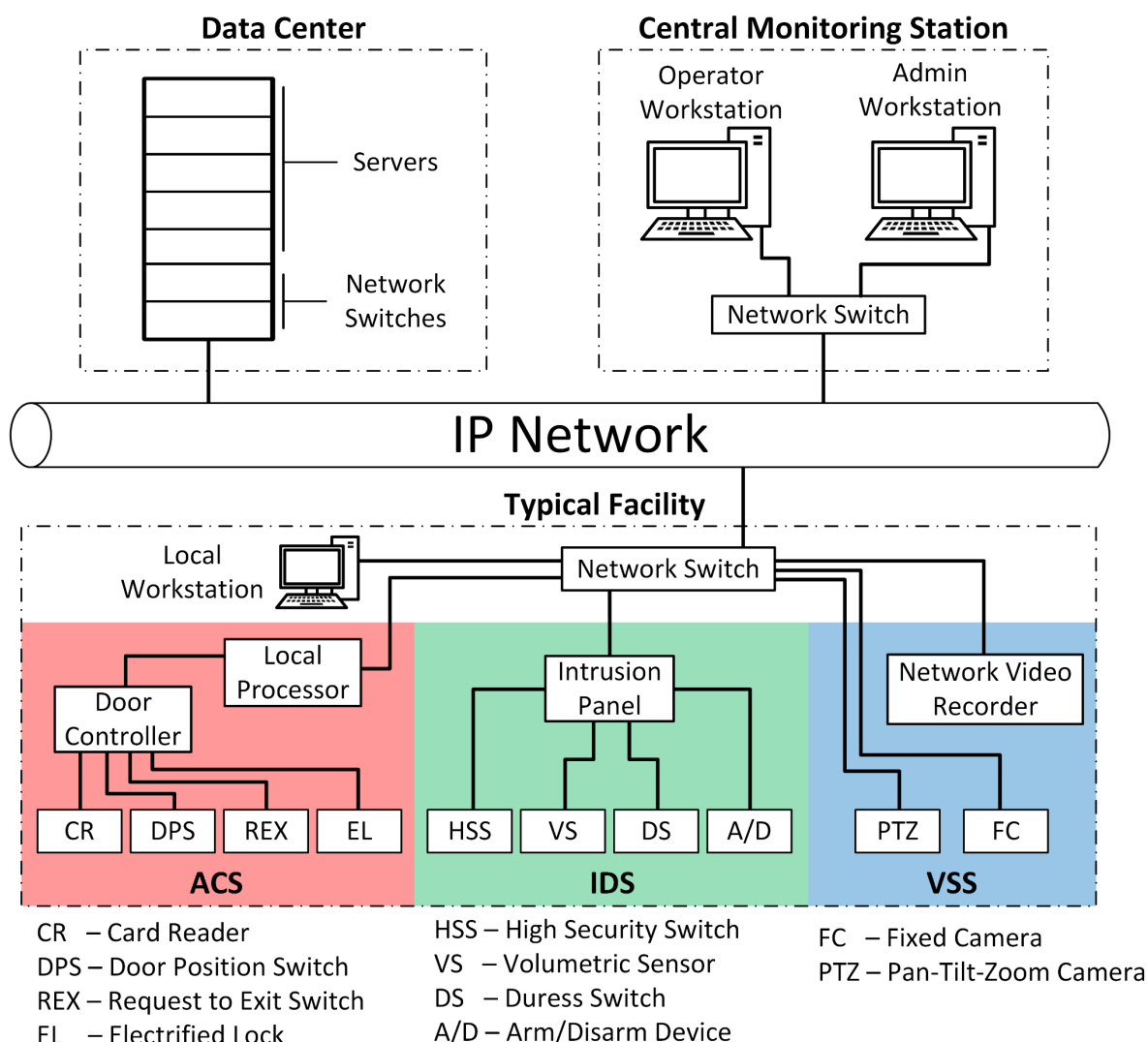
Appendix E contains a list of references used in this document. The publication date of the code or standard is not included in this document. Unless otherwise specified, the most recent edition of the referenced publication applies.

## CHAPTER 2 ELECTRONIC SECURITY SYSTEM OVERVIEW

### 2-1 SYSTEM DEFINITION.

An ESS is composed of three primary subsystems—intrusion detection system (IDS), access control system (ACS), and video surveillance system (VSS)—along with a supporting data transmission network and electrical power system. A conceptual system diagram for an integrated system is shown in Figure 2-1. Although the IDS, ACS, and VSS can be fully integrated, the type and extent of subsystem integration must be determined on a project-by-project basis, realizing that some projects may require only one or two of the three subsystems. Operational and regulatory requirements may also allow or prohibit certain integration strategies, for example, sensitive compartmented information facilities (SCIF) and special access program facilities (SAPF) require independent IDS and a Secure Room requires a separate premise control unit (PCU), but ACS for these areas may be centralized for SCIF/SAPF and Secure Room ACS may be combined with other areas with ACS. Biological Select Agents and Toxins (BSAT) at all Biosafety Levels (BSL) and registered spaces require ACS to operate on a closed computer network specifically designed and established for the ACS, DoDI 5210.88, *Security Standards for Safeguarding BSAT*. ESS components may be generally characterized as either end-point devices (sensors, keypads, card readers, and cameras), intelligent field controllers (ACS local processors, intrusion panels/PCUs), or central system equipment (file servers and workstation computers). It is important to note that an ESS is a facilities-related control system also identified as a platform information technology system (PIT). Specialized application software allows ESS users to monitor and manage system activity.

**Figure 2-1 Conceptual System Diagram for an Integrated System**



## 2-2 PHYSICAL SECURITY AND ESS.

Physical security for any asset is based on the concepts of deter, detect, delay, deny, defend, and defeat as defined in UFC 4-020-01. Although an ESS can detect attempts to gain unauthorized access to protected assets, it must be integrated with other protective measures, including barriers and locks, as well as standoff distance and security forces to ensure that adversaries are delayed and, ultimately, defeated. For certain high-value assets, physical security measures may be implemented to ensure adversaries are defeated before gaining any level of physical access. While this strategy ensures the protected asset is in no way compromised by the adversary, implementation costs may be very high due to the need for early detection, long delay, and rapid security forces response. For assets of lesser value, physical security measures will likely focus on defeating adversaries after some level of physical access

has been achieved, recognizing that the asset may be damaged or destroyed, depending on the objective and capabilities of the adversary. It is important to note that for any physical security strategy, the delay and defeat timeline does not begin until the adversary is detected, whether by ESS technology or direct human observation.

## **2-3 PROJECT CATEGORIES AND ESS DESIGN RESPONSIBILITIES.**

Projects associated with ESS can generally be categorized as either construction or equipment installation. Each of these project categories has special considerations for ESS acquisition strategy and design responsibilities.

### **2-3.1 Construction.**

This category includes both new construction and major renovation and is typically associated with the DoD Military Construction (MILCON) Program and Facilities Sustainment, Restoration, and Modernization (SRM) Program. The government may elect to procure and install the ESS through an option to the construction contract or through another specialized contract, separate from the construction contract. ESS design responsibilities for these projects are assigned to the designer of record (DOR), thus ensuring that ESS is fully coordinated with other facility design disciplines such as architecture, electrical, and telecommunications. The DOR is responsible for the complete ESS design and must clearly delineate in the design documents the responsibilities of the construction contractor and the responsibilities of the ESS contractor, such as procurement, installation, and testing of all ESS equipment and software. The design must clearly delineate the ESS supporting infrastructure (real property) from the ESS equipment (personal property). Supporting infrastructure includes items such as ESS boxes, conduit, electrical circuits, locks, and door hardware. ESS equipment includes items such as end-point devices, intelligent field controllers, and electronic security components.

### **2-3.2 Equipment Installation.**

This category addresses ESS projects that involve few, if any, facility modifications or construction. The project scope may include installing a new ESS, expanding or upgrading an existing ESS, or a complete ESS life-cycle replacement. For these projects, a single turn-key contract for ESS design, procurement, and installation is usually preferred. In this approach, the government often employs a performance-based services contract awarded to a specialized ESS contractor who assumes all ESS responsibilities, including design, procurement, installation, and testing. Another option involves the government developing an ESS concept design that serves as the scope for awarding an ESS contract. In this case, the ESS contractor is responsible for advancing the concept design to a final, detailed design and then procuring, installing, and testing the ESS.

## **2-4 PROJECT DESIGN REQUIREMENTS.**

When establishing project design requirements, the ESS designer must obtain accurate and detailed information from facility end-user representatives. In addition to basic preferences on functionality, several key factors must be addressed with the end-user early in the design process. The factors described in the following paragraphs apply to all ESS projects.

### **2-4.1 Regulatory Requirements.**

The designer must establish the ESS policy baseline for the project based on all applicable regulatory requirements. Regulations are generally associated with specific military programs and assets. For example, IDS requirements for Navy armories are stated in OPNAV Instruction 5530.13, *U.S. Navy Conventional Arms, Ammunition, and Explosives Physical Security Policy Manual*.

### **2-4.2 Risk Assessment Results.**

The designer must incorporate the results of previously conducted risk assessments into project design requirements. One example is antiterrorism risk management described in DoDI O-2000.16 V1, *DoD Antiterrorism (AT) Program Implementation*. Another example is DA PAM 190-51, *Risk Analysis for Unclassified Army Resources*.

### **2-4.3 Standard Systems.**

The need to install or integrate with standard systems can have a significant impact on project design requirements. Standardization may be at any organizational level within DoD, including an individual Service, agency, or command. A standard system may be designated as an acquisition program of record (POR) such as the Army ICIDS. Other standard systems, such as the Marine Corps Electronic Security System (MCESS), though not formally designated acquisition programs, have the essential elements of standardized equipment, software, and system configuration. Refer to Appendix E for points of contact for specific programs and approved product lists. A standard system may also have a centrally managed contract for procurement, installation, and life-cycle maintenance.

### **2-4.4 Existing Systems.**

Integrating with existing systems must be carefully considered when developing project design requirements. Whether the scale is small (existing VSS for a single building) or large (existing installation-wide ACS), the existing system will drive equipment selection, software integration, and network configuration for any ESS project that expands or otherwise modifies the existing system. For this reason, it is imperative that, early in an ESS project, the designer clearly defines requirements for connecting to existing systems in coordination with the facility/mission owner.

#### **2-4.5 Approved Components and Systems.**

Some DoD organizations maintain a list of approved electronic security components and systems that must be incorporated into project design requirements. Approval is generally based on market research and functional testing conducted by the organization to ensure listed items meet established performance standards. One example is the Air Force Life Cycle Management Center's (AFLCMC) Configuration Management Database. Applicability of any given list of approved components and systems is generally limited to ESS projects performed for the issuing organization.

#### **2-4.6 Alarm Monitoring.**

Many ESS projects, especially those that involve IDS, require that critical alarms be monitored and responded to on a continuous basis. For these projects, continuous alarm monitoring must be addressed in the design requirements. The most common approach is for each DoD installation to have one continuously staffed alarm monitoring station, such as a military police station, which serves all facilities on the installation. The Navy has consolidated alarm monitoring even further by integrating continuous alarm monitoring with regional dispatch centers (RDC). Some high-security facilities, such as nuclear weapons storage areas, have a dedicated alarm monitoring station with continuous staffing. For certain facilities, especially those not located on a DoD installation, a DoD organization may contract with a qualified alarm service company for continuous off-site alarm monitoring. Regardless of which monitoring approach is needed for a project, the ESS designer must ensure that monitoring station issues related to equipment compatibility and connectivity are addressed in the requirements.

#### **2-4.7 End-User Requests.**

In addition to the factors described above, facility end-user representatives may express a desire for ESS coverage or capability that is not directly tied to a regulatory requirement or supported by a formal risk assessment. These requests may be intended to counter a local threat or vulnerability or address site-specific operational conditions that affect security posture. Given that these requests will impact project cost, it is the responsibility of the facility end-user to verify through appropriate Service or agency approval channels that the desired ESS project features are appropriate, and that funding will be allocated for initial installation and life-cycle maintenance.

#### **2-4.8 Security-in-Depth**

Apply security-in-depth strategies throughout the design phase. Security-in-Depth is defined by DoDM 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*:

*A determination by the senior agency official that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences,*

*employee and visitor access controls, use of an IDS, random guard patrols throughout the facility during non-working hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of open storage areas without alarms and security containers during non-working hours.*

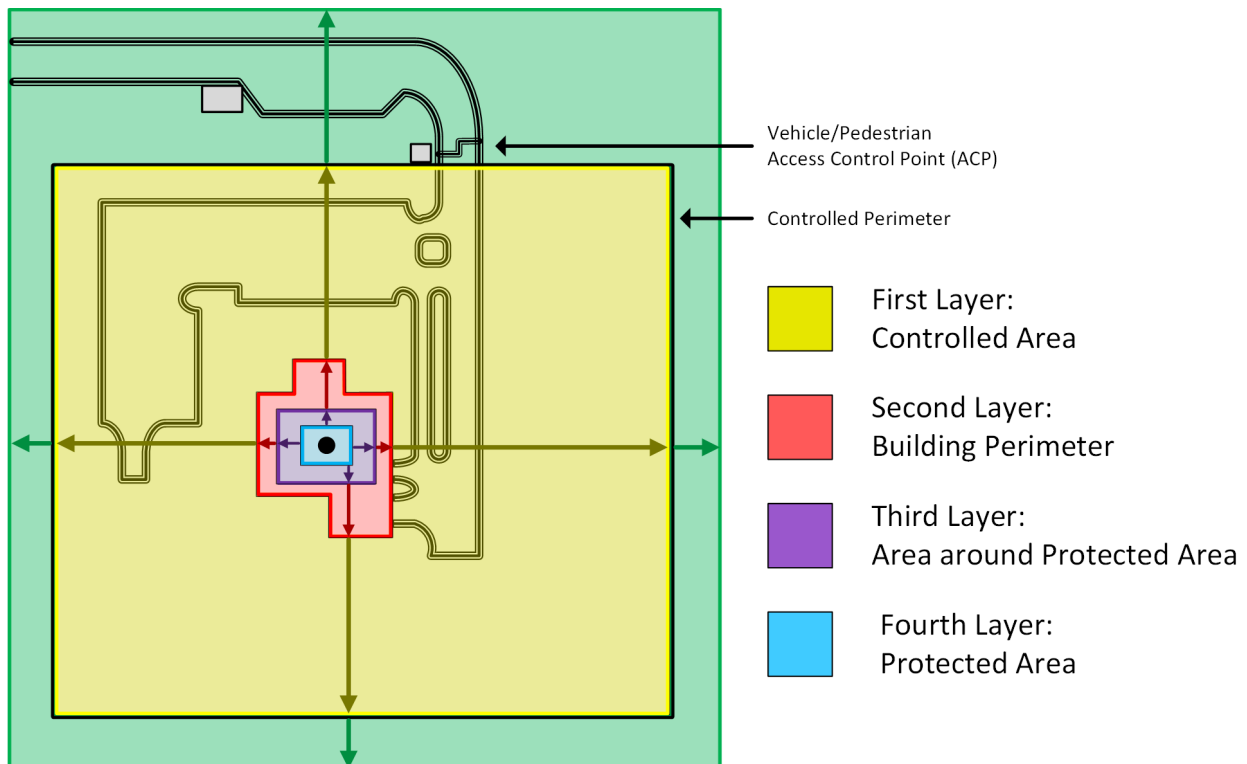
A key tool used in the determination of security-in-depth is the risk assessment. A risk assessment must be performed to facilitate a security-in-depth determination and aid identification and selection of supplemental controls that may need to be implemented. The analysis will, at a minimum, consider the following: local threats, both known and anticipated, and vulnerabilities; the existing security environment and controls; the ease of access to containers or other areas where classified data are stored; the criticality, sensitivity, and value of the information stored; and cost versus benefit of potential countermeasures. The risk assessment must be used to determine whether installation of an IDS is warranted or whether other supplemental controls are sufficient. See Figure 2-2.

Coordinate security-in-depth design with the security officials of the organization to determine security features already existing and in use and the risk assessment determination. For example, is the space located on a controlled-access military installation? Are there adequate security patrols and are they doing building checks after hours? Is the space located in a controlled compound? Is the space located in an access-controlled building and at what level is the area surrounding the space controlled? Is the building secured by IDS after hours or does it have dedicated security patrols of the structure? Typical design strategies are as follows:

- Follow the applicable Service and DoD regulatory requirements for coverage.
- If the cognizant security authority has made a written determination of security-in-depth, then work with the organization security official on a design that takes this into account.
- It may be possible to use motion detection to protect the path to the protected material rather than in every space that can store the material.
- Security-in-depth with authorizing official's concurrence may remove the requirement to cover all perimeter walls of a SCIF, depending on its placement in the building and at what level the surrounding area is controlled.
- Take into consideration the placement of the device. If there is a requirement for motion coverage of all doorways into a space along with a requirement to cover the perimeter walls, it may be possible to use one motion detector by adjusting the placement to cover both requirements instead of placing two motion detectors for each space.
- Also consider the furnishing of the space. If there is a requirement to cover the perimeter walls of a space and 4-foot-tall (1.2 meters) cubicles are

installed along that wall, you may be able to cover that space with one motion detector. However, if the cubicle walls are 7-feet-tall (2.1 meters), motion detectors will be needed to cover the same area. By placing the motion detector over the dividing wall of the cubicle, multiple spaces can be covered with one device.

**Figure 2-2 Security-in-Depth**



## **2-5 PROJECT PHASES.**

An ESS project, whether involving new construction, major renovation, or equipment installation, will typically progress through six phases, as described in the following paragraphs.

### **2-5.1 Planning.**

Activities performed during the planning phase will vary, depending on the project category. For MILCON and SRM projects, it is important to include basic ESS requirements and estimated ESS costs on the DD Form 1391. For projects involving existing facilities, an ESS site survey is usually needed to determine project scope and prepare a budgetary cost estimate. To assist with cost estimating, an ESS budget estimator spreadsheet is available at <https://www.wbdg.org/dod/ufc/ufc-4-021-02> under Related Materials. Defining ESS acquisition strategy and funding source(s) are essential elements of the planning phase as these decisions will affect all subsequent project phases. Acquisition and funding sources for ESS systems and components will

vary by Service and by system component. ESS design responsibilities and funding responsibilities should be clearly established by the end of the planning phase.

### **2-5.2 Design.**

The design phase of an ESS project may involve contributions from an in-house government design team, contracted architect-engineer services, or a specialized ESS contractor. For MILCON and SRM projects, the DOR must deliver a complete ESS design that is fully incorporated into the overall facility design. For projects not involving significant construction activities, ESS design services are often included with procurement and installation services in a single, turn-key ESS contract. Equipment installation projects typically require a detailed ESS site survey during the design phase.

### **2-5.3 Procurement and Installation.**

A specialized ESS contractor, working either as a prime contractor for the government or as a subcontractor for a facilities construction contractor, may perform procurement and installation services for ESS projects. A designated government representative is typically responsible for on-site coordination and quality verification of installation work. The DOR may be retained on MILCON and SRM projects to provide construction surveillance and inspection services during this phase.

### **2-5.4 Testing and Training.**

Acceptance testing of the installed system is most frequently conducted by the ESS contractor and witnessed by a designated government representative. In some cases, the government will perform the testing without assistance from the ESS contractor. Functional testing and burn-in testing are required to demonstrate satisfactory system performance. During this project phase, the ESS contractor also provides training to end-user personnel on the proper operation, administration, and maintenance of the installed system. See Chapter 11 for complete acceptance testing, training, and documentation requirements.

### **2-5.5 Final System Documentation.**

The ESS contractor is responsible for delivering the final system acceptance test (SAT) report, as-built drawings, and operation and maintenance manuals to the Government. This documentation is essential for the long-term maintainability of the installed system.

### **2-5.6 Maintenance and Sustainment.**

Maintenance should be performed by a manufacturer-certified technician to avoid voiding any warranty provided from the installer or the manufacturer. The applicable Service may provide or require use of a centralized maintenance and sustainment contract for ESS. The scope of the centralized contract could impact how the ESS is designed and must be evaluated during the ESS planning and design phase. Sustainment includes cybersecurity requirements like applying software and firmware updates, patches, and security scans. Avoid designing and building large and complex

systems that have high sustainment costs and may fall into disrepair quickly if sustainment funding is not available. Design systems to meet the regulatory requirements for the protection of the assets and kept as simple as possible.

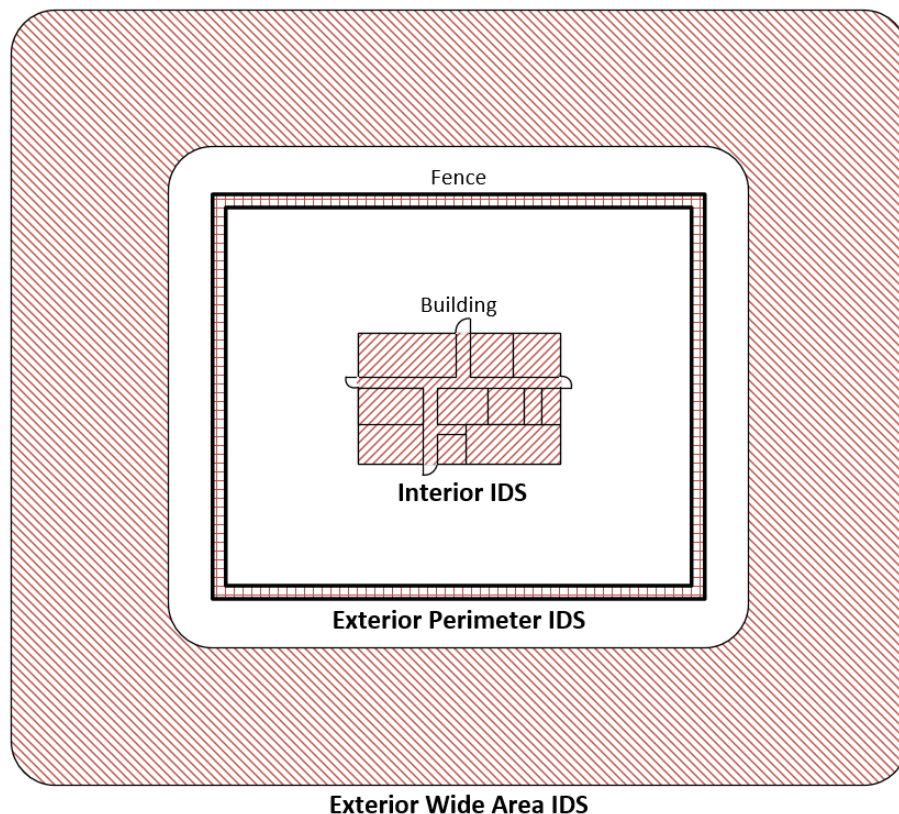
*This Page Intentionally Left Blank*

## CHAPTER 3 INTRUSION DETECTION SYSTEM

### 3-1 TECHNOLOGY OVERVIEW.

In its simplest form, an IDS consists of sensors connected via intrusion panels and a network to a central system consisting of a file server and an alarm monitoring workstation. IDS technology can be broken into three categories—interior, exterior perimeter, and exterior wide area—based largely on the specialized sensors associated with each category. Figure 3-1 illustrates these three IDS categories. IDS performance metrics are probability of detection, nuisance alarm rate (NAR), false alarm rate (FAR), and vulnerability to defeat.

**Figure 3-1 IDS Technology Categories**



### 3-2 INTERIOR INTRUSION DETECTION.

Interior intrusion detection is focused on protecting assets located in well-defined interior spaces. These spaces are typically referred to as zones or alarmed areas as described in paragraph 3-5.3. Typical design strategies are as follows.

- Identify specific regulatory requirements for the space.
- Identify the security perimeter of the space.

- Secure the perimeter of the space, man doors, rollup doors, emergency exit doors, roof hatches, and operable windows with point sensors. Regulatory guidance and approving cognitive authority may require additional sensors for protecting floors, ceilings, walls, and glass surfaces.
- Provide volumetric protection of doors, windows, any man-passable spaces, and coverage of specific assets housed in the zone (point detection).

See Appendix A for application of these design strategies based on the asset being protected and regulatory guidance. The following paragraphs describe commonly used sensors (high security switch (HSS), passive infrared [PIR], dual technology, beam-break, scanning laser, vibration, and glass-break) and provide design guidance for each. Duress switches, local annunciators, arm/disarm devices, and intrusion panels are also addressed in the following paragraphs.

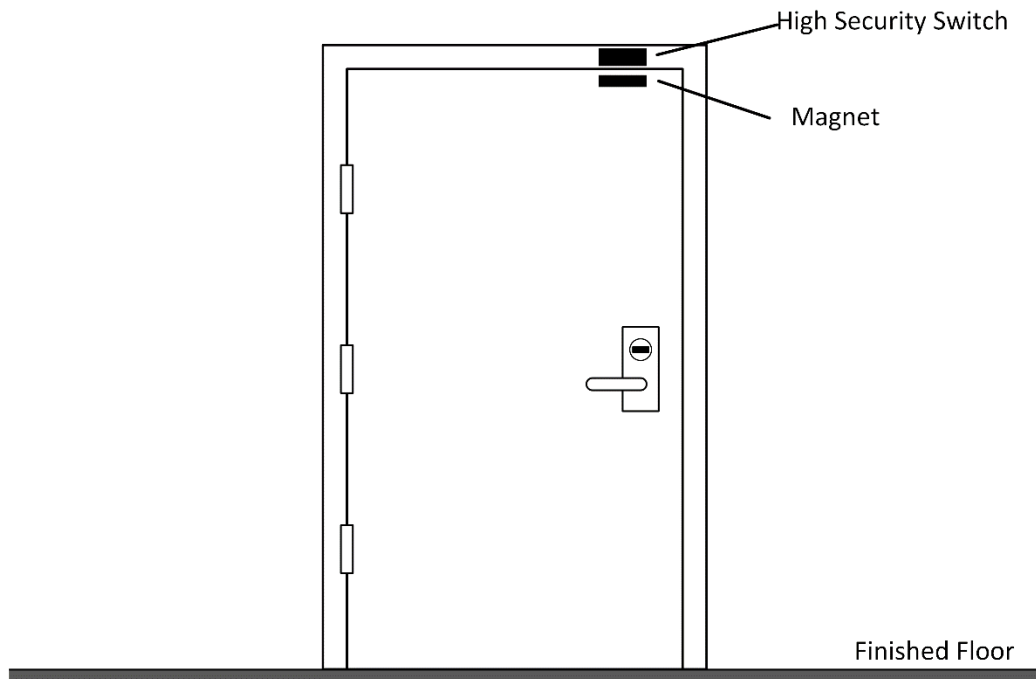
### **3-2.1 High Security Switch.**

An HSS is a sensor used to detect opening of doors, hatches, and operable windows. A typical configuration, as illustrated in Figure 3-2, involves installing the HSS on the frame and the associated magnet on the secure side of the door. As the door opens, the HSS and the magnet are no longer aligned, resulting in the switch changing from the “secure” state to the “alarm” state. This sensor is available in both surface-mount and recessed/concealed models. Design guidance is as follows:

- UL 634 Level 2 HSS are required for SCIFs and SAPFs. UL 634 Level 2 HSS meet additional requirements for performance, tampering, nuisance alarms, and reliability.
- Use UL 634 Level 1 or Level 2 HSS for non-SCIF/SAPF zones.
- Recessed/concealed models are preferred over surface-mount models, especially for new construction and major renovation projects.
- Install surface-mount models on the secure side of the opening.
- Overhead doors generally require special mounting brackets and give consideration to adding a switch on each side of the door.
- Doors must be properly aligned and seated prior to sensor installation.
- For double-leaf doors, ensure each door leaf has a sensor. Independent annunciation of each sensor is recommended.
- Select a sensor with two independent alarm contacts (double pole double throw [DPDT]) if the same sensor will be used by the IDS and ACS system.
- Ensure that both the alarm circuit and the tamper circuit (magnet tamper and pry tamper) are connected to the intrusion panel and programmed in

the IDS. Place the tamper circuit in continually monitored mode not in access mode.

**Figure 3-2 Typical HSS Secure Side Door Configuration**



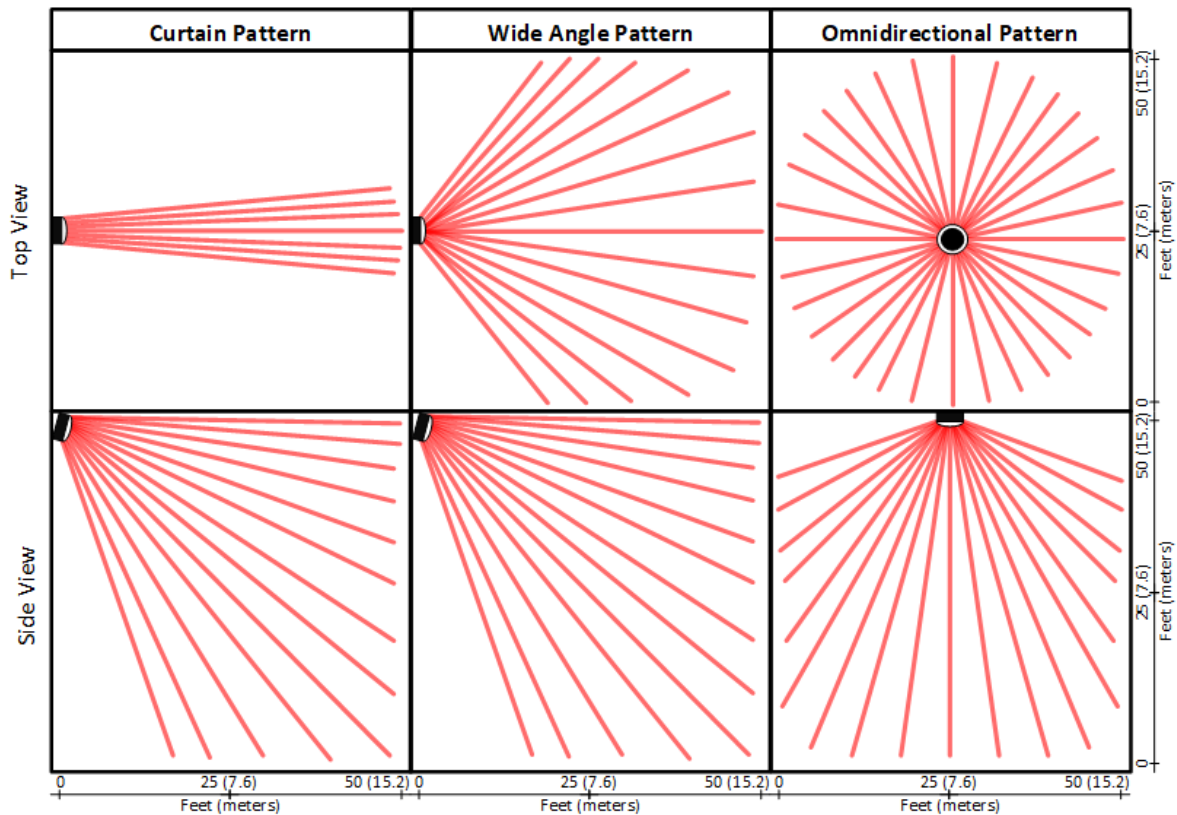
### 3-2.2 Volumetric Sensor.

A volumetric sensor, also known as a motion sensor, detects objects moving within a defined volumetric coverage pattern. Common patterns are curtain (narrow), wide angle (90 degrees), and omnidirectional (360 degrees) as illustrated in Figure 3-3. Basic technology options are PIR and microwave, with PIR being the most widely used. PIR detection is based on infrared (IR) energy (heat) changes within the coverage pattern, while microwave detection is based on a moving object shifting the frequency of the microwave energy. Some models, commonly called dual technology sensors, combine PIR and microwave sensors in a single unit. A wide range of PIR and dual technology models are offered, but commercial availability of “microwave only” models is very limited. Most dual technology models are factory set in the “and” logic configuration, meaning that both PIR and microwave detection are required simultaneously before the sensor goes into an alarm state. The benefit of “and” logic is the potential to reduce the NAR. The logic configuration of a few dual technology models can be field selectable for “and” or “or” operation, with the “or” configuration providing the potential for higher probability of detection. Design guidance is as follows:

- Ensure complete coverage at likely points of entry such as doors, windows, and hatches. A reasonable goal for sensor coverage is to detect an intruder within four steps of entering the secure space.

- Provide sufficient coverage to detect an intruder before they reach the protected asset.
- Consider coverage pattern obstructions caused by walls, furniture, and equipment when developing a sensor placement plan.
- If dual technology sensors are used in certain high-security areas such as SCIFs, the “or” logic configuration must be used. (Check applicable security policy for clarification.)
- A PIR sensor is most sensitive to motion perpendicular to its aim point direction.
- A microwave sensor is most sensitive to motion directly toward and away from the sensor.
- A microwave sensor, used by itself, can penetrate through walls and is susceptible to nuisance alarms by movement outside of the protected area.
- Microwave sensors are prone to nuisance alarms by moving objects (fan blades and small animals).
- PIR sensors are prone to nuisance alarms caused by heat sources (space heaters and windows).
- For non-environmentally controlled spaces such as warehouses, the probability of detection of PIR sensors may be reduced as the ambient temperature approaches the temperature of the human body.
- Volumetric sensors are often used as compulsory measures to cover areas where walls or ceilings do not meet structural requirements of security policy.

**Figure 3-3 Volumetric Sensor Coverage Patterns**

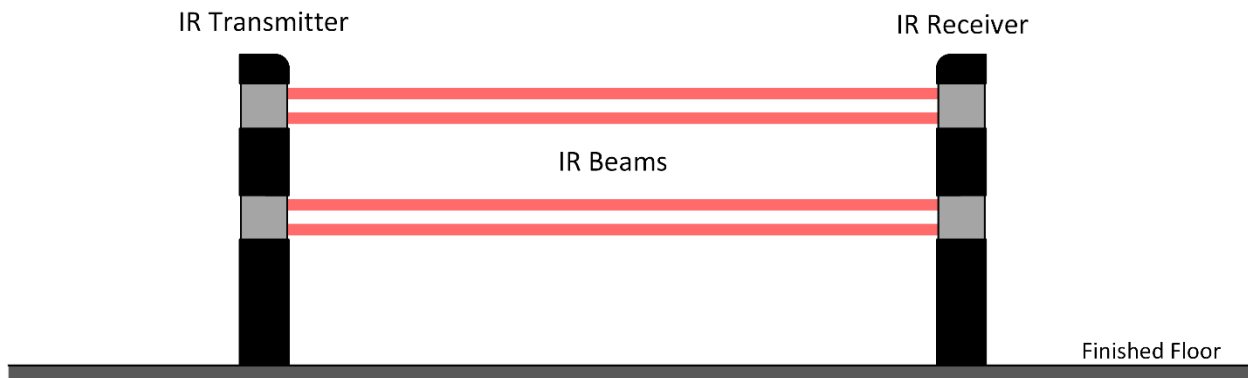


### 3-2.3 Beam-Break Sensor.

A beam-break sensor detects objects moving through one or more IR beams. These narrow beams are created by a transmitter and receiver separated some distance apart, as illustrated in Figure 3-4. Design guidance is as follows:

- Beams can be used on the perimeter of the secure space to detect intrusion through walls, windows, and doors.
- Beams can be used for perimeter intrusion detection around an individual asset such as an aircraft inside a hangar.
- A detection range of 200 feet (61 meters) for a single transmitter/receiver pair is possible with most sensor models. Some models have a range in excess of 1,000 feet (305 meters).
- Stable mounting and precise alignment are required for transmitter and receiver units.
- The space between transmitter/receiver pairs must be free of obstructions.

**Figure 3-4 Beam-Break Sensor Transmitter and Receiver**

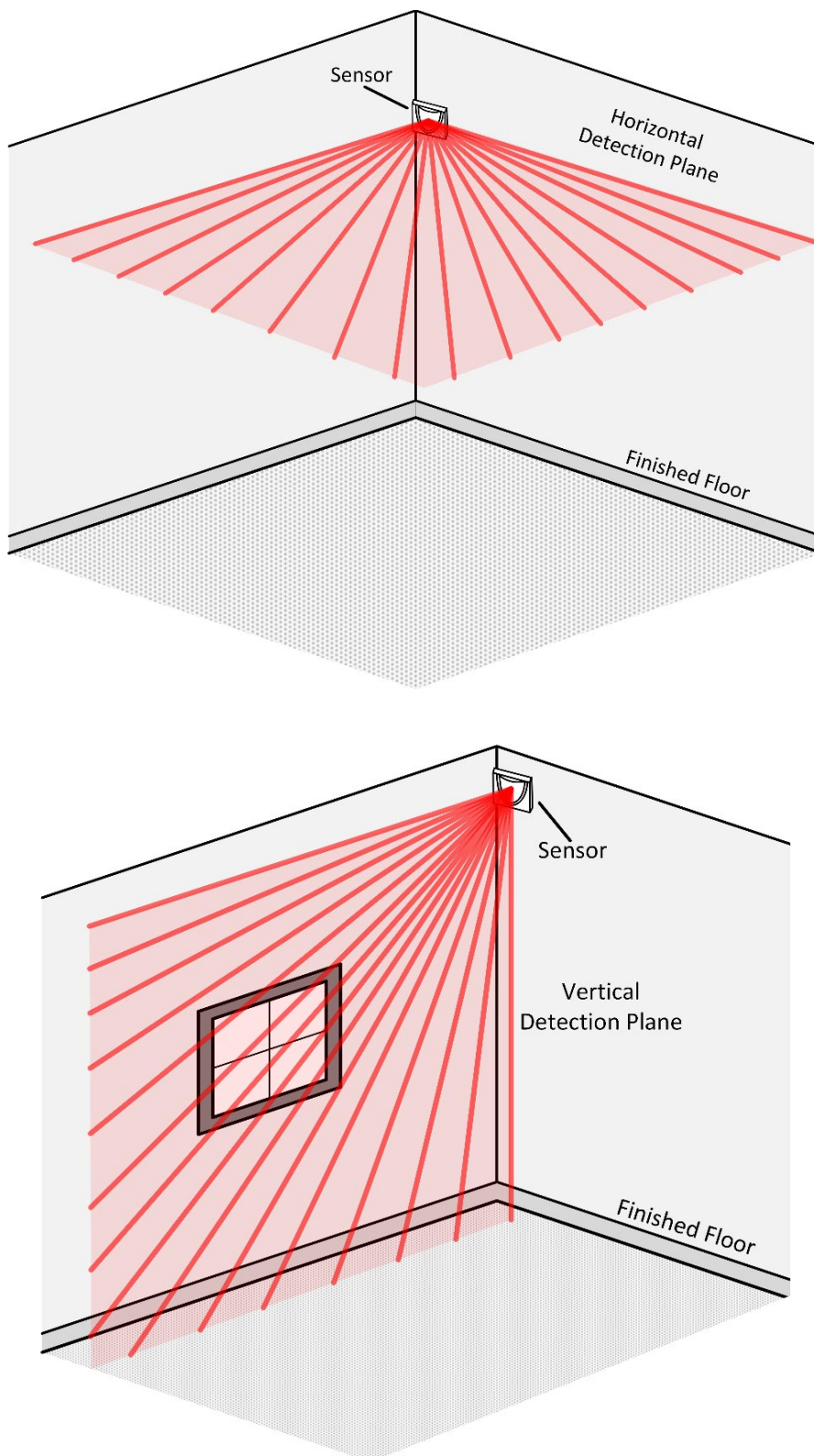


### **3-2.4 Scanning Laser Sensor.**

A scanning laser sensor detects objects moving through a planar coverage pattern created by a pulsed laser beam. Using time-of-flight analysis, the sensor is able to correlate changes in reflected energy with objects moving in or through its coverage plane. The sensor coverage pattern is illustrated in Figure 3-5. Design guidance is as follows:

- The sensor can be used to create a vertical (wall) or horizontal (ceiling) plane of detection.
- Provide a detection plane free of obstructions such as furniture and equipment.
- Maximum detection range is typically 165 feet (50.3 meters).

**Figure 3-5 Scanning Laser Sensor Coverage Pattern**

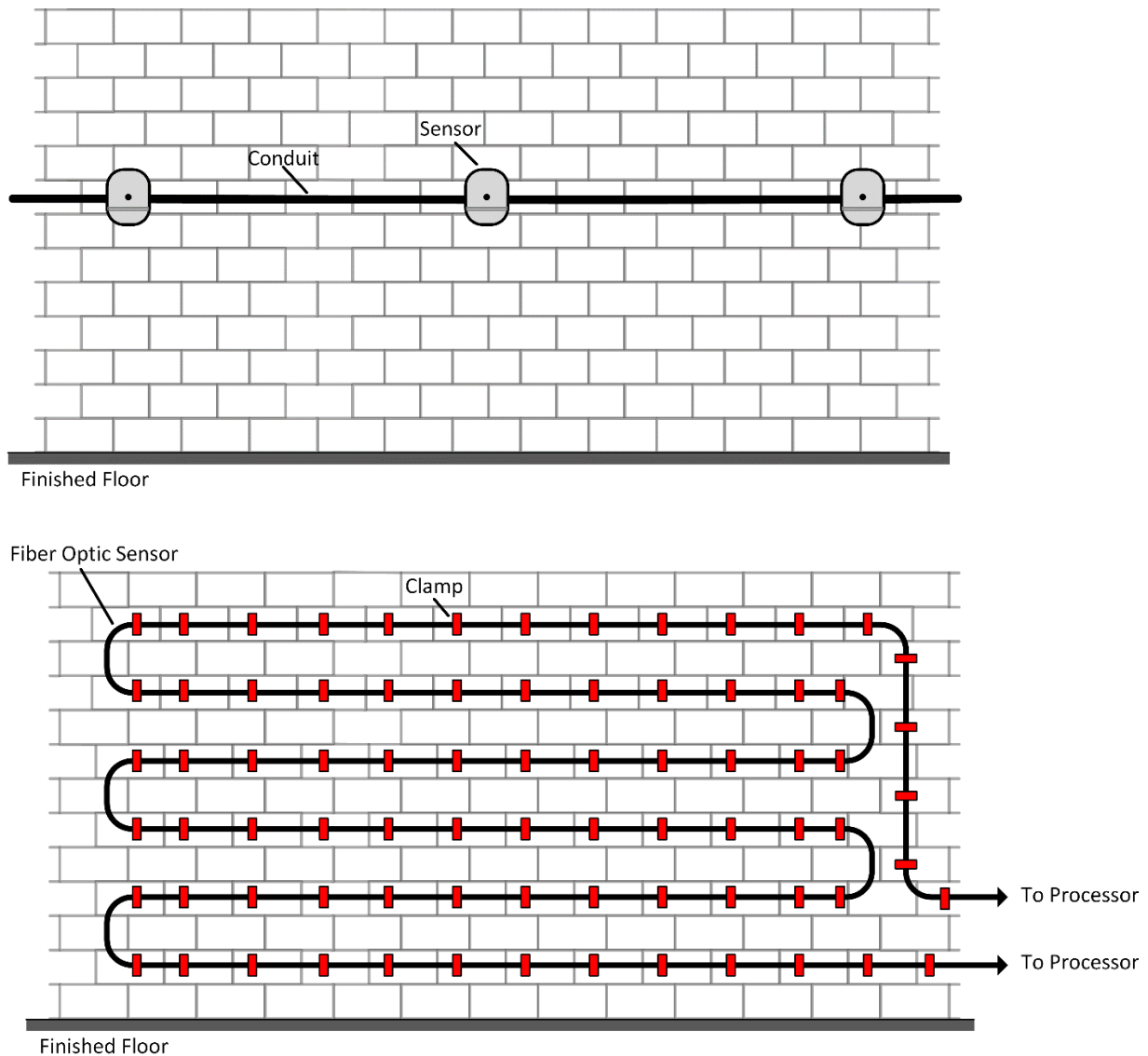


### 3-2.5 Vibration Sensor.

A vibration sensor detects breaching activities directed at a rigid barrier such as a concrete wall or modular steel vault. Two technology options are available for this purpose: seismic detectors and fiber optic sensors (see Figure 3-6). Seismic detectors are the preferred option for most rigid barrier applications due to their simple design, ease of installation, and low cost. Fiber optic sensors are adaptable to a variety of coverage patterns and can be calibrated to function in a range of operational environments. Design guidance is as follows:

- Place sensors to ensure adequate coverage of the barrier surface. Space seismic detectors at approximately 12 to 24 feet (3.7 to 7.3 meters), depending on barrier construction. Space parallel fiber optic sensor cable runs at approximately 2 feet (0.6 meter).
- Proper sensor-to-barrier attachment is essential for the transfer of energy from breaching activity through the barrier to the sensor.
- Less rigid materials such as plywood and drywall are not well suited for the use of vibration sensors.
- Consider the potential for nuisance alarms from nearby industrial machinery, railroad tracks, and high-explosive ranges and test areas before specifying vibration sensors for a facility.
- Fiber optic sensors can be used to meet information security requirements for an alarmed protective distribution system (PDS), also known as an alarmed carrier. In this specialized application, physical tampering with a conduit system is detected by fiber optic sensor cables installed inside the conduit. Refer to CNSSI No. 7003, *Protected Distribution Systems*, for additional information.

Figure 3-6 Vibration Sensors



**Note:** Sensor area of coverage and configuration is product specific and will be documented in the manufacturer's installation instructions.

### 3-2.6 Glass-Break Sensor.

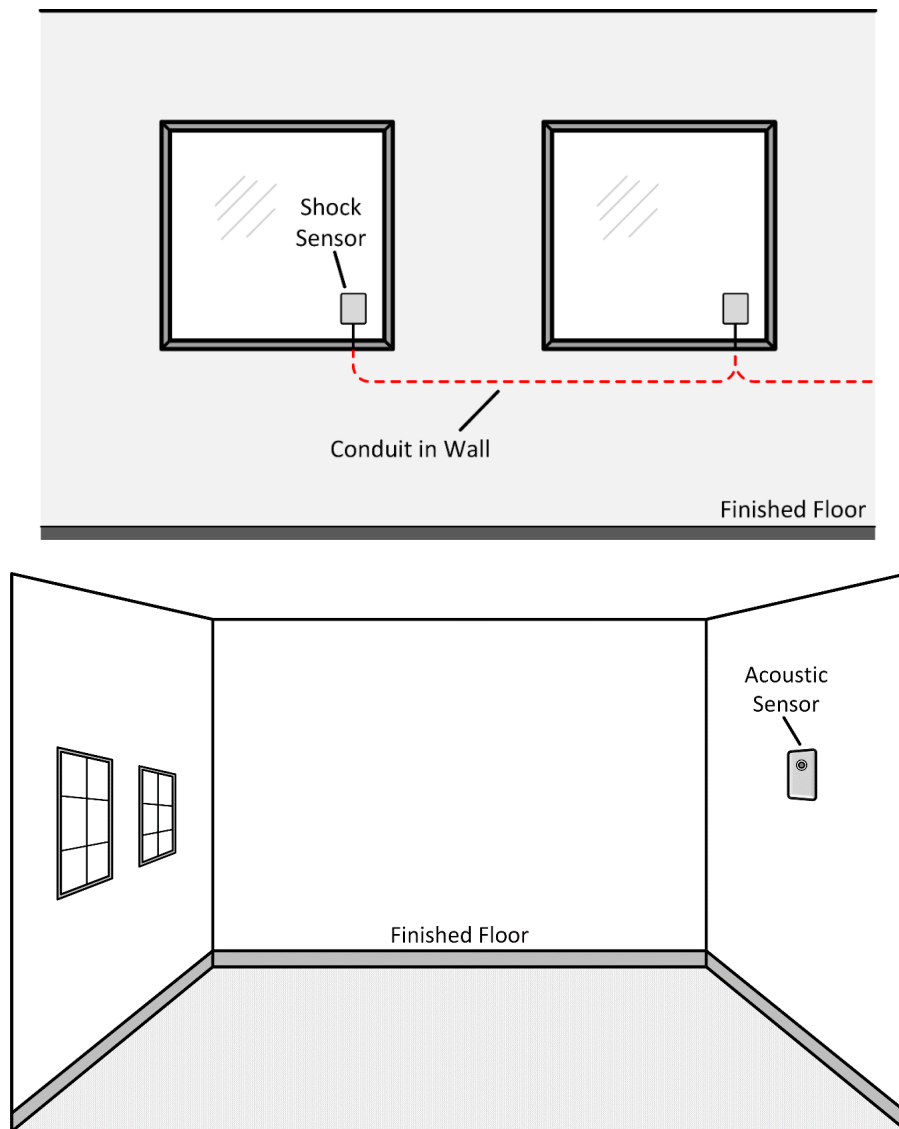
Two basic technology options are available for detecting breaking glass: shock sensors and acoustic sensors. Shock sensors are mounted directly to the glass using a specialized adhesive. Acoustic sensors are mounted on a wall or ceiling near the glass. Shock sensors detect the movement of breaking glass while acoustic sensors respond to the sound of breaking glass. Typical sensor installation is illustrated in Figure 3-7.

**Army and Navy Only:** Design guidance is as follows:

- Select a sensor that is rated for the type, thickness, and surface area of glass to be protected. In general, any sensor will perform well for plate glass and tempered glass up to 0.25-inch (6.3 millimeters) thickness. Additional consideration must be given for laminated glass and glass with anti-shatter film.
- Maximum detection area for a single shock sensor is 150 square feet (15 square meters). This is for a single continuous pane of plate glass up to 0.25-inch (6.3 millimeters) thickness. Detection area can be significantly less, depending on glass type and thickness.
- An acoustic sensor can cover multiple windows within a maximum effective range of 25 feet (7.6 meters).
- Curtains and other sound-attenuating objects will reduce the detection range of acoustic sensors.
- Acoustic sensors are not recommended for noisy environments due to the potential for nuisance alarms.

**Note:** Glass break sensors are not in the Air Force-approved Configuration Management Database and therefore not approved for Air Force use.

**Figure 3-7 Glass-Break Sensors**



### **3-2.7 Duress Switch.**

A duress switch consists of a switch and activation button installed in a protective housing. Some duress switches have a recessed button, as shown in Figure 3-8, to reduce the potential for false activations. Others have two buttons which must be pressed simultaneously to generate an alarm. Both latching and momentary operation switches are available, and latching switches require a special reset tool. A duress switch is designed for silent activation and is usually placed in a covert location accessible only to the intended user. Proper placement of a duress switch is critical and must be closely coordinated with end-user representatives. Common placement options are under a desk or service counter.

**Figure 3-8 Duress Switch with Recessed Activation Button**



### **3-2.8 Local Annunciator.**

A variety of sirens are available for local annunciation of IDS alarms. Indoor and outdoor models are available and decibel ratings range from 100 to 120 dB. Some models include an integrated strobe for visual annunciation. A local annunciator is not an alternative to annunciation of IDS alarms at a continuously staffed monitoring station nor is it generally required by security regulations. End-user representatives will provide the intended purpose and justification for the local annunciator as this will influence device placement and decibel rating.

### **3-2.9 Arm/Disarm Device with Zone Status Indicator.**

Several devices are available to enable local control of an IDS zone by an authorized user. Basic functionality includes arming and disarming the zone and viewing zone status, with some devices also providing access to advanced zone configuration settings and diagnostics. Device sophistication ranges from an intelligent graphic touchscreen at the high end to a basic numeric keypad with status LEDs at the low end. Figure 3-9 illustrates the difference between a touchscreen device and a basic keypad. User authentication is generally provided by a personal identification number (PIN) and keypad. For higher assurance, an integrated keypad and card reader can be used to achieve two-factor (card plus PIN) user authentication. Proper placement of the arm/disarm device is critical. Most applications require the device to be installed inside the zone, as required by many, but not all, security regulations. There may be operational conditions that dictate that the arm/disarm device be installed outside the zone; coordinate these exceptions with the end-user. Second, the device is typically

installed on the zone boundary in close proximity to the primary entry/exit door. Wall mounting at a height of 4 feet (1.2 meters) will provide accessibility to all occupants in compliance with Architectural Barriers Act (ABA) standards.

**Figure 3-9 Arm/Disarm Devices**



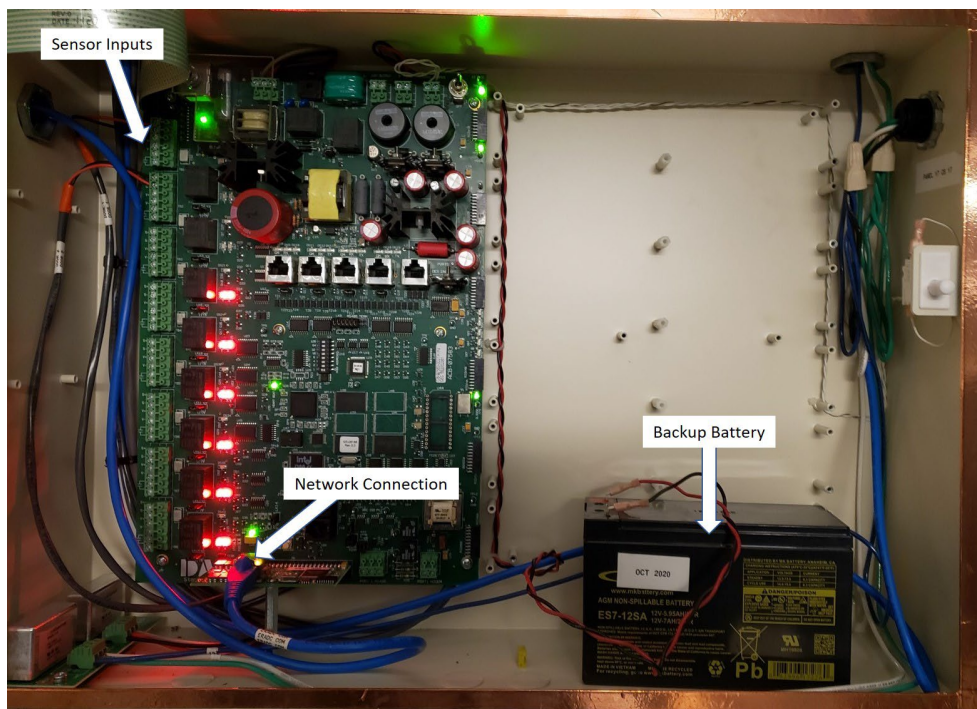
### 3-2.10 Intrusion Panel.

An intrusion panel controls all sensors within a zone and provides connectivity to an IDS network for transmitting alarm signals. Most panels have at least eight sensor inputs, with the ability to add expansion modules to accommodate additional sensors. Most panels also have at least two dry contact outputs to initiate sirens or other output devices. Figure 3-10 illustrates the basic features of an intrusion panel. Note that an intrusion panel is referred to as a PCU in certain security regulations. Design guidance is as follows:

- The panel must be installed inside the zone in a location where the panel will be protected yet still accessible for maintenance purposes.
- The panel, along with associated power supplies and batteries, must be installed in a lockable enclosure with tamper protection.
- Encryption for the transmission of alarm messages must meet requirements set forth in applicable security regulations. Options are native encryption on the panel or a separate encryption module.
- Provide capability for modular ESS expansion of inputs, outputs, card readers, and remote-control stations with minimal equipment modification. Software must be able to handle design requirements plus 25% spare capacity. Growth capacity is not to be limited by the provided products.

- SCIFs, SAPFs, and open storage locations require a visual indicator at the local field control panel that primary power was lost and backup electrical power source is in use.
- Intrusion panels may only control a single zone or have the ability to logically separate arm/disarm functions into two or more unique zones with a single panel. The ESS designer must validate the manufacturer's intrusion panel capabilities. Some protected areas or facilities such as SCIFs, SAPFs and secure rooms (Secret and Top Secret open storage) may require a physical and logically separate intrusion panel from other assets.

**Figure 3-10 Intrusion Panel**

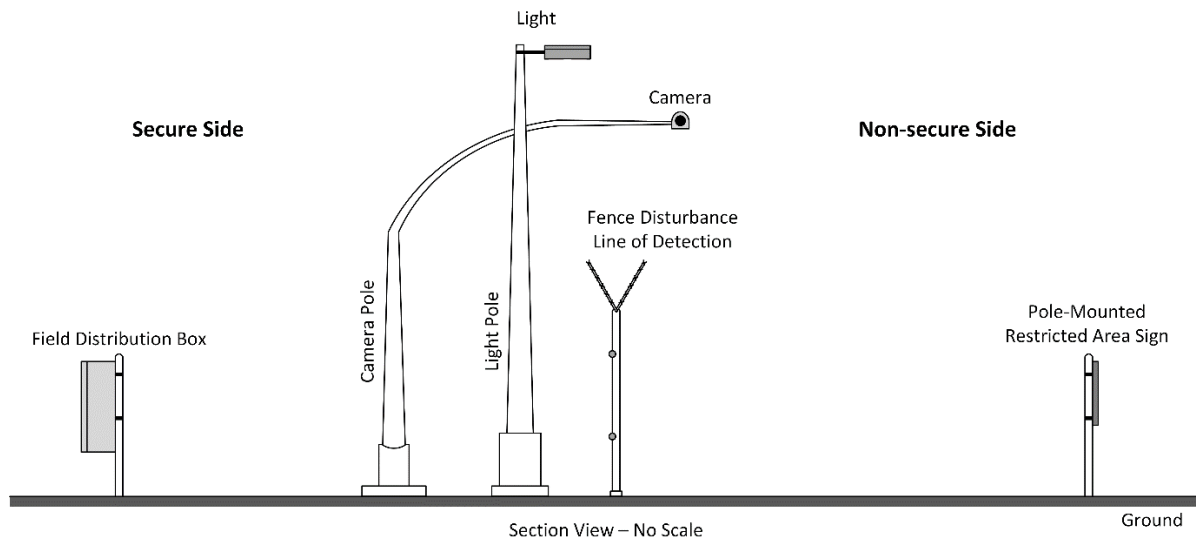


### **3-3 EXTERIOR PERIMETER INTRUSION DETECTION.**

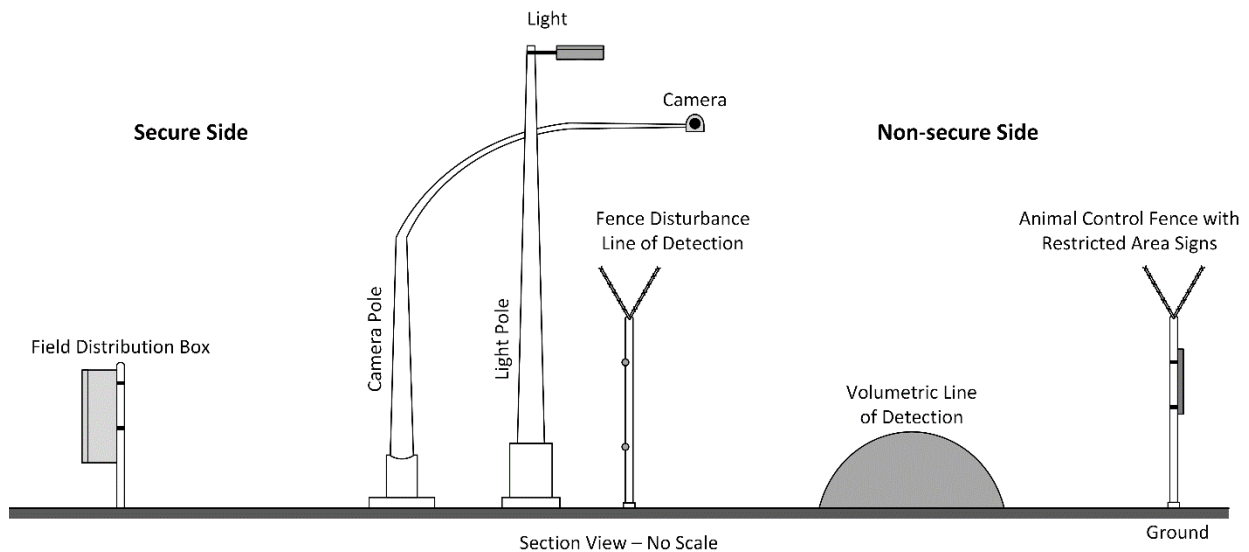
Specialized sensors may be installed outdoors to create a continuous line of intrusion detection along the perimeter of an area containing high-security assets. Exterior perimeter sensors are only required for the protection of specific assets as defined in regulatory requirements but may be considered for security-in-depth, mitigating risk in construction deficiencies, or other special circumstances. This line of detection is typically incorporated with other perimeter security features, such as fences, entry control facilities, restricted area signs, clear zones, lighting, and cameras. Examples of single and dual lines of detection are illustrated in Figures 3-11 and 3-12, respectively. The perimeter is divided into discrete zones (also referred to as sectors) for annunciation of intrusion alarms. Some sensors provide narrow, vertical coverage along the perimeter while other sensors provide a volumetric detection field. Sensors are able

to reliably detect common intrusion modes such as walking, running, crawling, climbing fences, and cutting fences. Field distribution boxes are installed along the perimeter to facilitate signal processing, electrical power, and network communications. Terrain, weather, and wildlife will affect sensor performance, and these factors must be addressed throughout the design and installation process. Basic principles of operation and design guidance for exterior intrusion detection sensors and field distribution boxes are presented in the following paragraphs.

**Figure 3-11 Single Line of Detection**



**Figure 3-12 Dual Lines of Detection**

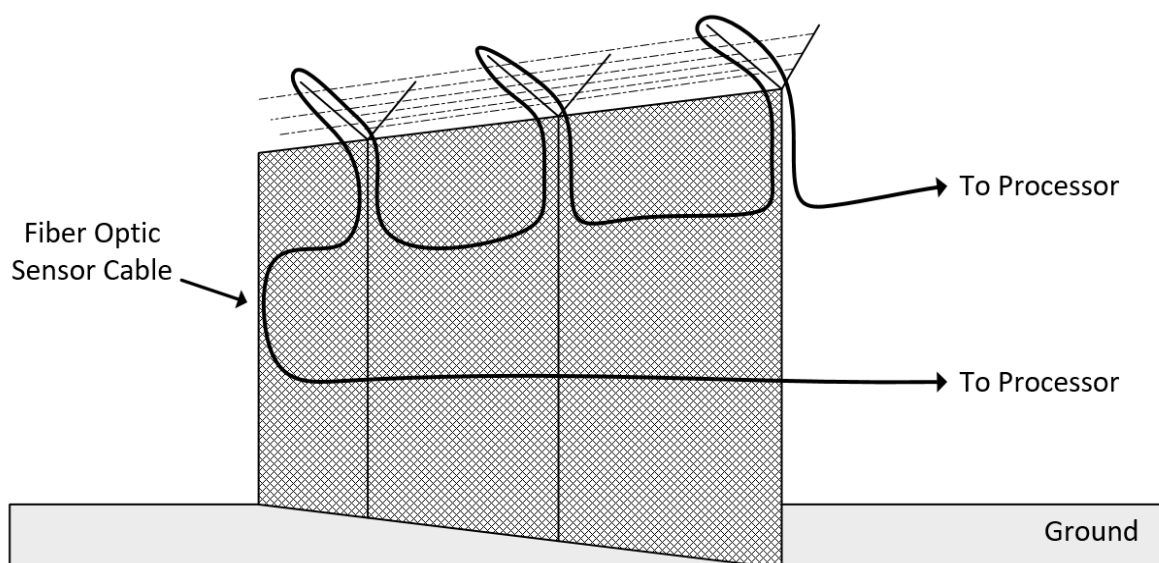


### 3-3.1 Fence-Disturbance Sensor.

A fence-disturbance sensor detects vibrations resulting from an intruder cutting, climbing, or lifting a chain-link fence. Although there are a variety of sensor technology options available, including fiber optic cables, strain-sensitive coaxial cables, and accelerometers, the basic principle of operation is the same. With sensors securely attached to the fence fabric, intruder-induced vibrations are analyzed by a signal processor. When these vibrations exceed a calibrated threshold value, the signal processor generates an alarm signal. Installation of a fiber optic sensor cable is illustrated in Figure 3-13. For many sensor models, zone boundaries are set based on the physical placement of sensors and signal processors. Zone boundaries may also be set if cameras are being used as an assessment tool. Some models offer precise location of intrusions and software zone definition based on principles of optical interferometry or time domain reflectometry (TDR). Design guidance is as follows:

- A fence-disturbance sensor is a good choice for site perimeters with standoff and clear zone restrictions.
- Optimal sensor performance is highly dependent on proper fence construction. Follow established Army and Air Force specifications for “sensor-capable” fence construction such as USACE Standard Drawing 872-90-04, *FE7 Chain-Link Security Fence Details for Non-Sensored Fence*, UFC 4-022-03, *Security Fences and Gates*, and Air Force LCMC ESE-SIT-0001, *Standard Electronic Security Equipment Siting and Design Guidance for Permanent Installations*. For retrofit applications, existing fences will often require re-tensioning of the fabric and other enhancements before sensor installation.
- Place sensors to ensure full vertical coverage of the fence. Sensor coverage may be extended into outriggers to enhance detection of climbing intruders and ladder impacts.
- Overlap sensor coverage at zone boundaries.
- High winds and/or wind-blown rain and debris may cause nuisance alarms. Consider another sensor technology if wind speed frequently exceeds 20 miles per hour (32 kilometers per hour).
- Alarms may be generated by animals climbing or impacting the fence. Assess the potential for nuisance alarms based on wildlife activity in the area.
- Although fence-disturbance sensors are best suited for chain-link security fences, installation techniques may be adapted for certain types of ornamental fencing.

Figure 3-13 Fiber Optic Sensor Cable

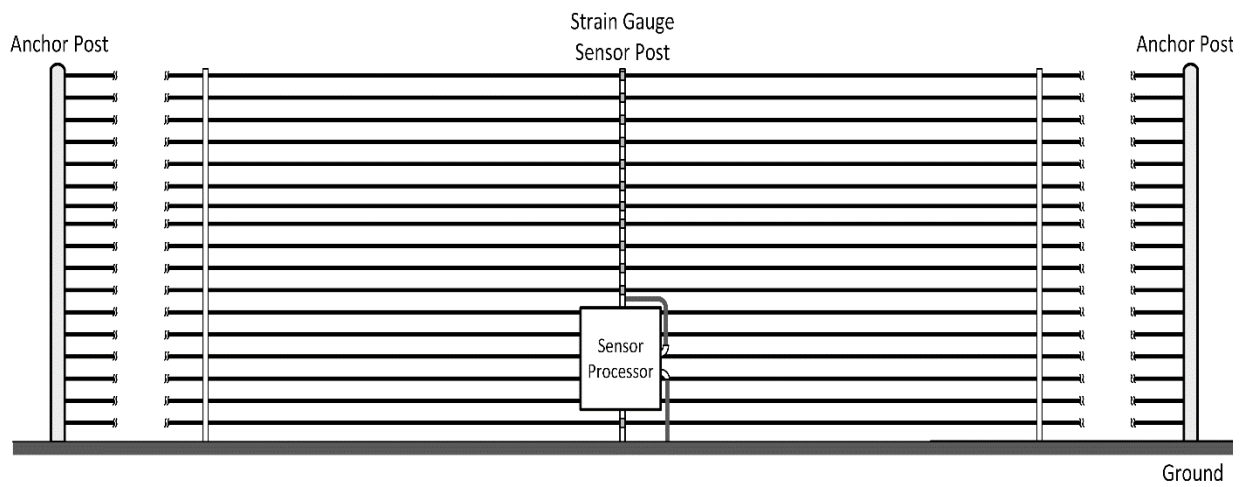


### 3-3.2 Taut-Wire Sensor.

A taut-wire sensor consists of an array of pre-tensioned parallel wires, each clamped to an individual sensor as illustrated in Figure 3-14. Wires are agricultural-style barbed wire. There are two sensor options: strain gauges and electro-mechanical switches. Sensors connect to a signal processor that generates an alarm in response to a change in wire tension. Intrusion attempts involving cutting, lifting, spreading, or climbing the wires are readily detectable as wire tension changes. A taut-wire sensor can be installed in a free-standing configuration, or it can be installed on a chain-link fence using specialized brackets. For a full-height configuration, wires extend from a few inches above the ground surface to a height of at least 8 feet (2.4 meters). Taut-wire sensors can also be installed as a “topper” for a fence or wall. Design guidance is as follows:

- A taut-wire sensor is a good choice for site perimeters with standoff and clear zone restrictions.
- A sensor post can cover a single zone up to a maximum length of 328 feet (100 meters). A typical zone configuration is a sensor post in the middle, an anchor post at each end, and slider posts at regular intervals along the length of the zone.
- Structural stability is a key factor in taut-wire sensor performance. Anchor posts, sensor posts, and slider posts must be constructed to support the tension applied to the wires.
- Consider installing a continuous concrete footing under the bottom wire in a full-height configuration to discourage shallow tunneling intrusions. This is especially important for loose, sandy soils that are easy to dig.
- A taut-wire sensor can operate with a low NAR in high-wind conditions, making it a good alternative to a fence-disturbance sensor for windy sites.
- Alarms may be generated by animals deflecting the lower wires or large birds landing on the upper wires. Assess the potential for nuisance alarms based on wildlife activity in the area.

**Figure 3-14 Taut-Wire Sensor**

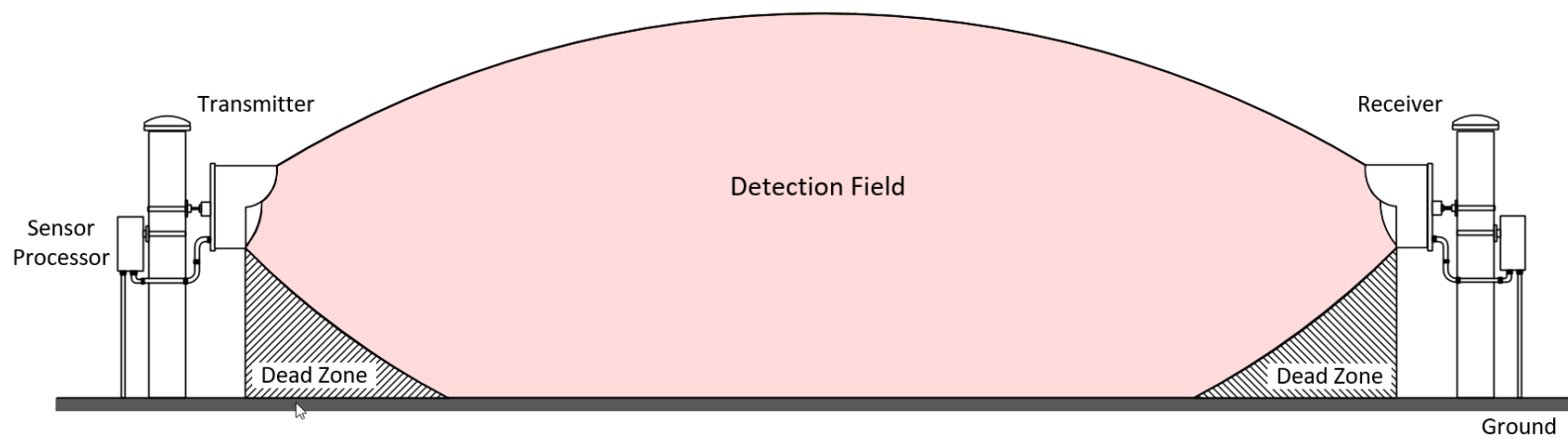


### 3-3.3 Bistatic Microwave Sensor.

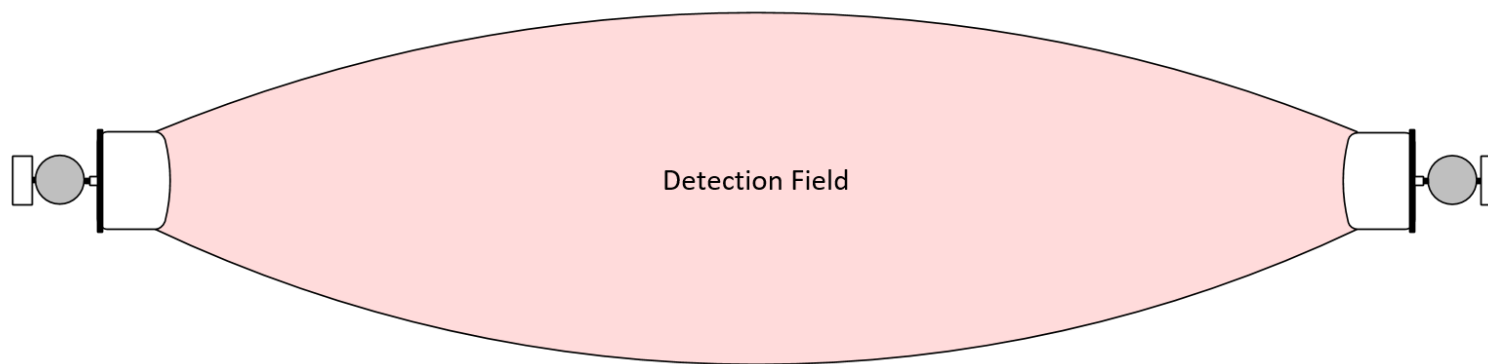
A bistatic microwave sensor provides active, volumetric intrusion detection coverage between a microwave transmitter and receiver separated some distance apart. As an intruder moves through the microwave field, the receiver detects the disturbance to the field and generates an alarm. Figure 3-15 illustrates a bistatic microwave field. Although analog models are still available, digital bistatic microwave sensors are preferred. A bistatic microwave sensor is capable of detecting common intrusion modes such as walking, running, and crawling. Design guidance is as follows:

- A bistatic microwave sensor is best suited for sites with flat terrain. Uneven terrain between a transmitter-receiver pair will result in detection gaps.
- Most bistatic microwave sensor models allow a transmitter-receiver separation distance up to at least 400 feet (122 meters). Some long-range models have a maximum separation distance of 1500 feet (457 meters).
- A clear zone width of at least 30 feet (9.1 meters) is needed along the perimeter to accommodate the volumetric microwave field.
- Mounting poles must be stable to ensure no movement of transmitters and receivers.
- Overlapping coverage is required at zone boundaries to compensate for “dead zones” near transmitters and receivers. Failure to properly overlap will result in detection gaps for crawling intrusions.
- Multiple transmitters and receivers can be “stacked” on a single pole to generate a larger detection pattern. In a “double stacked” configuration, as shown in Figure 3-16, the lower units are optimized for crawling intrusions while the upper units provide a greater height profile to detect jumping and bridging intrusions.
- Standing water or surface runoff will cause nuisance alarms. Grade the clear zone to ensure proper drainage.
- Because of the potential for wildlife-induced nuisance alarms, bistatic microwave sensors are typically installed on the inside of a single fence or in the isolation zone (between an outer animal control fence and an inner security fence) of a dual-fence configuration.
- The path between each transmitter-receiver pair must be kept free from obstructions. This includes vegetation control and snow removal.
- Placement of microwave units too close to the fence line could include the fence fabric within the detections zone and create nuisance alarms with the movement of the fence fabric.
- Use of bistatic microwave sensors must be coordinated with local military and government authorities responsible for managing the electromagnetic frequency spectrum. Consider using another sensor technology if there are concerns with frequency approval or electromagnetic interference.

**Figure 3-15 Bistatic Microwave Sensor**

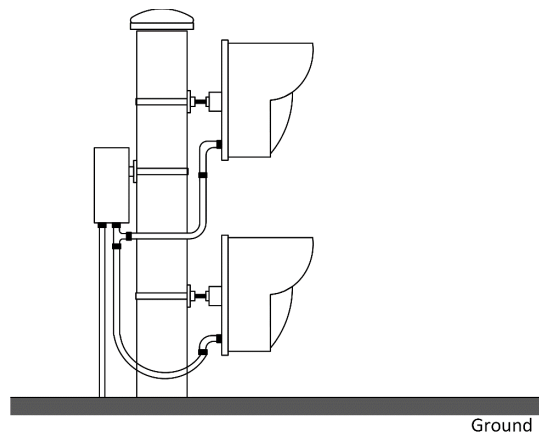


**Side View**



**Top View**

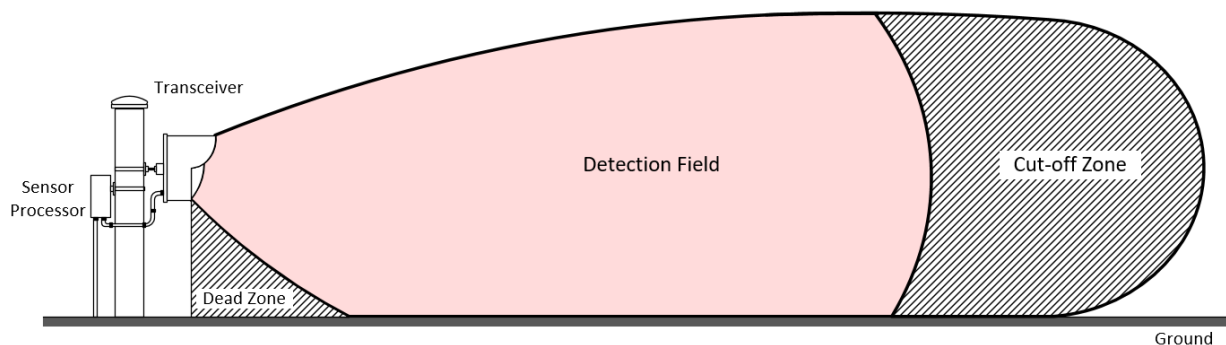
**Figure 3-16 “Double Stacked” Microwave Configuration**



### **3-3.4 Monostatic Microwave Sensor.**

A monostatic microwave sensor consists of a microwave transmitter and receiver co-located in the same housing. Sometimes referred to as a microwave transceiver, this sensor provides active, volumetric intrusion detection coverage as illustrated in Figure 3-17. Microwave energy reflected from the coverage area is continuously analyzed by the receiver. When objects moving through the coverage area alter the reflected energy, the sensor generates an alarm. A range cut-off setting allows activity beyond a user-selected distance to be rejected as an alarm stimulus. Although the principles of operation differ for monostatic and bistatic microwave sensors, both are able to detect walking, running, and crawling intrusions, and the same design guidance (see paragraph 3-3.3) applies to both, with one important exception. The range capability of a monostatic transceiver is significantly less than that of a bistatic transmitter-receiver pair, especially for crawling intrusions. For this reason, a monostatic microwave sensor is generally not preferred as a primary line of detection for a site perimeter. Monostatic microwave sensors may be appropriate as the primary sensor for certain short perimeter applications, but they are most useful in a supplemental role to fill gaps in primary sensor detection coverage.

**Figure 3-17 Monostatic Microwave Sensor**



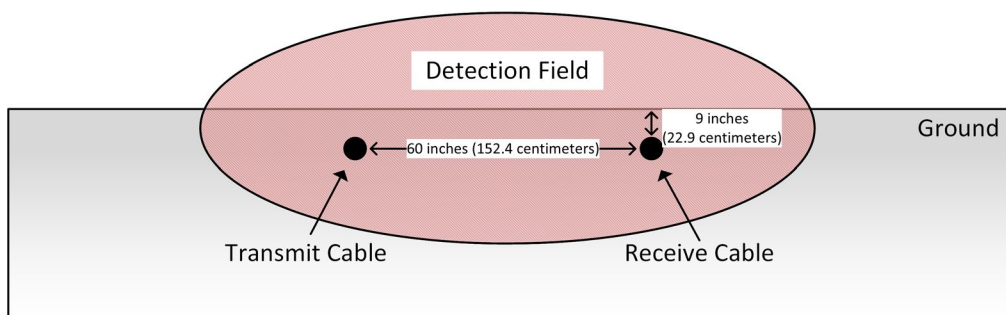
### 3-3.5 Ported Coaxial Cable Sensor.

A ported coaxial cable sensor is characterized as an active, radio frequency, volumetric sensor. This sensor employs two buried cables connected to a signal processor to create an above-ground electromagnetic field along the length of the cables. Figure 3-18 illustrates this electromagnetic field. The cables are installed in a parallel configuration, typically 5 feet (1.5 meters) apart, with each cable buried 9 inches (23 centimeters) deep in soil. Ports (openings) in the outer conductor of the coaxial cables allow energy to radiate from one cable (functioning as the transmitter) and couple into the other cable (functioning as the receiver), with the result being an electromagnetic field above, between, and below the cables. As an intruder moves through the above-ground portion of the field, the signal processor detects the disturbance to the field and generates an alarm. A ported coaxial cable sensor is capable of detecting common intrusion modes such as walking, running, and crawling. Design guidance is as follows:

- Because of the terrain-following nature of its electromagnetic field, a ported coaxial cable sensor is a good option for sites with uneven terrain.
- A ported coaxial cable sensor is a good option for sites where a covert line of detection is desired.
- Typical sensor cable installation involves trenching in soil and cutting slots in pavement. Trenching is recommended for certain thin pavements. Precise control of sensor cable depth and spacing must be maintained during the installation process.
- Zone boundaries are established electronically by the signal processor using time-of-flight analysis. Multiple alarm reporting zones can be set for a continuous length of sensor cable.
- A clear zone width of at least 30 feet (9.1 meters) is needed along the perimeter to accommodate the volumetric electromagnetic field.
- Detection field width and height are approximately 8 feet (2.4 meters) and 3.5 feet (1.1 meters), respectively. Consider another sensor technology with a greater height profile, such as a double- or triple-stacked bistatic microwave, if there are concerns with jumping or bridging intrusions.
- Verify soil suitability during the site survey and planning process. Certain soils exhibit very high electrical conductivity which will cause excessive attenuation of the radio frequency energy. Transitioning from soil to asphalt or concrete may also affect the attenuation of the radio frequency energy as well. This attenuation will reduce field strength above the ground and, in extreme cases, result in an unacceptably low probability of detection. Worst-case conductivity and attenuation are generally associated with heavy clay soils with a high moisture content. Coordinate soil suitability testing and analysis with the sensor manufacturer.

- Plan for seasonal calibration of the sensor for sites where significant soil freezing occurs in the winter. Electrical conductivity generally decreases when soil freezes, resulting in increased field strength above the ground. Conversely, when soil thaws, field strength decreases. Seasonal calibration will maintain a proper balance of probability of detection and NAR.
- Buried objects (such as pipes, cables, and culverts) below the sensor cables can affect performance. This includes steel reinforcing in concrete pavement. Identify buried objects prior to sensor installation and follow manufacturer's recommendations to mitigate performance impacts.
- Standing water or surface runoff will cause nuisance alarms. Grade the clear zone to ensure proper drainage.
- Because of the potential for wildlife-induced nuisance alarms, ported coaxial cable sensors are typically installed on the inside of a single fence or in the isolation zone (between an outer animal control fence and an inner security fence) of a dual-fence configuration.
- A ported coaxial cable sensor is compatible with up to 6 inches (152 millimeters) of grass height or snow accumulation. The clear zone must be maintained to stay within this range.
- Use of a ported coaxial cable sensor must be coordinated with local military and government authorities responsible for managing the electromagnetic frequency spectrum. Consider using another sensor technology if there are concerns with frequency approval or electromagnetic interference.

**Figure 3-18 Ported Coaxial Cable Sensor**



### 3-3.6 Electrostatic Field Sensor.

An electrostatic field sensor uses a vertical array of parallel steel wires connected to a processor to create a relatively narrow volumetric detection field, as illustrated in Figure 3-19. The number of wires can range from four to eight, depending on the desired height profile. Wires are tensioned and attached to insulators in an alternating pattern of transmit wires and receive wires. Wire terminations at the processor apply a

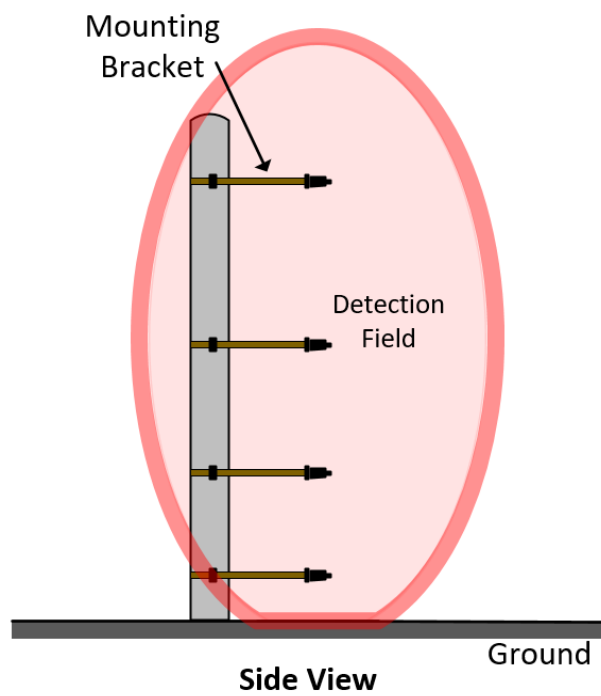
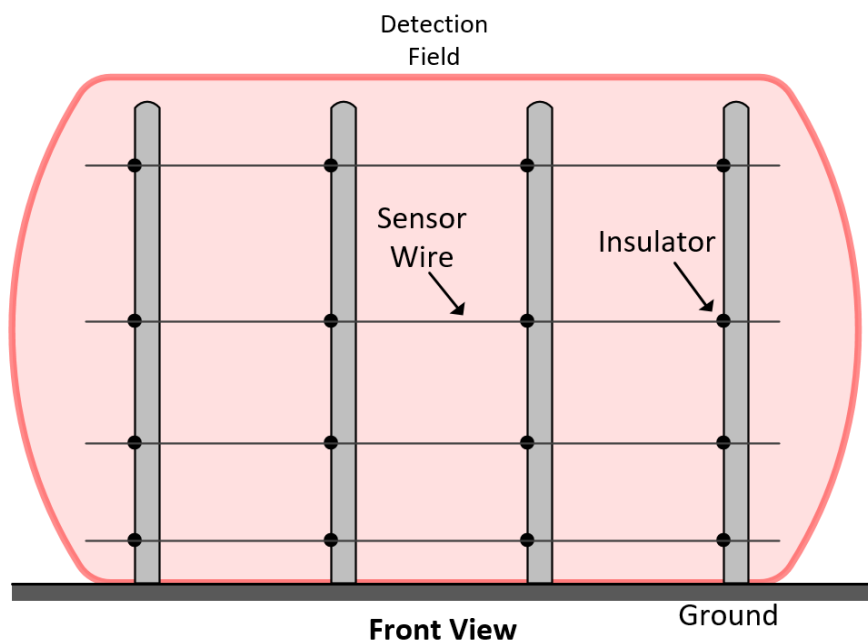
voltage to the transmit wires and ground the receive wires, creating an electrostatic field in close proximity to the wires. Disturbances to this field caused by an intruder moving through it are detected by the processor. An electrostatic field sensor can be installed on poles in a free-standing configuration, or it can be installed on a chain-link fence using specialized brackets and insulators. The maximum detection field height is approximately 12 feet (3.7 meters).

**Army and Navy Only:** Design guidance is as follows:

- An electrostatic field sensor has some terrain-following characteristics. With proper pole spacing, the sensor can be used at sites with moderately uneven terrain. Maintaining consistent spacing between the bottom wire and the ground surface is critical.
- A single processor can accommodate two adjacent zones, each with a maximum length of 328 feet (100 meters).
- A clear zone width of at least 15 feet (4.6 meters) is needed along the perimeter to accommodate the volumetric electrostatic field.
- Poles and brackets must be constructed to support wire tension, typically 50 pounds for each wire, and remain stable during all weather conditions.
- Proper grounding is essential to achieving good sensor performance. A low-resistance earth ground of 5 ohms or less is required.
- The ground surface in the vicinity of the sensor wires must be kept clear of vegetation (maximum height of 3 inches [76 millimeters]), water (standing or flowing), and snow.
- Because of the potential for wildlife-induced nuisance alarms, an animal control fence is recommended. Because of the potential for wildlife-induced nuisance alarms, electrostatic field sensors are typically installed on the inside of a single fence or in the isolation zone (between an outer animal control fence and an inner security fence) of a dual-fence configuration.

**Note:** No electrostatic field sensor has successfully completed Air Force testing; therefore, an electrostatic field sensor may not be used on an Air Force project.

**Figure 3-19 Electrostatic Field Sensor**

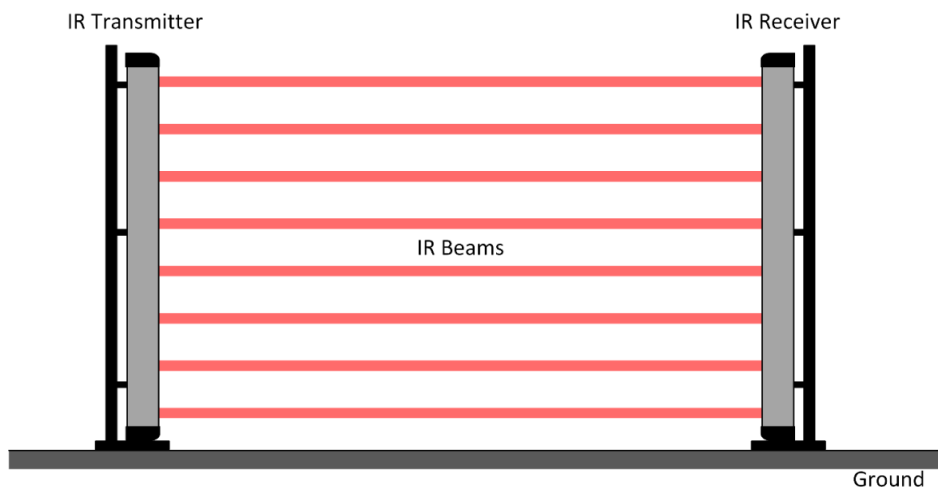


### 3-3.7 Active Infrared Sensor.

An active IR sensor provides a vertical series of narrow beams between two beam towers, as illustrated in Figure 3-20. Each beam is created by a transmitter-receiver pair installed in adjacent towers. A signal processor in the beam tower analyzes outputs from the receivers and generates an alarm when one or more beams is disturbed, enabling the detection of walking, running, and crawling intruders. Maximum tower height is approximately 10 feet (3 meters). Design guidance is as follows:

- A pair of beam towers can operate up to a maximum separation distance of 328 feet (100 meters).
- Since an active IR sensor does not generate a volumetric detection field, it can be used along perimeters that have very limited standoff.
- A level, smooth surface is required between each pair of towers. A paved surface is preferred.
- Stable mounting and precise alignment are required for beam towers.
- Nuisance alarms are likely during periods of heavy rain or fog.
- The path between the beam towers must be kept clear of obstructions, including snow accumulation. Obstructions will break the beam(s) and generate nuisance alarms.
- Because of the potential for wildlife-induced nuisance alarms, an animal control fence is recommended.
- Use of an active IR sensor must be coordinated with local military and government authorities responsible for managing the electromagnetic frequency spectrum. However, because it operates outside the radio spectrum, concerns with frequency approval or electromagnetic interference are minimal.

**Figure 3-20 Active Infrared Sensor**



### 3-3.8 Passive Infrared Sensor.

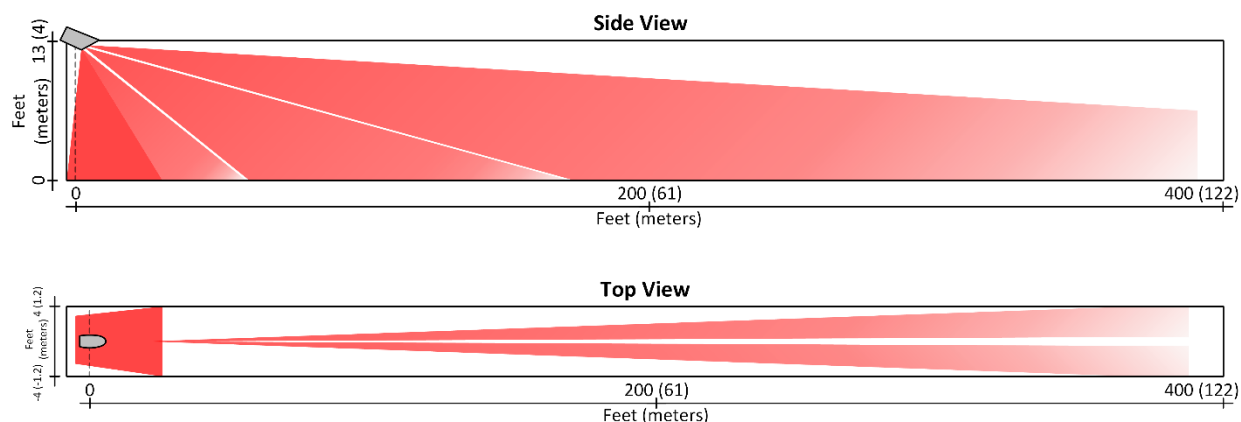
A PIR sensor detects walking, running, and crawling intruders by sensing changes in IR energy within its volumetric coverage pattern. The key to detection is the surface temperature contrast between an object of interest (intruder) and the background. Figure 3-21 illustrates the relatively narrow curtain coverage provided by a PIR sensor in an exterior perimeter configuration. Concerns over detection range and probability of detection limit consideration of PIR sensors as a primary line of detection.

**Army and Navy Only:** The design guidance follows:

- Although a PIR sensor can tolerate slight changes in surface elevation, uneven terrain may result in dead zones. Generally flat terrain in the coverage pattern will avoid creating dead zones.
- The dead zone (no detection coverage) beneath the sensor must be compensated for by overlapping coverage at zone boundaries or use of a supplemental sensor.
- A PIR sensor has no inherent range limiting capability, making it difficult to reliably set detection zone boundaries. Although a person can be detected out to a range of approximately 328 feet (100 meters), large heat sources such as vehicles and aircraft may be detected over 3,280 feet (1,000 meters) away. Aiming the sensor toward a solid object such as a wall or berm will limit the detection range.
- A clear zone width of at least 15 feet (4.6 meters) is needed along the perimeter to accommodate the volumetric detection field.
- Lack of sufficient temperature contrast between a person and the background will result in detection gaps. Avoid using PIR sensor where background temperatures in the range of 96 to 101 degrees Fahrenheit (35.5 to 38.3 degrees Celsius) are expected.
- Dense fog or heavy snow will reduce detection range for a person to 164 feet (50 meters) or less.
- Because of the potential for wildlife-induced nuisance alarms, an animal control fence is recommended.

**Note:** PIR sensors are not approved by the Air Force for exterior perimeter intrusion detection applications.

**Figure 3-21 Passive Infrared Sensor**



### 3-3.9 Dual Technology Sensor.

A dual technology sensor consists of a PIR detector and a microwave transceiver combined in a single housing to create a volumetric detection pattern. The detection range is approximately 50 feet (15.2 meters) for a wide-angle pattern and 100 feet (30.5 meters) for a narrow pattern. For most models, detection logic is factory set in the “and” state to reduce the potential for nuisance alarms. Even with “and” logic, proper sensor placement and aiming is necessary to avoid detecting people, vehicles, and wildlife outside the intended coverage area. Sensor mounting must be stable and the detection pattern free from obstructions. Although not appropriate for use as a primary sensor, dual technology sensors are effective in filling gaps in primary sensor detection coverage. One “gap filler” application is detecting climbing intrusions at a large gate post as shown in Figure 3-22.

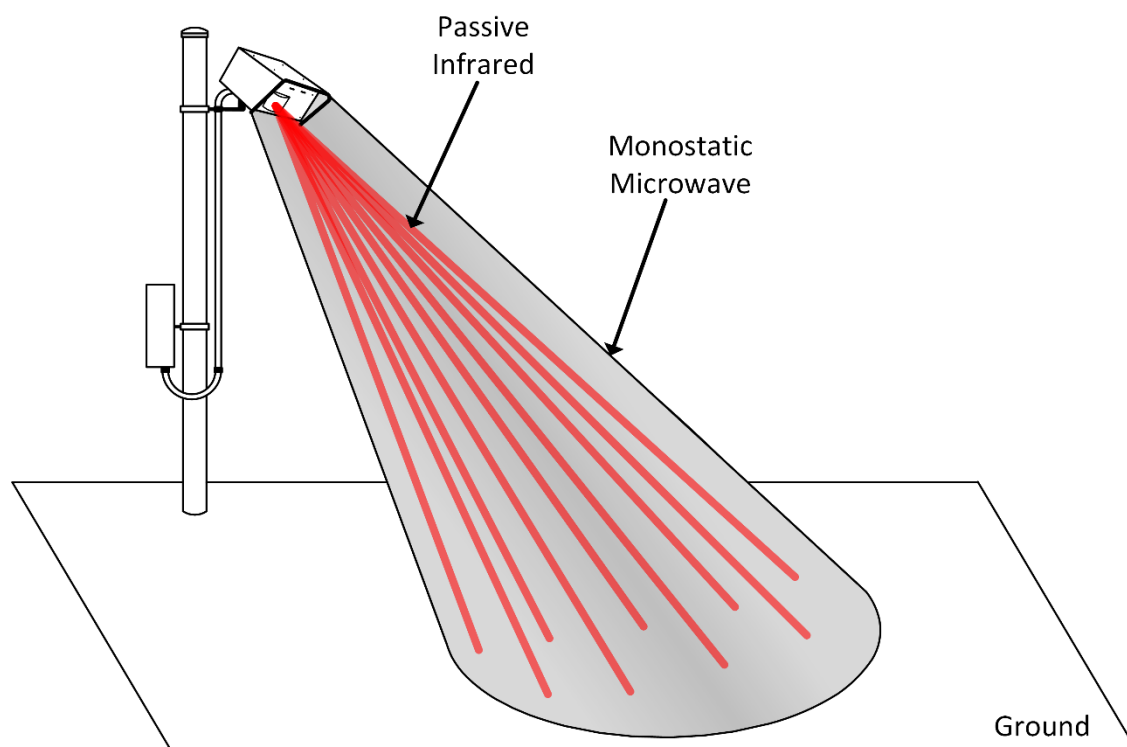
### 3-3.10 Scanning Laser Sensor.

The operating principle of a scanning laser sensor is described in paragraph 3-2.4. This sensor may be used as a “gap filler” where short-range (65 feet [19.8 meters] maximum), vertical planar coverage is needed to supplement a primary sensor. Stable mounting is required, and the detection plane must be free from obstructions. A mounting height of at least 13 feet (4 meters) is recommended for outdoor applications.

### 3-3.11 High Security Switch on Perimeter Gates.

Where required to detect unauthorized opening, install HSS on each perimeter gate. A UL 634 Level 1 HSS is preferred. The switch must be installed on the secure side of the gate, and the gate must be stable, with a positive latching mechanism to facilitate proper switch alignment. Excessive gate movement in windy conditions will cause nuisance alarms.

Figure 3-22 Dual Technology Sensor

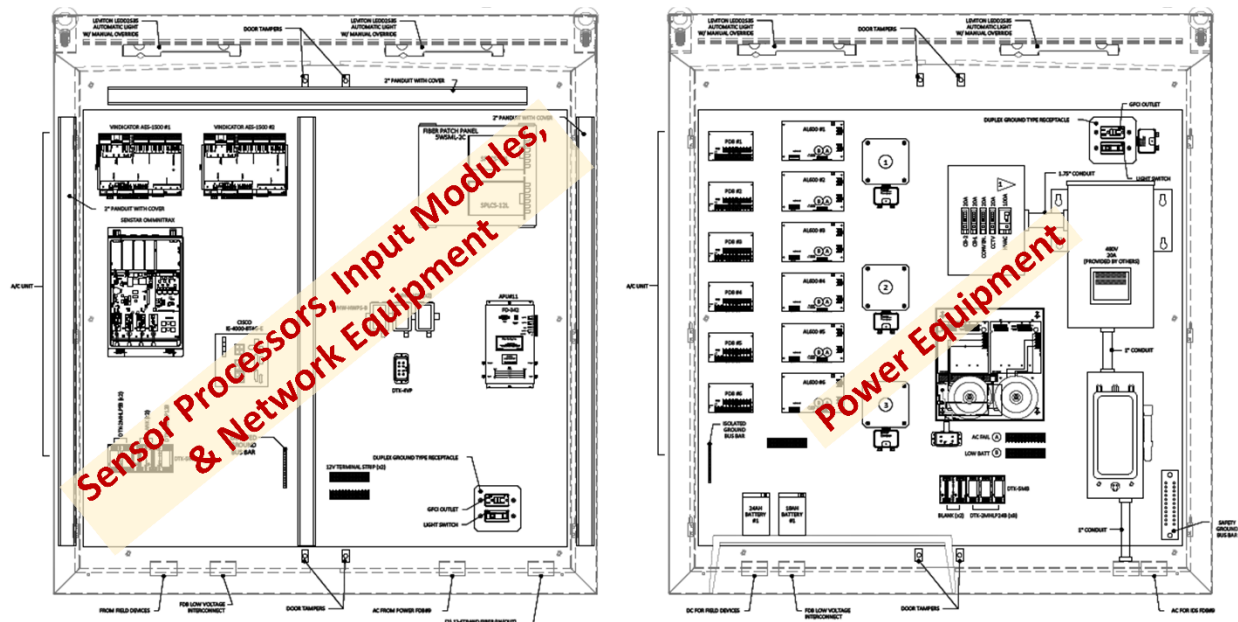


### 3-3.12 Field Distribution Box.

A field distribution box (FDB) serves as a critical node for sensor processing, data transmission, and electrical power along a site perimeter. Figure 3-23 illustrates some of the key features of an FDB. Design guidance is as follows:

- FDBs must be installed within the secure side of the perimeter fence. For a double fence configuration, this applies to the inner fence. Offset distance from the fence must be consistent with clear zone requirements. Typical offset is 30 feet (9.1 meters).
- An FDB is typically required at every other zone boundary. For example, a 20-zone system would require approximately 10 FDBs. This is a general guideline; exact quantity and placement of FDBs must be determined on a site-specific basis.
- FDB placement must provide ease of access for maintenance personnel.
- Each FDB must be sized to accommodate all perimeter security equipment and associated wires and cables without excessive crowding. In addition to intrusion detection equipment, FDBs will also house equipment associated with the perimeter ACS, VSS, and data transmission network.
- The FDB must provide environmental protection for the installed equipment. A NEMA Type 4, IP 66, or equivalent enclosure is appropriate for many sites. Use a NEMA Type 4X, IP 66, or equivalent with corrosion-resistant material enclosure at sites where additional corrosion protection is needed. A heater or air conditioner may be needed depending on the local climate and the temperature ratings of the installed equipment.
- Each FDB must be grounded.
- FDB power must include both alternating current (AC) power (primary) and battery backup.
- An FDB must be lockable and must have a tamper switch to detect unauthorized opening. A large FDB will require a tamper switch at the top and bottom of each enclosure door.
- When conditions allow, locate all FDB penetrations into the bottom to prevent an avenue of entry for rain and other weather elements.

Figure 3-23 Field Distribution Boxes



### 3-4 EXTERIOR WIDE AREA INTRUSION DETECTION.

Exterior wide area detection sensors are occasionally used at sites requiring exterior IDS in special use situations requiring early warning of a potential threat. These technologies will not be extensively detailed in this UFC but only included so the reader knows they exist and can research further as necessary. These sensors are typically placed for detection of potential threats outside of a traditional physical perimeter or boundary but may be used at any site where there is a desire for early detection of threats before crossing a line of demarcation, visible or otherwise. Coverage areas are typically open uncontrolled space, and inherently will have a higher probability for false alarms due to the wide area and various topographies being covered. In addition, the systems are typically relatively expensive when compared to traditional exterior ESS systems. In a traditional system with a defined perimeter/boundary, it is recommended to use these technologies only as a supplement to traditional exterior IDS systems. Some non-traditional examples of wide area sensor deployment may be on waterways with restricted traffic requirements; at any site where there is desire for awareness of potential threats in close proximity before actual contact with the perimeter/boundary has been made; or tactical sites requiring detection of approaching adversaries where the detection area is completely uncontrolled space, and no visually defined boundary exists.

Wide area sensors are differentiated from traditionally used exterior sensors in that they typically will not be held to the same requirements for meeting probability of detection rates, confidence levels, and NAR/FAR. These systems generally will include an operator workstation displaying threat location and movement on a site map or aerial photo along with video from an associated camera. This automated association of

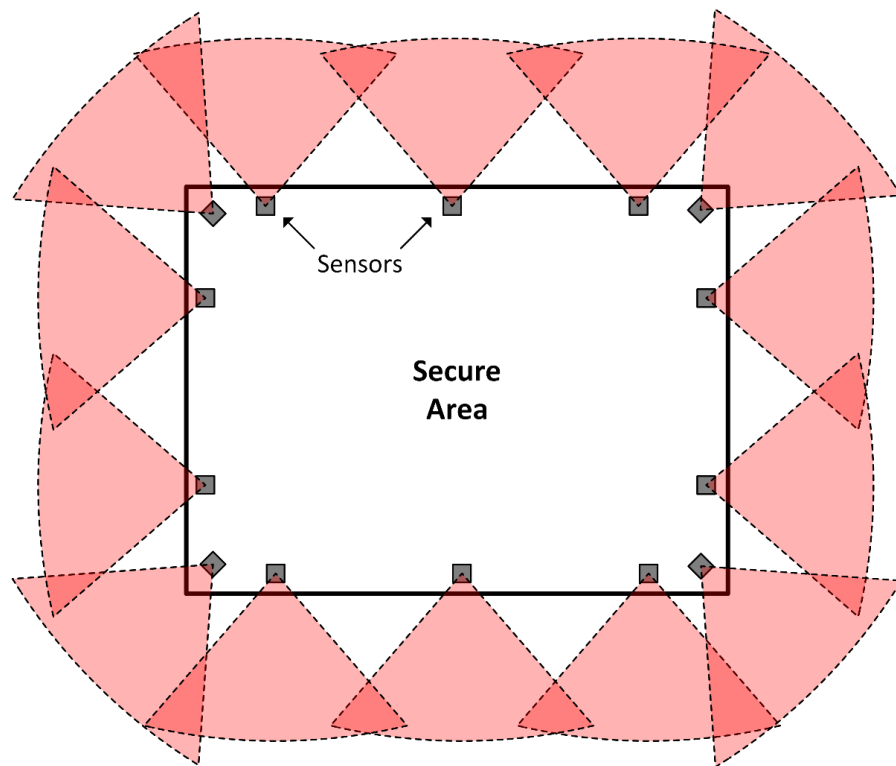
georeferenced object information with video allows an operator to make a real-time assessment of the potential threat posed by the object. Some of the technologies that may be used as described below.

### **3-4.1 Ground Surveillance Radar.**

Ground surveillance radar units may be installed along a high-security outdoor perimeter to detect objects moving within a defined coverage area. Units may be deployed as a single unit or a system of units based on the system selected. When used as a system, the preferred configuration, as illustrated in Figure 3-24, is to orient the radar units to provide continuous overlapping coverage of “public space” beyond the secure perimeter. This orientation provides early warning of personnel and vehicles approaching the perimeter and is an effective complement to exterior perimeter intrusion detection technology. Based on the principle of Doppler shift, a ground surveillance radar unit is able to detect a moving object, determine its location, and track its movement. Multiple objects can be tracked simultaneously. The coverage area is highly dependent on model and can range from 5 acres up to a few hundred acres. Design guidance is as follows:

- Level, unobstructed terrain free from excessive vegetation provides the optimal background for ground surveillance radar. Above-ground features, whether natural or man-made, will create gaps in radar coverage.
- Detection range is dependent on the radar cross-section of the object of interest. Range is greatest for vehicles and much less for a person walking. Consistent detection of a crawling intruder is limited to short ranges. Other technologies, such as microwave or buried line sensors, are better to meet this requirement.
- The radar coverage area is usually a large uncontrolled space; hence, detection of a wide range of human and animal activity must be anticipated. Video assessment is highly recommended to enable immediate visual assessment.
- Ground surveillance radar can be used over water to detect surface objects such as boats and personal watercraft.
- Use of ground surveillance radar must be coordinated with local military and government authorities responsible for managing the electromagnetic frequency spectrum.
- For in-depth technical information and siting guidance, see Air Force LCMC ESE-SIT-0001.

**Figure 3-24 Ground Surveillance Radar**



### **3-4.2 Video Analytics.**

Video analytics systems, although not recommended as a typical ESS exterior sensor technology (see paragraph 3-5.11), can be used as a form of early warning intrusion detection. Often, when used in this scenario, a low or no light video imaging technology is chosen (for example, thermal, IR, or near-IR technologies) and paired with a pan-tilt-zoom (PTZ) mechanism for long range use. Due to the non-natural image produced in the case of thermal imaging technologies, a thermal camera is often paired with a visual light spectrum camera, such that the two camera outputs are combined to produce a familiar but enhanced long-range visual representation of potential threats. The system may consist of a single imaging device, or several devices used to cover a large area with varying terrain or other obstructions. When paired with signal processing of the video analytics system, long-range determination of friend vs. foe and real time threat tracking capabilities are realized, regardless of the presence of visual light. Table 3-1 provides information helpful in choosing a camera technology for early warning analytics.

**Table 3-1 Imaging Technology for Video Analytics (Wide Area IDS)**

Technology	Range (Nominal)	Light Source	Support	Relative Cost	Advantages	Disadvantages
Traditional visual spectrum camera	(Not typically used in early warning scenarios due to lack of low light and long-range capabilities with exception when paired with another technology listed below)					
Camera with infrared illuminators	Short: 100 to 300 yards (90 to 275 meters)	Infrared illuminators (built-in or separate)	Power for camera and illuminator; video cable; illuminators	Low	Night vision capable; low total cost of ownership	Limited to the range of the associated infrared illuminators
Near-infrared system	Medium: 1000 to 3000 yards (900 to 2700 meters)	Near-infrared laser	Composite system of laser and camera	Medium to high	No interference from heat and visible light; natural-contrast night image	Performs best as synchronized system
Thermal camera (uncooled)	Long: 1000 to 5000 yards (900 to 4500 meters) (height of eye)	Heat energy emitted from object/scene	Power for camera; internal temperature-adjusting controls	Medium	Autonomous system: visible light or supporting illumination not needed	Non-natural image; requires trained operator to interpret thermal images
Thermal camera (cooled)	Long: 1000 to 10000 yards (900 to 9000 meters) (height of eye)	Heat energy emitted from object/scene	Power for camera; internal refrigerant system	High	Highest detection sensitivity; autonomous system	High cost; maintenance on coolant system; non-natural image may require operator training

### 3-4.3 Electronic Harbor Security System (EHSS).

The EHSS integrates electronic sensors and video systems to detect, assess, and track waterside surface and subsurface threats. The surface threat detection consists of a video imaging and radar component (typically mounted on guard towers), while the subsurface detection relies on a system of submerged sound navigation and ranging (SONAR) transponders. For further information on EHSS, see UFC 4-025-01, *Security Engineering: Waterfront Security*.

### **3-5 GENERAL DESIGN CONSIDERATIONS.**

#### **3-5.1 Compliance with Security Regulations.**

Determining which assets require IDS coverage is an essential first step in the IDS design process. The designer must work closely with the facility owner/user to understand what assets are present and then determine whether or not IDS is required based on applicable security regulations. For a given building, the goal is to focus interior IDS coverage where it is required (such as arms room and SCIF) while avoiding frivolous investment to cover low-security areas (such as office suite and conference room). Examples of assets that require exterior perimeter IDS are special weapons (nuclear, chemical) storage facilities, high-value aircraft parking areas, and ballistic missile defense sites. Security regulations are generally silent on requirements for exterior wide-area intrusion detection.

#### **3-5.2 Alarm Monitoring Location.**

Since intrusion detection is primarily concerned with protecting unattended high-value assets, the designer must identify the best method for continuous alarm monitoring during periods when the secure area is not occupied. For a facility that has a continuously staffed security desk, local IDS alarm monitoring may be the best option. Most facilities on military installations, however, do not have around-the-clock security staffing. This is especially true of smaller buildings that may have only one or two interior IDS zones. The best option for these facilities is connecting the local IDS zone(s) to a base-wide IDS with a continuously staffed central monitoring station. For some projects, it may be appropriate to provide the capability to monitor IDS alarms locally (at the security desk during duty hours, for example) and also at the central monitoring station (primarily after duty hours). **Note:** Security policy may require central monitoring of IDS.

#### **3-5.3 Zone Definition.**

The designer must define zones for both interior IDS and exterior perimeter IDS. Guidance for defining zones is as follows.

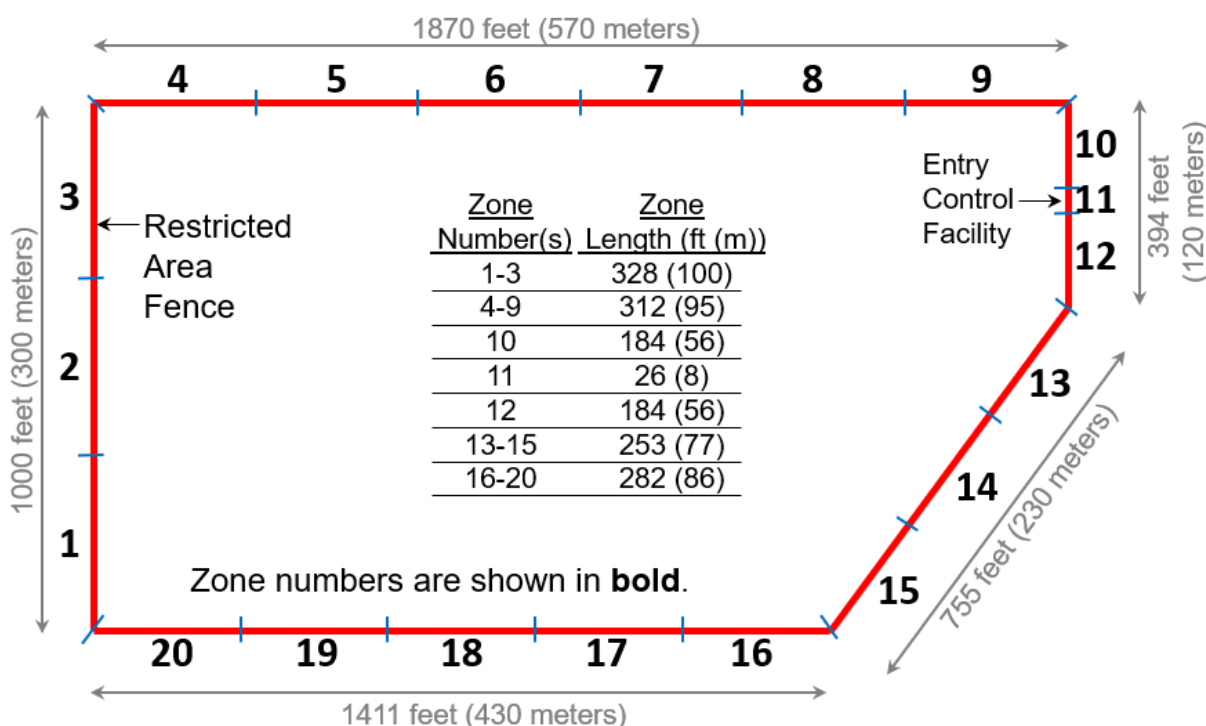
##### **3-5.3.1 Interior IDS Zone.**

An interior IDS zone is a room or space within a building that can be armed and disarmed independently from all other zones. The simplest interior zone is a single room with a specialized function protected by a few sensors connected to an intrusion panel. A good example of a simple interior zone is an arms room. A large zone may encompass several adjacent rooms (to include an entire floor, wing, or office suite in some buildings) or a large open area, and it may have twenty or more sensors connected to the panel. Security policy may require logical and/or physical separation of some assets, resulting in the need for separate intrusion panels for each zone. Examples of interior IDS zones are provided in Appendix A.

### 3-5.3.2 Exterior Perimeter IDS Zone.

An exterior perimeter IDS zone is a continuous section of perimeter for which alarms are annunciated independently from all other alarm zones. Like its interior counterpart, an exterior IDS zone can also be independently armed and disarmed. The designer must determine the appropriate perimeter zone layout based on the shape of the perimeter, length of each side or fence segment, location of the entry control facility, and the range capability of the candidate sensor technology. As a general rule, shorter zones enhance alarm assessment and response, but longer zones are more economical. A standard zone length of approximately 330 feet (100 meters) typically achieve a good balance between system cost and system effectiveness and is well within the range capabilities of most sensor technologies. Another advantage of a 330-foot (100 meters) zone is that alarms can be visually assessed anywhere in the zone with a single fixed camera (assuming the appropriate setback distance, lens focal length, and faceplate resolution are specified). Ideally, each entry control facility will be a separate zone and each corner or bend will be a zone boundary. An example of an exterior perimeter IDS zone layout is shown in Figure 3-25.

Figure 3-25 Exterior Perimeter IDS Zone Layout



### 3-5.4 Sensor Selection and Placement.

Long-term IDS performance depends on sensor selection and placement decisions made during the design process. Base these decisions on design guidance presented

previously in this chapter, but, more importantly, they must incorporate product-specific planning and installation instructions provided by sensor manufacturers. Any concerns with site conditions negatively impacting sensor performance must be resolved with manufacturers during the design process.

### **3-5.5 Performance Metrics.**

An intrusion detection sensor must provide a probability of detection of at least 95%, with a goal of 99%. These values apply to the detection of intrusion attempts within the sensor's intended coverage area. Meeting this probability of detection standard can be achieved through proper sensor installation and calibration. A nuisance alarm is caused by a clearly identifiable stimulus that does not represent an intentional intrusion attempt. Weather and animals are examples of nuisance alarm stimuli. A false alarm is an alarm for which no cause can be determined. Allowable NAR and FAR are as follows:

- Interior Sensor. NAR must not exceed three alarms per month. FAR must not exceed one alarm per month. These values are considered averages for a 12-month evaluation period.
- Exterior Perimeter Sensor. NAR must not exceed three alarms per day. FAR must not exceed one alarm per day. These values are considered averages for a 30-day evaluation period.
- Exterior Wide-Area Sensor. NAR must not exceed 15 alarms per day. FAR must not exceed three alarms per day. These values are considered averages for a 30-day evaluation period.

Vulnerability to defeat is a sensor performance metric that addresses the potential for an intruder to employ specialized knowledge, skills, tools, and equipment to avoid detection. Commonly known limitations of sensor coverage area and range are not associated with a sensor's vulnerability to defeat. No additional discussion of vulnerability to defeat is provided in this document due to concerns over security classification.

### **3-5.6 Multi-Layered Detection.**

Provide multi-layered detection to the greatest extent practical, beginning at the protected asset and moving outward. Each additional layer increases the overall probability of detection, but this benefit must be carefully balanced with increased cost and regulatory requirements.

### **3-5.7 Supervision and Encryption.**

Any disruptions to data connections between IDS components must be immediately annunciated at the alarm monitoring workstation, resulting in end-to-end supervision of the entire system. Using Figure 2-1 as a reference, this applies to the following connections: sensor–panel, panel–server, and server–workstation. Direct current (DC) line supervision is typical for a sensor–panel connection with an end-of-line resistor

installed inside the sensor housing. Panel–server and server–workstation connections typically employ some form of poll-and-response supervision over the network. Although encryption of IDS data connections is not a universal requirement, it is called for in certain security regulations. Encrypt panel–server and server–workstation connections in accordance with applicable security regulations.

### **3-5.8 Tamper Switches.**

Tamper alarms must be immediately annunciated at the alarm monitoring workstation in response to physical tampering attempts. This applies to sensors as well as components installed in IDS panels and enclosures. Ensure each sensor has a factory-installed tamper switch that is integral to the sensor housing. Equip each IDS panel and enclosure with a tamper switch to detect opening. Some tamper switches have a maintenance position to prevent tamper alarms from annunciating while authorized service is being provided.

### **3-5.9 Alarm Annunciation.**

Configure the IDS to annunciate a uniquely identifiable alarm for each sensor type. Example, “Intrusion” and “tamper” alarms must be distinguishable for each sensor.

### **3-5.10 Alarm Assessment.**

A video system can be used in conjunction with an IDS to provide immediate visual assessment of intrusion alarms. This allows an operator to describe the apparent cause of the alarm to the response force before they arrive at the IDS zone. The VSS and IDS must be tightly integrated to provide maximum operator efficiency. Remote video assessment is especially important for exterior perimeter and wide area intrusion detection because of the relatively high nuisance alarm rate associated with outdoor sensors. Without video cameras, “eyes on” alarm assessment by a person is typically required.

### **3-5.11 Video Analytics for Intrusion Detection.**

Although video analytics can be very effective as a surveillance tool (see paragraph 5-11.1), it is not considered a primary IDS technology on par with the proven interior and exterior sensors described in this chapter. For most common IDS applications, traditional IDS sensors are generally superior to video analytics in terms of probability of detection, nuisance alarm rate, integration with alarm monitoring systems, and cost. The designer may consider specifying video analytics as an intrusion detection sensor for projects where unusual site conditions bring into question the viability of all other sensor technology options.

### **3-5.12 Operational Availability.**

IDS recommended operational availability (also referred to as “uptime”) is no less than 99.99% with a goal of 99.999%. This applies to the entire system, including the data transmission network and electrical power source. Refer to IEEE Standard 493, *IEEE*

*Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*, for guidance on calculating and analyzing operational availability.

**Note:** Whether it is a user-owned network or a service provider network, any network used to pass ESS data must provide the same backup power requirements needed for the ESS.

### **3-5.13      Latency.**

Latency is the delay between activation of a sensor in an IDS zone and annunciation of the corresponding alarm at the alarm monitoring workstation. IDS latency in the range of 3 to 10 seconds is considered acceptable for most systems.

### **3-5.14      Backup Power.**

Provide backup power for IDS and ensure uninterrupted system operation upon primary power loss. Backup power is typically provided by batteries and uninterruptible power supplies (UPS), as well as generators or a combination of all three. IDS for some assets requires longer backup power runtime; comply with applicable security regulations. Annunciate primary power fail alarms and low battery alarms at the operator workstation.

### **3-5.15      Wireless Sensors.**

Do not use wireless intrusion detection sensors on DoD projects.

### **3-5.16      UL 2050.**

As a general rule, UL 2050, *National Industrial Security Systems*, does not apply to an IDS that is owned and operated by DoD. However, UL 2050 does apply to facilities for which IDS monitoring and maintenance is performed by a UL 2050 alarm service company (ASC) under contract to a DoD organization. Since a very high percentage of DoD facilities that require IDS are connected to a DoD-owned central monitoring station, compliance with UL 2050 is not a consideration for most projects. Security policy may require IDS to be installed in accordance with UL 2050 Extent 3, which is detailed in UL 681, *Standard for Installation and Classification of Burglar and Holdup Alarm Systems*.

## CHAPTER 4 ACCESS CONTROL SYSTEM

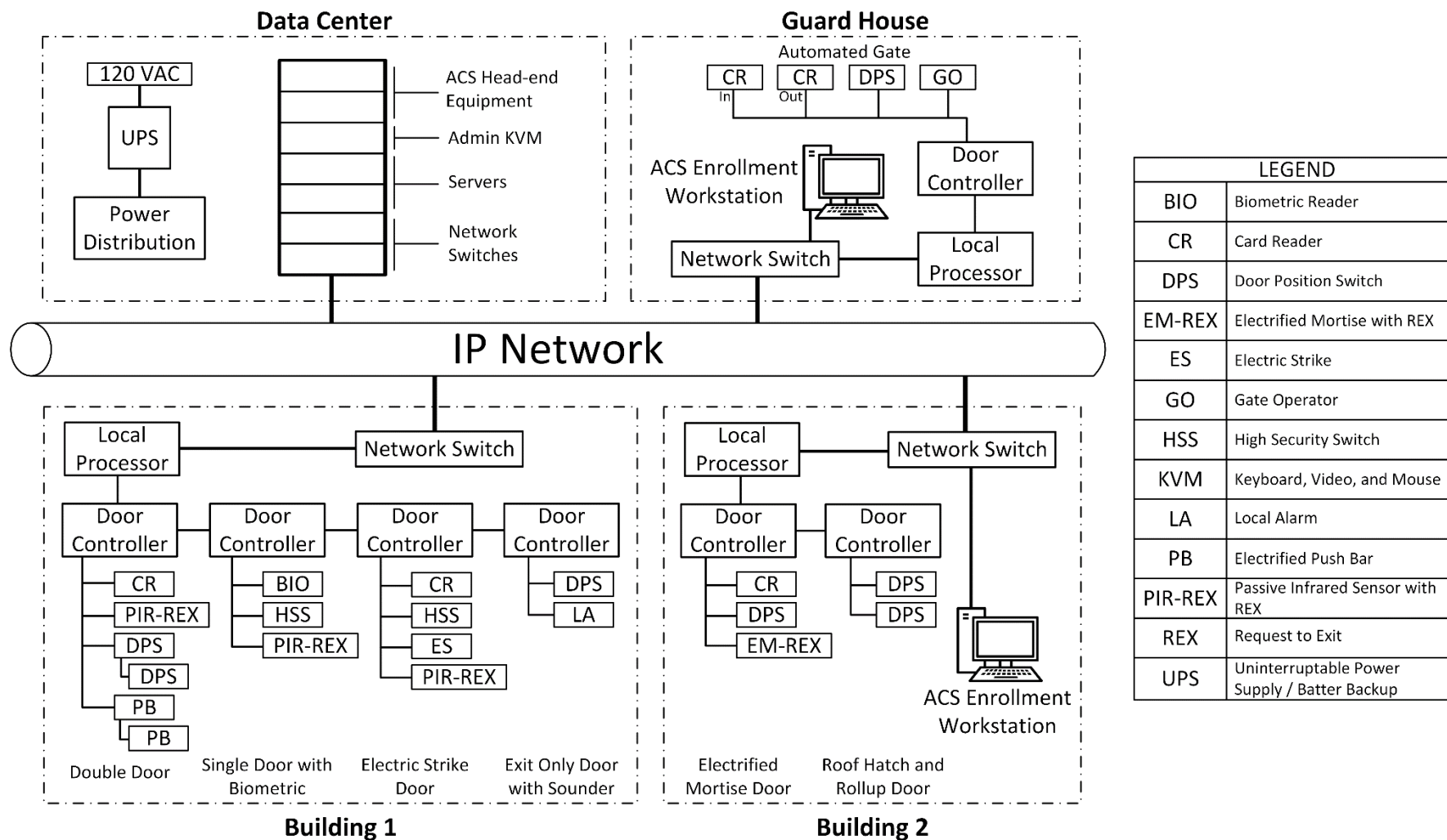
### 4-1 TECHNOLOGY OVERVIEW.

The primary function of an ACS is to ensure that only authorized personnel are permitted into controlled spaces or restricted areas. The ACS will log and archive all transactions and events, alert authorities of unauthorized entry attempts, forced entries, door held open, and other intrusion and tamper alarm events. An ACS consists of entry devices, exit devices, electronic locking devices, and monitoring switches, connected via local control panels and a network to a central system consisting of a file server and enrollment and alarm monitoring/operator client workstations. While ACS devices and control panels are considered specialized security equipment, the security network components and infrastructure, central system, and client workstations are considered PIT. The primary documents describing the required features of a DoD ACS and which outline a strategy for the design and implementation of a DoD ACS are National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 201, *Evaluation Program Approved Products List (APL)*, *Physical Access Control System (PACS) Components*, and NIST SP 800-116, *Guidelines for the Use of PIV Credentials in Facility Access*. Personnel involved in the planning, design, and procurement of a DoD ACS must utilize these documents in conjunction with this UFC.

### 4-2 SYSTEM CONFIGURATION.

An ACS may consist of a single or group of stand-alone programmable integrated electronic lock set or many integrated components, including entry devices such as a card reader, request-to-exit (REX) devices, electronic locking devices, and door/gate position monitoring switches, all monitored and controlled by a distributed processing system that includes local control panels, head-end server equipment, and one or more administrative, enrollment, and operator client workstations. ACS client workstations allow security personnel to enroll authorized users in the system, set user access permissions, monitor events, register and display alarms, and run reports on past system activity. Figure 4-1 shows an example of an ACS configuration, and detailed descriptions of the various components of an ACS are provided later in this chapter. ACS typically log and archive all transactions and alert authorities of unauthorized entry attempts. ACS can be interfaced with an IDS and video management system (VMS) to help security personnel assess unauthorized entry attempts.

Figure 4-1 Example Access Control System



### **4-3 PRINCIPLE OF OPERATION.**

In general, an ACS compares an individual's identifier or federally issued personal identity verification (PIV) certificate against a verified user database. A FIPS 201 compliant ACS is capable of performing an encrypted challenge and response of the federally issued digital certificates issued with an individual's Common Access Card (CAC) or federal PIV card, thus providing a higher level of authentication and identity assurance. If an individual's identity is verified/authenticated, the ACS sends output signals to allow that authorized individual entry through controlled portals such as gates or doors. The system has the capability of logging entry attempts (authorized and unauthorized) that are archived. Typically, the ACS interfaces with the IDS for input of digital alarm signals at access portals controlled by the ACS. An example of this would be a "door forced" alarm at an access-controlled door. Similarly, the ACS interfaces with the VSS in that cameras could be called up or placed at remote gates to verify identity of entrants before manually actuating the remote gate. Signals from the ACS are communicated to a local security monitoring workstation or central monitoring station through the transmission lines of the data transmission media (DTM).

### **4-4 ACS ENTRY DEVICES.**

Entry device technologies are grouped into three primary categories:

- Credential devices
- Coded devices
- Biometric devices

These devices operate on three basic techniques:

- Something a person has, such as a CAC
- Something a person knows, such as a personal identification number (PIN). The PIN may be a locally stored number on the system or associated with a CAC.
- A person's unique physical characteristic, such as a biometric identifier (fingerprint)

#### **4-4.1 Credential Devices.**

Credential devices allow a person possessing a recognized credential or digital certificate to enter a controlled area. A coded credential (such as a CAC) contains a machine-readable code, Card Holder Unique Identifier (CHUID), and digital certificates. In its simplest terms, when the card is read, and if the code or certificate stored on the credential matches the code or certificate stored in the system, an electric signal unlocks the door. Various technologies are used to store a code or digital certificate in/on a card. The most common types of cards are described in more detail in paragraph 4-6.6.

Each type of card and card reader has its own advantages and disadvantages. Refer to paragraphs 4-6.5 and 4-6.6 for more on the advantages and disadvantages of each.

#### **4-4.2 Coded Devices.**

Coded devices such as keypads operate on the principle that a person has been issued a code or PIN to enter into the device that will verify the authenticity of the code entered. Any person entering a correct code is authorized to enter the controlled area. Keypads are often integrated with card readers in order to provide two-factor (card + PIN) authentication for a greater level of identity assurance. For information about the different types of coded devices, see paragraph 4-6.7.

The number of allowable unique codes can be limited. For example, a four-digit PIN, which is the recommended minimum number of digits, only provides 10,000 different possible codes. The more digits required, the more possible codes, thus making it more difficult to guess or duplicate a PIN.

#### **4-4.3 Biometric Devices.**

Biometric devices rely on the comparison of a specific biological characteristic to a template that is stored on the card holder's credential (CAC) itself or in the ACS user database. Fingerprint, hand geometry, and iris scanning are the predominant biometric modalities used within DoD. Individual biometric characteristics are stored in a device's memory or on a card, from which stored reference data can be analyzed and compared with the presented biometric at the reader. A one-to-many (identification) or a one-to-one (verification) comparison of the presented template with the stored template can be made, and access granted if a match is found (depending on the authorized security level). Verification mode generally provides faster transaction times but does require a user to present a credential or enter a code to cue a specific stored template for the one-to-one comparison. Verification is the preferred mode of operation for ACS biometric applications in DoD.

##### **4-4.3.1 Biological Measurements.**

Because of the potential differences in biological measurements made over time, the comparison of the current biological measurement with the stored template is not likely to result in a perfect match. Therefore, the algorithm allows for a small percentage of variation. While the allowed variation is small, it does raise the possibility of the two types of errors associated with ACS. The first is false rejection (commonly referred to as a Type I error), where the difference between the current biological measurement and the stored template is beyond the level of acceptable variation. The second is false acceptance (commonly referred to as a Type II error), where an individual's biological characteristic is sufficiently close to that of another individual, so access is incorrectly granted. While biometrics can introduce both types of errors, the most likely impact will be on the overall false rejection rate of an ACS. All ACS have some percentage of false positive (accept) alarm events, and ESS system designers must understand the issues and work to minimize their occurrence. From a logistics perspective, missions cannot be

accomplished if false rejection rates are high and authorized personnel are regularly unable to enter their workspace or facility.

For information about the different types of biometric technologies, see paragraph 4-6.8.

#### **4-4.4 Combining Entry Authorization Identifiers.**

A site's security can be significantly enhanced by combining two or more entry authorization identifiers, such as a biometric characteristic with a smart card with a PIN code. However, combining identifiers results in increased verification time and will decrease throughput rate. Throughput rate must be considered when making decisions about whether or not to use multiple identifiers. Another consideration in combining two identifiers is that a system can be required to use one identifier during lower risk times (such as during normally staffed times) and two identifiers (card + PIN) during higher risk periods (such as nights and weekends). The same philosophy can be applied for access control enhancement during times of heightened force protection threat levels.

#### **4-4.5 Selecting Entry Authorization Identifiers.**

The type of identifier (credential, PIN code, biometric attribute, or a combination thereof) that will be used needs to be determined early in the project. This determination will drive the specifications for entry devices required, and it will influence the layout of access control equipment at doors and other portals. The ESS designer must solicit user input concerning the level of identity assurance and type of identifier required at each portal or door.

### **4-5 OTHER ACS FEATURES.**

Other features to consider implementing as part of an ACS include anti-passback, anti-tailgating, two-man rule, and event tracking. These are described in the following paragraphs.

#### **4-5.1 Anti-Passback.**

Anti-passback is a functional characteristic employed within ACS. It is used to eliminate/mitigate the risk of someone giving their credential (passing it back) to another person after that credential is used to access a secure area. Anti-passback requires that a person present a credential to enter an area or facility, and then again use the credential to "badge out." This makes it possible to know how long a person is in an area, and to know who is in the area at any given time. This requirement also has the advantage of instant personnel accountability during an emergency or hazardous event. In a rigid anti-passback configuration, a credential is used to enter an area and that same credential must be used to exit. If a credential holder fails to properly "badge-out," entrance into the secured area can be denied. Anti-passback is a standard software feature for commercial-off-the-shelf (COTS) ACS, but enabling this feature requires that every portal be equipped with two credential readers, one on the entry side and the other on the exit side.

An alternative approach to “badging out” that is not as rigid as the process described above is use of a time delay on entrance readers. In this design, the credential (card or PIN) cannot be reused within a prescribed minimum time period. This time delay feature can be programmed and set for a time period such as a half-hour. During the half-hour time period, the same card and/or PIN cannot be used for a second entry. While affording some increased security, this process is not as rigid or secure as a ‘badge-out’ process.

#### **4-5.2 Anti-Piggybacking/Anti-Tailgating.**

While not commonly required, a project may require anti-piggybacking/anti-tailgating devices and features to detect and deter piggybacking and/or tailgating. The difference between the two terms is that piggybacking implies that the person who has opened the door with their credentials knows that others are following them in through the secure door. Tailgating is the act of a person following another authorized person closely in order to gain ingress through the same portal without the knowledge of the person who has opened the door. An example of where anti-piggybacking/anti-tailgating features may be required is at standard pedestrian turnstiles. Standard turnstiles are easily defeated so mantraps, entry booths, or sally ports with anti-piggybacking / anti-tailgating features may be required. **Note:** Use of anti-piggybacking/anti-tailgating devices may slow down access and impact portal throughput rates.

#### **4-5.3 Two-Man Rule.**

The two-man rule is a strategy where two people must be in an area together, thus mitigating insider threats to certain critical areas. Two-man rule programming is optional with many ACS. It prevents an individual cardholder from entering a selected empty security area unless accompanied by at least one other person. Once two card holders are logged into the area, other card holders can come and go individually as long as at least two people are in the area. Conversely, when exiting, the last two occupants in the secure area must card out of the area one right after the other by presenting their cards to an exit reader. **Note:** Use of exit readers must be procedural only and cannot be required to prevent someone from leaving the area freely. The ability to freely egress the area must be maintained at all times regardless of the required exit procedures.

#### **4-5.4 Escort Feature.**

The escort feature is also optional with many ACS, and is similar to the two-man rule in that this feature can help enforce escort requirements. It prevents an individual cardholder (visitor) who may require an escort from entering or exiting an area unless accompanied by an authorized escort.

#### **4-5.5 Event Tracking/Event Logs.**

Event tracking/event logs are lists or logs of security events recorded by the ACS that indicate the actions performed and monitored by the system. Each event log entry contains the time, date, and any other information specific to the event. This feature

allows security personnel to query the ACS database based on specific portals, persons, or time periods of interest.

#### **4-6 ACS EQUIPMENT.**

Once the type of identifier, credentials, identity assurance levels, and other implementation strategies are determined, the ESS designer must identify the type of equipment necessary to implement all required system features. Various types of ACS equipment are available, as described in the following paragraphs.

##### **4-6.1 ACS Central Computer.**

The central computer is where the ACS application software and database reside and where all system activity is archived. For a small ACS, a single personal computer (PC) may be sufficient, but a large ACS may require one or more servers. A multi-server "cluster" configuration provides failover redundancy and ensures high availability for the ACS application software and database. The central computer, together with all distributed local processors, can be thought of as the "brain" of the ACS.

##### **4-6.2 ACS Workstation.**

An ACS workstation allows personnel to view and interact with the ACS hardware and software. The central computer can function as a workstation for small systems, but a large system will likely require multiple client workstations connected to the ACS server(s) via network. The required type, quantity, and location of all ACS client workstations must be identified early in the design process, recognizing that any computer with the appropriate network access and ACS software can function as a workstation.

##### **4-6.3 Badging/Enrollment Equipment.**

The CAC is the principal identity credential for supporting interoperable access to installations, facilities, buildings, and controlled spaces. Supplemental visitor or temporary badging may be required for certain controlled access facilities. Badging equipment may include:

- Credential encoding device (enrollment reader)
- Blank card stock (card technology must be compatible with FIPS 201 approved reader and reader configuration)
- Camera for capturing photographs of personnel
- Software for creating badge templates and images
- Biometric template capture device (where applicable)
- Badge printer capable of printing a color ID template on the front and back of the badge. There are new technology printers that are capable of

printing pseudo holograms on the clear protective laminate, which may be considered for higher security applications.

- ACS enrollment workstation for retention and programming of the security credential database. This computer may be a standalone or client workstation that is connected to the ACS server database in client/server architecture.

If there is no existing badging location and equipment, the design must include the badging/enrollment workstation infrastructure described above as well as space allocation for equipment and storage requirements. If there is an existing system, an interface to an existing personnel database where the necessary information is stored and maintained will be required. If so, requirements for this database interface and security must be established.

#### **4-6.4 ACS Local Controller / Control Panel.**

Local ACS control panels and their associated modules collect inputs from card readers, keypads, biometric devices, door sensors, and REX devices, and provide output signals to electronic door locks, electric door strikes, turnstiles, or gate operators. With its onboard microprocessor and memory, a local controller is able to process portal transactions even during periods when its connection to the central computer is down. This continuity is a major benefit of the distributed intelligence architecture employed by an ACS.

#### **4-6.5 Entry Devices.**

The most common device used for entry into a secure area is a card reader that may also have a keypad where two-factor authentication is required. There are a number of different types of card readers with varying card holder authentication capabilities.

##### **4-6.5.1 Contactless Card Reader.**

Contactless readers require that a user hold their card up to the face of the reader to gain entry. Contactless readers are generally considered more convenient for users when compared to requiring a user to insert their card into a card reader. However, contactless readers alone are not capable of providing a high level of assurance. Contactless-only readers are generally used to control access to general or low-security areas or to control access into individual rooms within a secure area once inside.

##### **4-6.5.2 Contactless Card Reader with Keypad.**

Contactless readers with keypads require that a user hold their card up to the face of the reader and the embedded keypad offers system owners the ability to also require a PIN to gain entry. For example, system owners may require the use of a PIN as a second factor (card + PIN) for entry after normal duty hours or during a higher Force Protection Condition (FPCON). Requiring a PIN as a second factor increases the identity assurance level. **Note:** Some contactless reader technologies do not support

Public Key Infrastructure (PKI) authentication and are not capable of providing a high confidence or very high confidence identity assurance level.

#### **4-6.5.3 Contact/Contactless Card Reader with Keypad.**

Contact/contactless card readers use a combination of the same contactless technology outlined previously with a contact or insertion type reader that may require the card holder to insert the card into a slot near the bottom of the reader in order to read the contact chip on the credential. Once a valid card read and PIN entry (if required) is completed, the card holder then removes the card to trigger the unlocking of the door. Most combination contact/contactless card readers come standard equipped with a keypad. Contact/insertion readers are generally considered less convenient for users when compared to contactless readers. This inconvenience factor, coupled with the mechanical wear associated with inserting cards, favors the selection of contactless readers over insertion readers. These types of readers are generally used where a High or Very High identity assurance level or PKI authentication is required.

#### **4-6.5.4 Contact/Contactless Card Reader with Keypad and Biometric Reader.**

Contact/contactless card readers with keypad and biometric reader use a combination of the same contact/contactless technology outlined previously with the addition of a biometric reader. The addition of the biometric reader allows for three-factor authentication (card + PIN + bio). The card holder inserts their card, enters their CAC PIN, then presents their fingerprint for comparison to the print template stored on the card or within the ACS database to gain entry. These types of three-factor-capable readers are generally used where very high confidence level of identity assurance is required or warranted.

#### **4-6.6 Card Types.**

Card readers use a number of different card types, the most common of which are described in the following paragraphs.

##### **4-6.6.1 Common Access Card.**

The CAC is a credential used by DoD to allow access to DoD computers and physical locations worldwide. For each individual, one card works for all access to computers and physical locations. The CAC is a Java-based smart card. It can store a number of personal demographic data elements. It supports multiple tokens and methods for validation/authentication from a simple free read of the Federal Agency Smartcard Number (FASC-N) or CHUID, which is equivalent to a standard Wiegand proximity card base system and provides Little or No Confidence regarding identity assurance levels, all the way up to validation of the PIV authentication digital certificate which when used in combination with PIN or a biometric offers a Very High level of confidence assurance level. These multiple tokens resident on a single card make the card extremely versatile.

Per DoD 5200.08-R, *Physical Security Program*, "...the CAC must be the principal identity credential for supporting interoperable access to installations, facilities, buildings, and controlled spaces." For physical access control, the contactless smart chip is the preferred feature of the CAC. However, a dual-technology smart card reader allows the contact interface to be used (via insertion) as a fallback if the contactless antenna in a card become damaged.

#### **4-6.6.2 Smart Cards.**

Contractors, personnel, and visitors who are not issued a CAC or other federal PIV card are often issued a "CAC-like" smart card to gain access to a restricted area when authorized. The term "smart card" is commonly used to describe cards with integral microprocessing and read/write data storage capability. A principal security advantage of smart cards is that cryptographic capabilities can be used to send card information to legitimate readers and encrypts that transmission such that the system remains immune from replay attacks. It is difficult to clone or copy security credential information onto a forged card. For more information on the federal standard for electronic smart cards, refer to NIST FIPS 201. Smart cards are available as a "contact" type or as a "contactless" (and wireless) type. An example of a contact smart card is one that can interface to a computer through the embedded contact. The contactless, wireless smart card operates at 13.56 MHz, which is more than a hundred times faster than the data exchange rate of 125 kHz proximity cards. There are also hybrid cards available, which have both types of smart card chips in one plastic body or have both contact and contactless interfaces to one microprocessor in the plastic body. Smart cards can also store data such as access transactions, licenses held by individuals, qualifications, safety training, security access levels, and biometric templates.

#### **4-6.7 Keypads and PIN Codes.**

Coded devices use a series of assigned numbers commonly referred to as a PIN. This series of numbers is entered into a keypad and is matched to the numbers stored in the ACS. By itself, this technology does not offer a high level of security since a PIN can be stolen by even casual observation. However, coded devices can be effective when used in combination with a credential or biometric technology. For an ACS that uses keypads as the sole entry authorization identifier, microprocessor-controlled or scramble-type keypads are preferred. Unlike a standard keypad, a scramble-type keypad alters the arrangement of numbers each time it is used, thereby making it more difficult for an onlooker to determine a PIN by observing which keys are pressed. Numbers are displayed on LEDs with a narrow viewing angle so that only the person directly in front of the keypad can clearly see the numbers.

#### **4-6.8 Biometric Readers.**

Biometric readers verify specific personal biological metrics (biometrics) of an individual. Biometric readers may be used in addition to credential devices or with a PIN code. Biometric readers are well suited for very high security areas but may not be

appropriate for portals where high throughput is a primary design objective. Designers must evaluate the tradeoff between added security and decreased throughput.

There are several types of biometric characteristics that can be used. The most common are described in the following paragraphs.

#### **4-6.8.1 Fingerprint.**

Fingerprint technology scans the loops, whorls, and other characteristics of a fingerprint and compares it with stored templates. When a match is found, access is granted. This technology is mature and well understood but performance can be degraded if cuts or sores appear on fingers or if grease or other medium contaminates the fingers and the scanning plates. Some systems create two templates for two different fingers, in the event that one finger is altered by injury or other means. Fingerprint technology is not convenient in environments where workers wear gloves. Early fingerprint readers were compromised by picking up a valid fingerprint from a reader with a manufactured "finger." To combat this shortcoming of the technology, sensors were equipped with the ability to sense a pulse and temperature. Fingerprint technology is the first-choice biometric method per FIPS 201.

#### **4-6.8.2 Facial Recognition.**

This technology measures the geometric properties of the subject's face relative to an archived image. Specifically, the centers of the subject's eyes must be located and placed at precise (within several pixels) locations. Facial imaging is the backup technology for biometric authentication per FIPS 201.

#### **4-6.8.3 Hand Geometry.**

This technology assesses the hand's geometry: height, width, and distance between knuckle joints and finger length. Advantages of hand geometry are that the systems are durable and easily understood. The speed of hand recognition tends to be more rapid than fingerprint recognition. Hand recognition is reasonably accurate since the shape of each hand is unique. A disadvantage is that they are not approved for use under the FIPS 201 Evaluation Program and tend to give higher false acceptance rates than fingerprint recognition. As with fingerprint technology, hand geometry is not convenient in environments where workers wear gloves.

#### **4-6.8.4 Iris Patterns.**

Iris recognition technology passively scans or captures the unique pattern of the iris. Iris readers do not "actively scan" like old retinal technology. Iris readers basically capture an image of the iris and compares the individual's unique iris pattern with stored iris templates. Iris scanning is the most accurate and secure biometric. After DNA, irises are the most individualized feature of the human body. Even identical twins have different irises, and each person's two irises differ from each other. The unique pattern of the human iris is fully formed by ten months of age and remains unchanged through a person's lifetime. A benefit of iris recognition is that it is not susceptible to theft, loss, or

compromise, and irises are less susceptible to wear and injury than many other parts of the body. Iris scanners allow contactless scanning to occur from up to 16 inches (406 millimeters) away. A disadvantage of iris readers is that they are currently not approved for use under the FIPS 201 evaluation program and some people are reluctant to have their eye scanned. Throughput rate for this technology must be considered. Typical transaction time is two seconds. If a number of people need to be processed through an entry portal in a short period of time, this can be problematic.

#### **4-6.9 Mobile PIV Certificates.**

The ACS industry, in partnership with the government, is working on what is referred to as a derived PIV. A derived PIV is a digital credential that can be loaded on a mobile device and used for both physical and logical access just like the CAC. Approval and implementation standards are outlined within FIPS 201 update.

Modern ACS currently have the ability to allow access to facilities utilizing a digital certificate stored on an individual's personal device like a smartphone or smart watch. However, due to the inherent information security risks associated with wireless communications technologies, these devices are not allowed inside secure areas that may contain or process classified information.

#### **4-6.10 Locking Devices.**

##### **4-6.10.1 Electric Locks.**

The electric lock is a very secure method to control access at a door. An electric lock actuates the door bolt/latch. In some cases, power is applied to release the handle, so the user can retract the bolt vice the electric operator actually retracting the bolt/latch. Most electric locks may have built-in latch position and/or REX switches; however, these switches are typically not a standard feature, often having their own part number, and must be special ordered with the lock set or exit hardware. In addition to the electric lock itself, a special door hinge and internal REX switch are required. Electric locks can be configured for fail-safe or fail-secure operation.

##### **4-6.10.2 Electric Strikes.**

The difference between an electric strike and an electric lock is the mechanism that is activated at the door. In an electric lock door, the bolt is moved. In an electric-strike door the bolt remains stationary and the strike (or cover latch) is retracted. As in electric locks, electric strikes can be configured for fail-safe or fail-secure operation. The logic is the same. In fail-safe configuration the strike retracts when de-energized on loss of power. This allows the door to be opened from the public side. In fail-secure configuration the strike remains in place, causing the door to be locked from the public side and requires manual key entry to unlock the door from the public side. Again, as with electric locks, unimpeded access is allowed in the direction of egress by manual activation of the door handle/lever when exiting from the secure side. For retrofit

situations, electric strikes rarely require door replacement and can often be done without replacing the doorframe.

Using cover guards to protect electric strikes increases security by reducing the risk of tampering. Exposed electric strikes can be over-ridden (pried open) by an intruder with a pocketknife or screwdriver.

#### **4-6.10.3 Magnetic Locks.**

The magnetic lock is popular because it can be easily retrofitted to existing doors. The magnetic lock is surface-mounted to the door and doorframe. Power is applied to magnets continuously to hold the door closed. Magnetic locks are normally fail-safe, which may be a problem for unstaffed facilities in that a power disruption will leave the site unsecured until security personnel arrive or power is restored. Magnetic locks are the designer's last choice for door locking mechanisms.

Magnetic locks do have a security disadvantage. In the United States, life safety requirements generally favor the use of a PIR sensor as the primary REX device for doors equipped with magnetic locks. While enhancing overall building safety, this configuration in which a REX PIR sensor is mounted above the secure side of the door allows possible compromise of the magnetic door lock in the following scenario:

- Person A is on the secure side and walks past the door, activating the REX PIR with no intent to exit.
- The magnetic lock is released by the activation of the REX PIR sensor. This activation generates a "click" sound.
- Person B is on the public side of the door and, upon hearing the "click," opens the unlocked door and enters the secure area.

#### **4-6.10.4 Integrated Electronic Lockset (IEL).**

IELs include a keypad, card or biometric reader or a combination of these entry devices, a door position switch (DPS) or latch monitor, and a REX signaling switch, all integrated into a single locking hardware set or a group of these devices all integrated with the door. These newer integrated locksets come in both wired and wireless models. The use of an integrated-style lockset for access control is increasing due to the reduced amount of ACS cabling and conduit infrastructure required to equip a door.

**Note:** Consider FIPS 201 approved card readers or biometric devices used on these IEL components. IEL door hardware compatibility with a FIPS compliant ACS is limited based on the IEL manufacturer's reader design.

#### **4-6.11 Request-to-Exit (REX) Devices.**

Doors and other portals secured with an ACS must provide a means of authorized egress for personnel inside the controlled space. A REX device performs this function by initiating a temporary shunt of the door sensor alarm, thus allowing the ACS to

distinguish between an authorized exit and an unauthorized (forced) entry. For some door configurations, the REX device also releases the door locking/latching mechanism.

An ACS designer must work closely with the security manager and project architect to analyze each controlled door and portal to determine the appropriate electronic locking hardware and REX device, considering security, life safety, ABA, aesthetics, ergonomics, and wiring. An overview of the four categories of REX devices follows.

#### **4-6.11.1 Door Exit Hardware.**

Practically any type of door hardware can be equipped with an internal REX switch. This approach eliminates the need for an external REX device but requires that wiring be extended to the door either through an electrified hinge or exposed armored flex conduit. Use of door hardware with an integrated REX switch is preferred on new construction and on major renovations where doors and/or door hardware are being replaced. REX switches installed inside the exit hardware are preferred on door(s) equipped with magnetic locks. The exit hardware REX switch(s) must be wired properly to physically cut power to the magnetic lock(s) as well as integrate with the ACS to shunt the door alarm.

#### **4-6.11.2 Buttons.**

A button labeled "PUSH TO EXIT" may also be used as a REX device. Exit buttons are typically mounted on the door frame or an adjacent wall on the secure side. Push-to-exit buttons may be used on doors that utilize magnetic locks and, like exit hardware, the button must be wired properly to physically cut power to the lock directly. Push-to-exit buttons are typically used in conjunction with motion sensors (see paragraph 4-6.11.3) to ensure compliance with life safety requirements.

#### **4-6.11.3 Motion Sensors.**

A motion sensor can be mounted above the door to detect a person approaching from the secure side. This is generally considered to be the least secure REX device due to the potential for false activations or manipulation techniques.

Magnetic locks do have a security disadvantage. In the United States, life safety requirements generally favor the use of a PIR sensor as the primary REX device for doors equipped with magnetic locks. While enhancing overall building safety, this configuration in which a REX PIR sensor is mounted above the secure side of the door allows possible compromise of the magnetic door lock in the following scenario:

- Person A is on the secure side and walks past the door, activating the REX PIR with no intent to exit.
- The magnetic lock is released by the activation of the REX PIR sensor. This activation generates a "click" sound.
- Person B is on the public side of the door and, upon hearing the "click", opens the unlocked door and enters the secure area.

#### **4-6.11.4 Card Readers, Keypads, and Biometric Devices.**

Using a card reader, keypad, or biometric device as a REX device offers the potential for “who’s in and who’s out” accountability. **Note:** Requiring the use of an exit reader, keypad, or other device alone upon exit must be procedural only and may not prevent free egress.

#### **4-6.12 Door Position Monitoring Devices.**

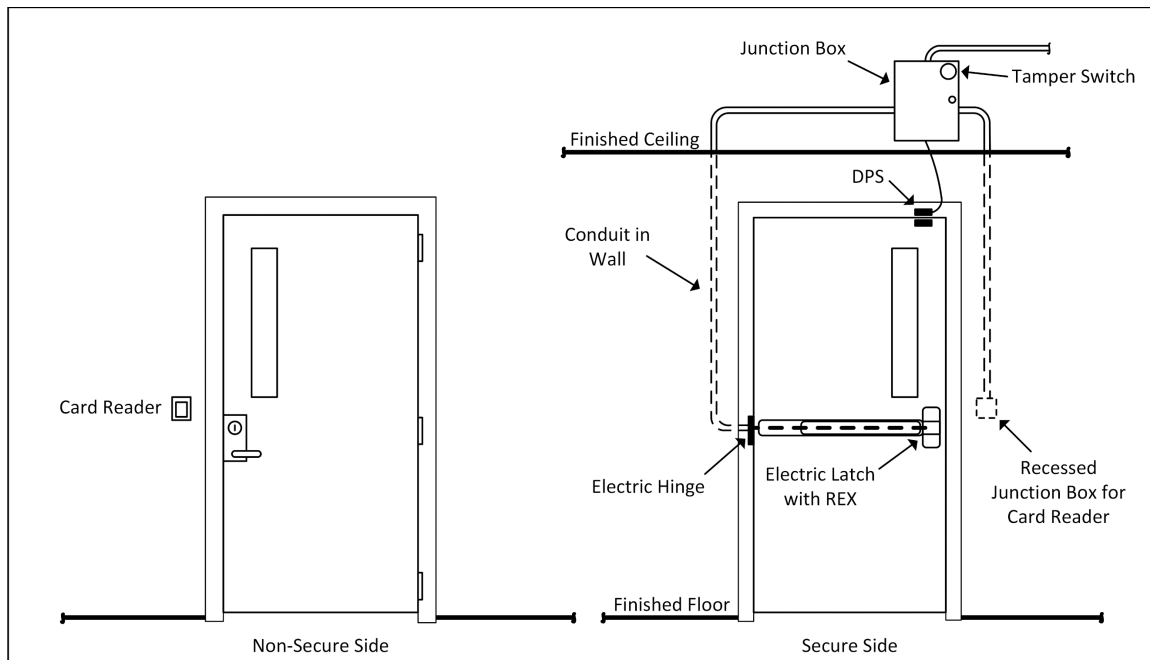
In order to establish an effective ACS, the position of all access controlled and secure area perimeter doors, including emergency exit doors, must be monitored. Door position switches (door contacts) must be UL 634-listed or -certified Level 1 or Level 2 HSS. The type of switch will depend on the minimum level of security required to protect the asset(s) within the secure area. For example, doors leading into a general administrative low-security area may only require a simple switch that is UL 634 listed, whereas doors into Secret areas or arms storage rooms require a minimum of a UL 634 certified Level 1 switch. Doors leading into a SCIF/SAPF require a minimum of a UL 634-certified Level 2 switch.

Secure areas requiring both IDS and an ACS may utilize a DPDT door contact that reports to both systems to monitor the door position without the use of two separate devices. Where IDS and ACS require physically and logically separate, use two separate devices.

#### **4-6.13 Access Controlled Door Configuration.**

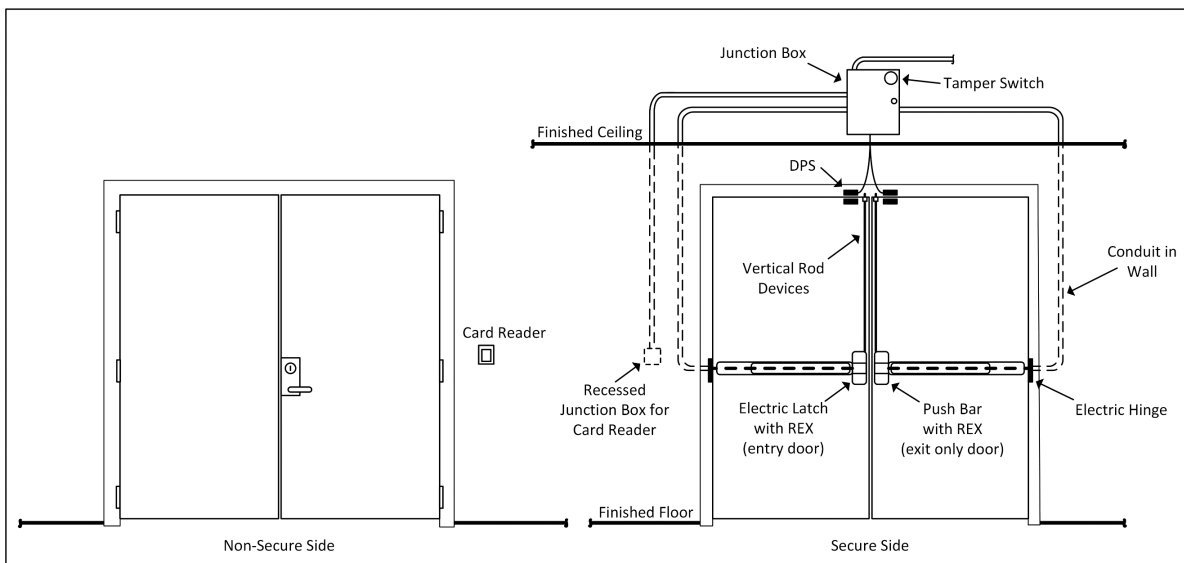
Figure 4-2 provides a typical configuration for a single door equipped with a card reader and electric lock. Figure 4-3 provides a typical configuration for a double door equipped with a card reader and electric locks. Figure 4-4 provides a typical configuration for an exit-only double door equipped with monitored DPSs. Refer to Chapter 10 for additional information on door hardware types and interface considerations. There are exceptions to this configuration for SCIFs and SAPFs. Access control door hardware configuration and infrastructure must be approved by the accrediting official (AO).

**Figure 4-2 Sample Access Controlled Door Configuration (Single Door)**



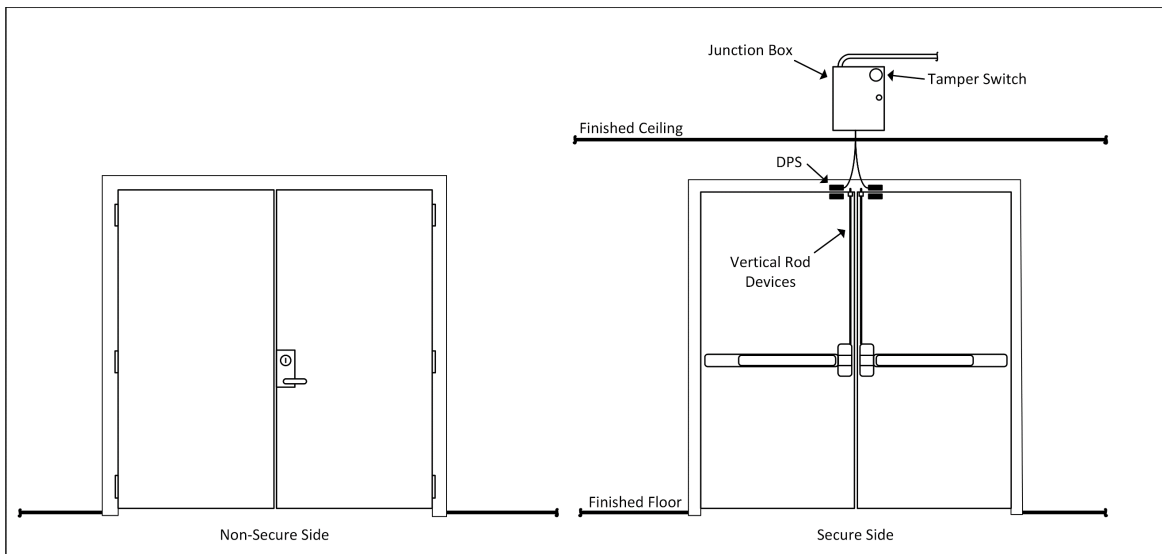
**Single Door with Push Bar with REX Switch in Push Bar**

**Figure 4-3 Sample Access Controlled Door Configuration (Double Door)**



**Double Door with Vertical Rods and Push Bar with REX Switch in Push Bar**

**Figure 4-4 Sample Access Controlled Door Configuration (Exit-Only Double Door)**

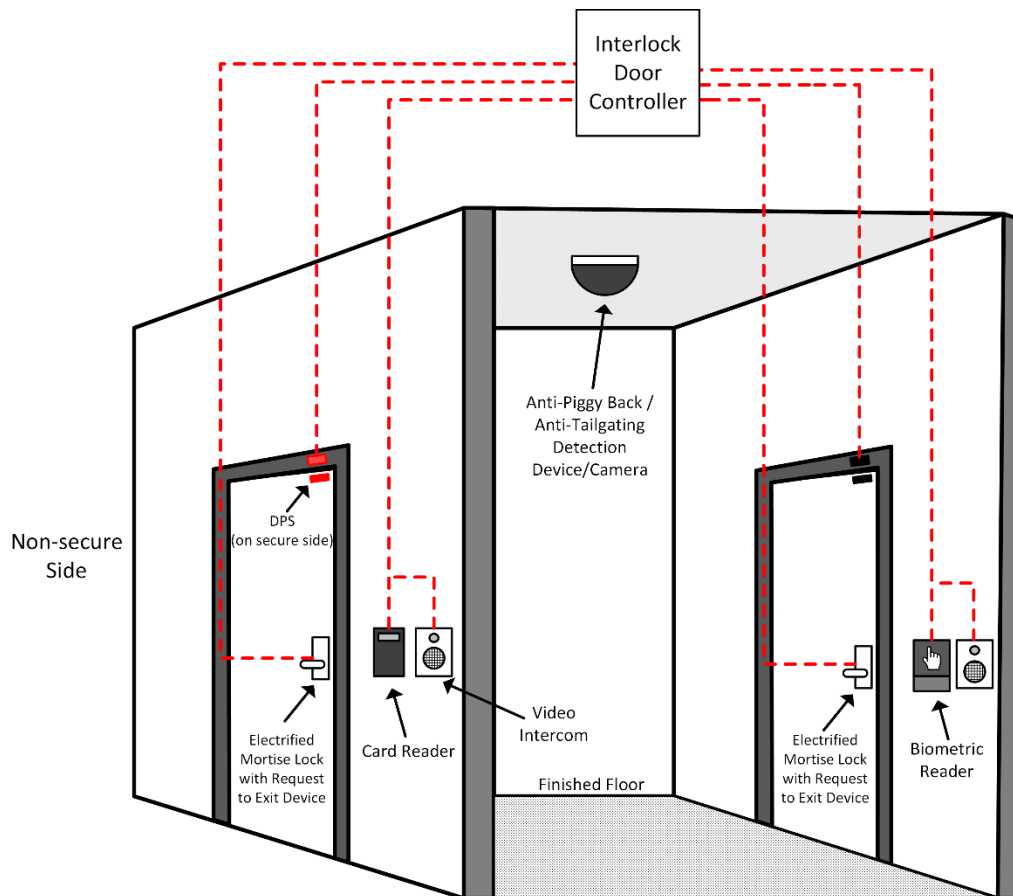


**Exit Only Double Door with Vertical Rods with Monitored Balanced Magnetic Switches**

#### 4-6.14 Typical Access Controlled Booth / Sally Port Configuration.

Figure 4-5 provides a typical configuration for what is often referred to as a mantrap, entry booth, or sally port, where two-factor authentication is required, and anti-piggybacking / anti-tailgating devices are employed. A card holder authorized to enter the area would present their credential at the outer reader first to open the outer door. Once inside, and the outer door is closed and secured, the user would enter a PIN or present a biometric to access the inner door. The inner door would only open if the outer door is secured, the second factor matches, and the system's anti-piggybacking/anti-tailgating detection device(s) are not triggered. **Note:** The inner and outer doors cannot use the same identifier. Equip mantraps, entry booths, and sally ports with a video intercom system monitored by security personnel who can assess the situation and render assistance to the user if needed and manually override the inner door to allow access when authorized.

**Figure 4-5 Sample Access Controlled Booth / Sally Port Configuration**



#### **4-7 ACS DESIGN CONSIDERATIONS.**

There are several questions that must be answered early in any ESS project.

- Work with the end user/customer and/or utilize regulatory guidance to identify restricted area boundaries and determine what level of identity assurance is required to gain entry into each and every access-controlled door/portal. Define the minimum and maximum level of identity assurance level that is required or may be required for each door, gate, and portal, and include those details in the requirements documents and on the security door hardware schedule.
- Work with the project architect to clearly define access-controlled boundaries and required door hardware components early in the design process. Specify the entry and exit function of each access-controlled door/portal and identify any special portal equipment such as turnstiles and security booths. Ensure that the Life Safety Plan addresses any egress restrictions associated with the ACS.

- Work with the project architect and local designated fire protection engineer (DFPE), as defined in UFC 3-600-01, *Fire Protection Engineering for Facilities*, to address life safety requirements for special design features and door hardware for entry doors that require the use of combination locks that meet Federal Specification FF-L-2740B, *Locks, Combination Electromechanical*, and the use of pedestrian door deadbolt devices approved under Federal Specification FF-L-2890C, *Lock Extensions (Pedestrian Door Lock Assembly Preassembled, Panic and Auxiliary Deadbolt)*.
- Work with the project architect and end-user to address the role of "exit only" and "emergency exit only" doors in controlling access. Although not used for entry, monitoring exit-only doors is important to the design of an effective ACS.
- All ACS hardware, software, and card readers must be UL 294 listed and FIPS 201 approved. Refer to <https://www.idmanagement.gov/fips201/> and ACS components for a list of approved products.
- Card readers located in non-environmentally controlled locations may require special exterior housings, shrouds, or seals. Most manufacturers offer what is often referred to as an outdoor kit for exterior applications. Refer to manufacturer's specifications and/or best practices for external applications.
- A common cable type for card readers is a twisted, shielded cable (typically, eight conductor). One pair is used for low voltage DC power, one pair is used for data transmission, one pair is normally used for LED or signal illumination, and one pair is used for tamper protection. Verify the cable requirements with the equipment manufacturer.
- In general, the ESS designer must balance security requirements with life safety, fire-alarm interface, and normal operational convenience factors.
- Avoid using a life safety emergency exit as a high security entry portal.
- Limit the number of entrances into access-controlled areas. Secure areas like SCIFs, SAPFs, arms rooms, and armories are examples of areas typically limited to one primary entrance.
- Coordinate with the architect to ensure proper doors, door frames, and door hardware are provided. For example, when an electric door strike is specified, the door frame and hardware must be checked or specified such that they are compatible with the strike in terms of wiring and latching.
- Consider throughput and traffic flow of normal operational traffic and emergency evacuation requirements. Ensure that entry throughput at controlled portals will be adequate for the morning surge period.

*This Page Intentionally Left Blank*

## CHAPTER 5 VIDEO SURVEILLANCE SYSTEM

### 5-1 OVERVIEW.

The VSS is another core subsystem of an overall ESS. It is the collection of cameras, storage media, switches, keyboards, and monitors that allow viewing and recording of security events. The VSS can be integrated with ACS and IDS and may be centrally monitored at the central monitoring station or locally monitored by security personnel at an individual facility. The use of VSS for security services includes several different functions as described below. Configure the VSS with products that comply with the Open Network Video Interface Forum (ONVIF) *Core Specification V2* standard in order to provide standard interfaces and interoperability of Internet Protocol (IP) -based products. The procurement of VSS components must comply with Federal Acquisition Regulation (FAR) 52.204-25, *Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment*.

#### 5-1.1 Alarm Assessment.

When alerted by an alarm notification, video cameras allow security personnel to visually assess the situation and decide what type of response may or may not be required. An example would be an intrusion alarm at a remote facility. Visual assessment and other confirmation may indicate an unannounced maintenance crew at work. Assessment of the intrusion would lead to an appropriate response.

#### 5-1.2 Access Control.

Cameras can be used by security personnel to visually identify persons and/or vehicles requesting entry prior to releasing a controlled portal (such as door, turnstile, gate, and vehicle barrier).

#### 5-1.3 Surveillance.

Video cameras can be used to give security personnel the capability to be made aware of or view visual events at multiple locations from a centralized remote viewing area. Video camera technology makes visual information available that would normally only be available through multiple (possibly roving) human resources. Video analytics can significantly enhance surveillance effectiveness by cuing scenes of interest and highlighting areas within scenes for priority viewing by an operator.

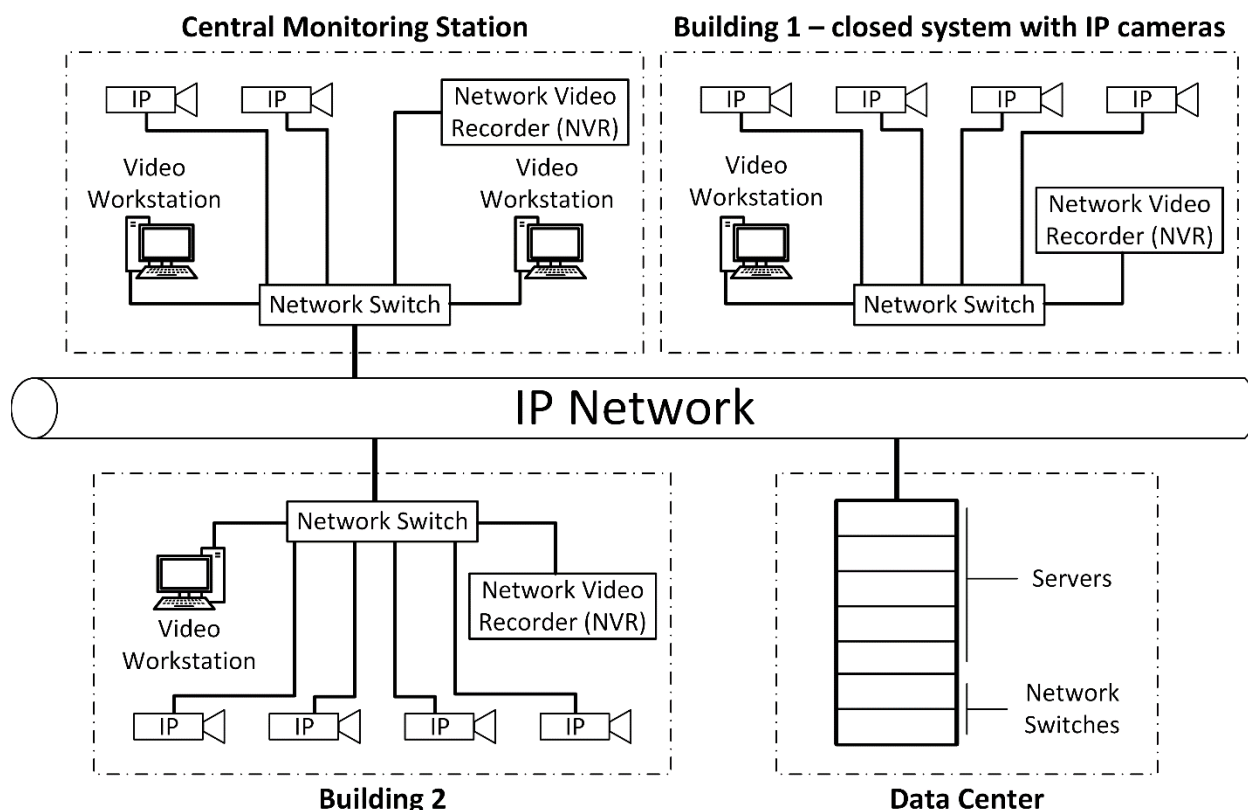
#### 5-1.4 Evidentiary Archives.

Retrieval of archived images may be helpful to identify or prosecute trespassers, vandals, or other intruders.

As shown in Figure 5-1, a large network VSS may encompass several buildings and can include multiple workstations where live and recorded video can be viewed. IP cameras gather video images that are stored in a digital format. Building 1 represents a

closed system with no connection to an outside network, in which case all video recording, viewing, and management is done within the building.

**Figure 5-1 Example Block Diagram for a VSS**



**Note:** A network switch may not be required on smaller systems. The cameras and video workstation could be connected directly into the NVR.

## 5-2 CAMERAS.

Selecting the appropriate camera type is critical to a VSS design. Another important consideration is to select the camera housing or enclosure based on the environment in which the camera will be installed. For example, a vandal-resistant housing may be appropriate for facilities where the risk of physical damage is high. The following paragraphs provide guidance regarding basic camera types and features.

### 5-2.1 Network Camera.

A network camera is often referred to as an IP camera. As shown in Figure 5-1, an IP camera connects directly to an Ethernet switch from which the camera signal can be transmitted to any network node for viewing or recording. To ensure reliable video storage and viewing, IP cameras generally require a network with high bandwidth, high availability, and low latency. IP cameras utilize bi-directional communication, allowing data to be sent and received over the video network via an integrated Ethernet

interface. Most IP cameras are Power over Ethernet (PoE), meaning that both power and data are supported via the Ethernet interface subject to the PoE distance limitation of 328 feet (100 meters) and the PoE power budget of the supporting network switch. A midspan, or power injector, is a device that can be installed between the network switch as an additional power source if the network switch is at capacity or does not support PoE.

A network camera is an intelligent device that has the ability to communicate over the network and provide status information. Some cameras are equipped with built-in inputs that can accept alarm input from other devices. Video communication loss is also a feature that can be reported over the video network by the camera.

### **5-2.2 Indoor Cameras.**

Indoor camera installations reduce the complexity of the system, but care must be taken to correctly specify the lens, field of view (FOV), and camera hardware. Indoor cameras need:

- Sturdy, secure mounting
- Auto-iris for lighting control
- Auto-white balance to ensure proper color correction to accommodate changes in color temperature of lighting if it is dimmed or lighting is changed due to a light outage
- To be mounted in a position to prevent glare from overhead lighting

### **5-2.3 Outdoor Cameras.**

Outdoor camera installations cost more than indoor cameras due to the need to environmentally house, heat, and ventilate the outside camera. When mounting a camera outdoors, the lighting requirement changes depending on the time of day and the weather. Because of this, consider the following for outdoor cameras:

- Shrubs, trees, and other vegetation in a camera's line of sight may cause obstructed views. Designers need to be aware of this when determining where to place cameras. Also, video motion detection systems can register a false positive when plants in the FOV move in windy conditions.
- Provide heaters in cold weather applications.
- Always use auto-iris lenses with outdoor cameras. The iris automatically adjusts the amount of light reaching the camera and thereby optimizes its performance. The iris also protects the image sensor from getting damaged by strong sunlight. Always set the focus in low light with an auto-iris lens. If the adjustment is made in sunlight, it is very easy to focus, but at night the iris diameter increases, and the image is not in focus anymore. Special dark focus filters called neutral density (ND) filters help reduce

lighting by one or more stops of exposure. These filters do not affect the color of the image.

- Use caution when mounting a camera behind glass. If you mount a camera behind glass, such as in the camera enclosure, make sure that the lens is positioned close to the glass. If the lens is too far away from the glass, reflections from the camera and the background will appear in the image.
- Always try to avoid direct sunlight in an image. Direct sunlight blinds the camera and may permanently bleach the small color filters on the sensor chip, causing stripes in the image.
- When using a camera outdoors, avoid viewing too much sky. Due to the large contrast, the camera will adjust to achieve a good light level for the sky, and the landscape and objects that must be assessed might appear too dark. One way to avoid these problems is to mount the camera high above ground. Given mounting choices, mount cameras facing away from the rising or setting sun, realizing that this varies by season.
- Always use sturdy mounting equipment to avoid vibrations caused by strong wind. This is especially important with a long focal length lens. These lenses amplify even the smallest movement of the camera. Building mounts are generally more stable than pole mounts. When in extremely windy conditions for a critical camera, consider using a gyro-stabilized lens to avoid vibration caused by wind. The gyro-stabilized lens has a cost premium and is not appropriate for general applications.

#### **5-2.4 Fixed Position Cameras.**

After being mounted, aimed, and focused by an installer, a fixed position camera provides a FOV that cannot be changed via remote control. When used for visually assessing intrusion or access control alarms, fixed cameras are good for review of pre-alarm conditions because there is a constant view of the scene in which the alarm was triggered. Pre-alarm allows the review of video information for the time period (typically ten to fifteen seconds) immediately before the alarm occurred. Pre-alarm video is often the most useful video content for determining the actual cause of the alarm. Because of their static FOV, fixed cameras are well suited for video motion detection but are not able to track a target of interest after it leaves the camera scene. The installation and cost of fixed cameras is lower because there is no associated motor and control wiring.

#### **5-2.5 Pan/Tilt/Zoom (PTZ) Cameras.**

A PTZ camera contains a motorized mechanism for adjusting camera aim point and lens focal length, thus allowing an operator to dynamically change the FOV via remote control. This gives the operator a much better view of the overall area compared to a fixed camera. PTZ cameras are often used for both alarm assessment and video surveillance applications; however, they are not well-suited for pre-alarm assessment because they may not be focused on the alarm area at all times. Because of the drive

motor, housing, and control mechanism, PTZ cameras are typically two to three times more expensive than fixed cameras. Table 5-1 compares other salient parameters of fixed and PTZ cameras.

A PTZ camera can be controlled by an operator or it can be programmed to perform a guard tour during which it moves sequentially through a series of user-defined preset views. When not under operator or guard tour control, a PTZ can be set to return to a home position preset corresponding to the most important scene of interest. Preset views for alarm conditions can be programmed to override operator control, guard tour, and home position.

**Table 5-1 Fixed Versus PTZ Cameras**

Camera	Applications	Cost	Pre-alarm Review	Video Motion Detection	Intruder Tracking Capability
<b>Fixed</b>	Alarm assessment for doors, gates, and fence lines	Lower	Recommended	Recommended	None
<b>PTZ</b>	Surveillance for large open areas such as ports and airfields	Three times more expensive than a fixed camera	Poor application	Only for fixed, preset scenes	Good

### 5-2.6 Dome Cameras.

A dome camera is mounted within a hardened plastic dome, which is commonly smoke-colored to conceal the camera. The use of smoke-colored domes provides covert lens positioning, while the use of clear domes provides for better low-light performance. Dome cameras are a good design solution for applications where the camera needs to be protected from the environment (such as dust) or it is desired to conceal the camera's aim point. The variety of dome cameras is extensive, giving the designer a dome option for nearly any security application: fixed or PTZ, indoor or outdoor, full-size or mini-dome. A common application of dome cameras is in office buildings with suspended ceilings where aesthetics and ease of installation are important factors. PTZ dome cameras can move quickly from a home position to any preset, typically in less than two seconds.

## 5-3 ILLUMINATION.

### 5-3.1 Illuminance.

The VSS designer must coordinate with the project's lighting engineer, landscape architect, and interior designer to ensure that illuminance within scenes of interest is sufficient for cameras to render full video. Meeting this objective involves analyzing two parameters, faceplate illuminance and scene illuminance, which are illustrated in Figure 5-2 and related in Equation 5-1.

#### Equation 5-1. Illuminance

$$C = BR\left(\frac{T}{4N^2}\right)$$

Where:

*C* = faceplate illuminance (units are foot-candles or lux)

*B* = scene illuminance (units are foot-candles or lux)

*R* = scene reflectivity factor (dimensionless number between 0 and 1)

*T* = lens transmittance efficiency (dimensionless number, typical value is 0.8)

*N* = lens f-number (ratio of lens focal length to aperture diameter)

To illustrate the use of this equation, consider the following example:

A specific outdoor fixed camera has been proposed for use at an aircraft parking area. The manufacturer's data reveals the camera requires 0.0007 foot-candle of illuminance at the faceplate to generate useable video. To achieve the desired FOV, a 5-mm lens with an f-number of 1.6 and transmittance efficiency of 0.8 is proposed. During a nighttime lighting survey, it is determined that the scene of interest includes dark-colored rotary-wing aircraft parked on asphalt concrete. The reflectivity factor for this scene is estimated to be 0.07. Noting that existing light fixtures are in place, light meter readings are taken at several locations within the scene and the average illuminance value is calculated to be 1.2 foot-candles. Using this average scene illuminance, faceplate illuminance is calculated as follows:

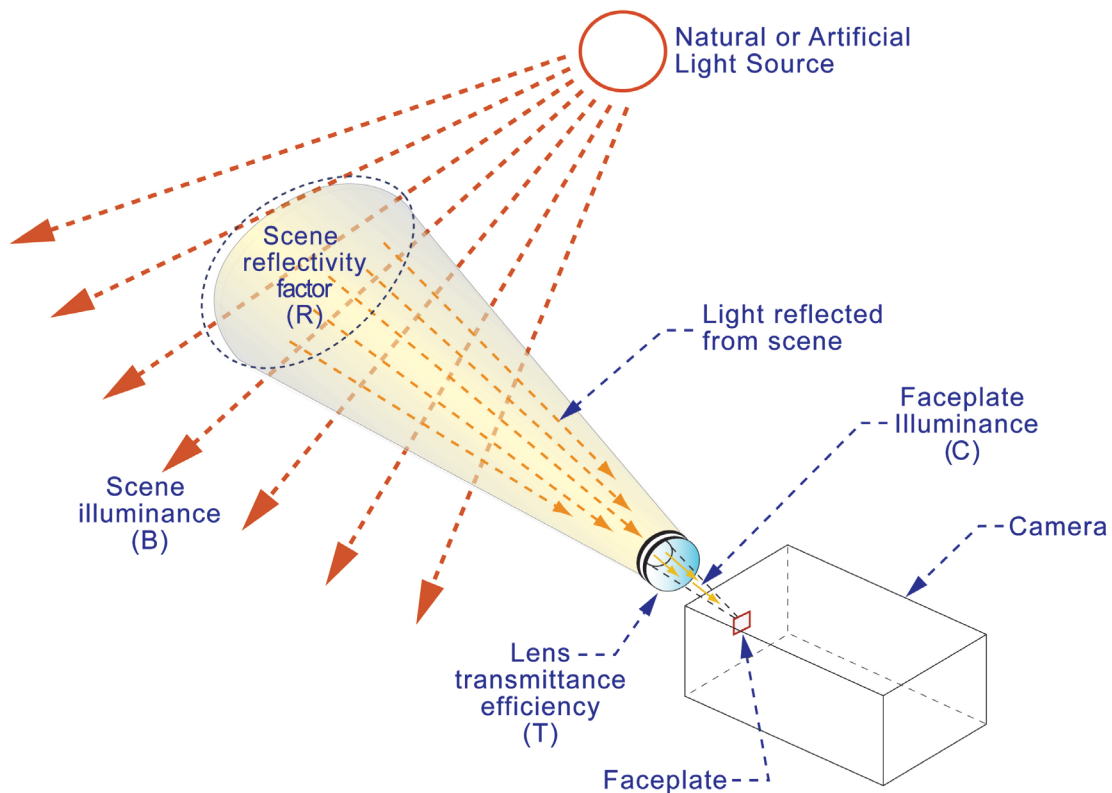
$$C = (1.2)(0.07) \left[ \frac{0.8}{(4)(1.6)^2} \right] = 0.007 \text{ foot candles}$$

Comparing this calculated value with the manufacturer's specification (0.0007 foot-candle) indicates that existing nighttime illumination at the aircraft parking area is more than adequate to support full video capture by the proposed camera.

### 5-3.2 Uniformity.

Uniform illuminance within a camera scene yields the highest video quality. While not always achievable, design for an average-to-minimum uniformity ratio no greater than 4:1 within a scene of interest. Video quality degrades noticeably when the uniformity ratio exceeds 8:1. For additional guidance on uniformity and other camera illumination parameters, refer to UFC 3-530-01, *Interior and Exterior Lighting Systems*.

**Figure 5-2 Scene Illuminance and Faceplate Illuminance**



Reflectivity factors for a range of surface conditions are presented in Table 5-2. These values can be used to estimate reflectivity for actual scenes of interest.

**Table 5-2 Reflectivity Factors for Various Surface Conditions**

Scene Description	Reflectivity Factor
Asphalt concrete	0.07
Grass and trees	0.2
Red brick	0.35
Portland cement concrete	0.4
White matte painted surface	0.6
Glass window or wall	0.7
Snow-covered surface	0.85

### 5-3.3 Glare Reduction.

Glare is very detrimental to camera performance, as illustrated in Figure 5-3. Glare reduction can be achieved by specifying full cut-off luminaires and ensuring that luminaires are not in a camera's FOV. In general, the source of illumination is best located above the level of the camera. The VSS designer must coordinate with the lighting designer to ensure these glare-reduction objectives are met.

**Figure 5-3 Effect of Glare on Camera Image Quality**



### 5-3.4 Dynamic Range.

Dynamic range is a term that refers to the range or ability of a video camera to capture the brightest and darkest areas of an image. Most modern cameras include a feature

known as wide dynamic range. This feature allows a video camera to accommodate both bright and dark conditions within a scene and provide a quality image.

### **5-3.5 Interior Lighting.**

Interior lighting for video presents special issues that need to be considered by the designer. For example, after-hours lighting may be significantly lower than normal operation lighting. Two solutions help minimize this impact.

- The first technique is the use of cameras with automatic backlight compensation. Backlight compensation is a camera feature that enables the camera to automatically adjust picture brightness depending on lighting conditions, which compensates for bright backgrounds so foreground objects are not silhouetted. Frequently, video cameras near windows are affected by backlighting, causing shadows and silhouettes, so the use of appropriate cameras with backlight compensation is effective.
- The second technique is the use of cameras with automatic gain control, a feature that amplifies existing video to help a camera create an enhanced video signal at low light levels.

Both of these techniques enable cameras to function more effectively in interior low-light conditions and are useful for outdoor cameras as well. In some cases, the integration of video cameras with night lights and intrusion sensors can be very effective. The sequence of events might be as follows: an intruder activates an interior presence sensor which, in turn, activates instant-on lighting for video camera assessment.

## **5-4 VIEWING IN LOW-LIGHT CONDITIONS.**

In addition to increasing the illumination level of the surrounding area, several technology solutions are available to permit viewing under low-light conditions. These include black/white switching cameras, IR illuminators, or thermal imagers. These technologies are often used where visible light either brings undesired attention to a critical facility or surrounding property owners object to visible light adequate for good visual camera operation.

### **5-4.1 Black/White Switching.**

Many cameras will automatically switch from color during daytime to black/white at night, which permits viewing under low light conditions. This can be an effective solution in situations where the existing illumination levels are too low during night conditions to permit color camera use but color camera use is desired during daytime conditions. Numerous camera manufacturers offer auto-switching black/white cameras.

### **5-4.2 Infrared Illuminators.**

The human eye cannot see IR light. Thus, invisible IR light from either an LED or laser source can be used to illuminate a scene, which allows night surveillance without the

need for additional artificial lighting. IR illumination patterns can be matched to the camera's FOV. A variety of patterns are available, ranging from narrow to wide-angle and short to long-range coverage. LED IR illuminators are a good choice for short-range flood coverage and medium-range spot coverage. Approximate coverage ranges for a 26-watt LED illuminator are 65 feet (20 meters) for a 120-degree flood pattern and 310 feet (95 meters) for a 10-degree spot pattern. Consider laser IR illuminators when the desired coverage range exceeds the capabilities of LED illuminators. For example, a 60-watt laser IR illuminator can project a 10-degree pattern to a maximum effective distance of approximately 2300 feet (700 meters). IR provides the following benefits over conventional lighting:

- Extended service life—up to 10 years.
- Lower running costs (but higher installation costs).
- Covert surveillance—no visible lighting to alert or annoy neighbors.

It is important to design illumination specifically for the video camera being used. Cameras used in conjunction with IR illuminators must have an automatic switching feature to go from color to black and white because cameras will not render color images when used under IR illumination. The range that the camera will see in the dark depends on sensitivity and spectral response of the camera and lens combination. Dual-mode cameras that can switch from color to monochrome operation in low light conditions must also automatically remove the IR filter, if equipped, for the reason cited above.

#### **5-4.3 Thermal Imagers.**

Thermal imagers use a special technology that senses heat signatures rather than visual information. These cameras operate under complete darkness. Thermal imagers are best used in long-range detection and surveillance applications. Thermal imagers detect and display images based on IR energy emitted from objects rather than visible light reflected off objects. The most common technology is forward looking infrared (FLIR). Thermal cameras work on a temperature differential between the object and the background. In desert environments, the background is white, and people are black. In cooler environments, the background is black, and people are shown as white images. A key advantage of long-range thermal imagers is that they are less susceptible to environmental influences from rain and fog in comparison to visible-light cameras. The disadvantage of thermal imagers is the high cost and the inability to discern facial features and other fine details in the scene.

Typically, thermal imagers are classified as medium or long wavelength, as illustrated in Table 5-3. For security applications in which the object of interest is a man-size target within a thousand feet (a few hundred meters) of the camera, uncooled long-wavelength imagers are preferred because of their lower cost, both in terms of initial purchase and lifecycle maintenance. Cooled medium-wavelength imagers, though more costly, can resolve very small thermal gradients and, equipped with the appropriate lens, can capture images of man-size targets at ranges out to 10,000 feet (3000 meters).

**Table 5-3 Characteristics of Thermal Imagers**

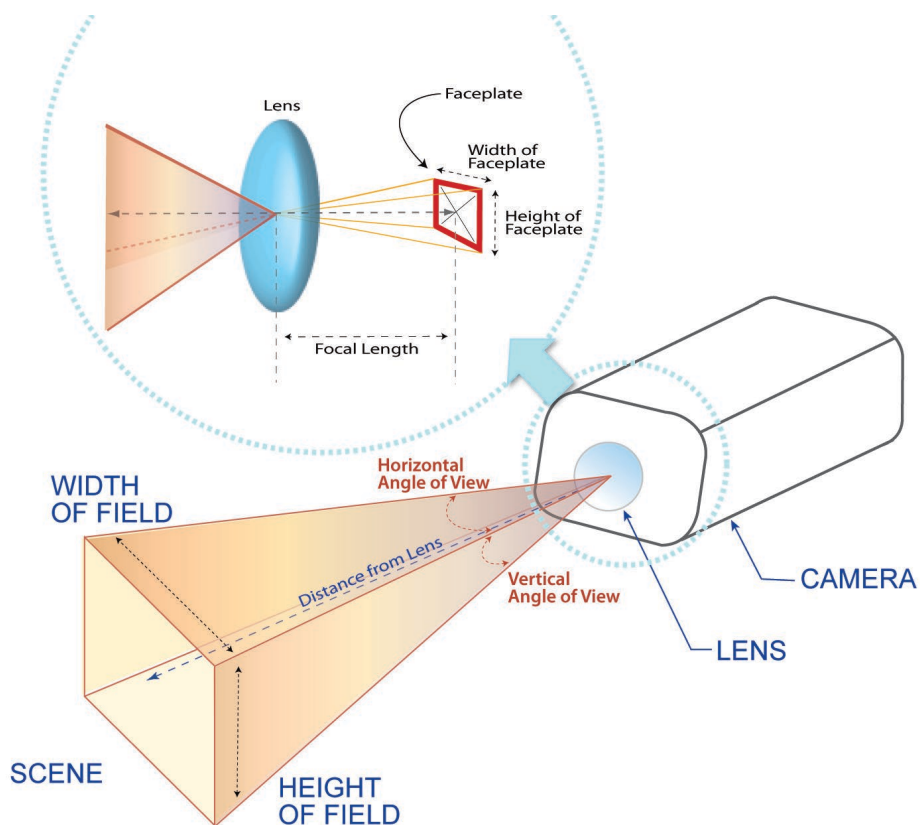
Classification	Wavelength	Cooling	Cost	Recommended Service Period
Medium wavelength	3–5 microns	Cryogenically cooled	\$50K–\$150K	7,500 hours
Long wavelength	7–14 microns	Uncooled	\$3K–\$50K	30,000 hours

## 5-5 ANGLE OF VIEW AND FIELD OF VIEW.

### 5-5.1 Field of View.

An important consideration when designing a VSS is determining the desired FOV for each camera. FOV and angle of view are illustrated in Figure 5-4. Based on the desired FOV, the designer must specify the appropriate camera mounting location, aim point, format, and lens focal length to capture the required image.

**Figure 5-4 Angle of View and Field of View**



### 5-5.2 Angle of View.

Camera format refers to the nominal diagonal measure of the image sensor (also called the faceplate) and typical sizes are shown in Table 5-4. Given the faceplate dimensions and the lens focal length, the angle of view for any camera–lens combination can be calculated as shown in Equation 5-2.

#### Equation 5-2. Angle of View

$$\alpha = 2 \tan^{-1} \frac{l}{2f}$$

Where:

$\alpha$  = angle of view (horizontal or vertical)

$l$  = length of image sensor (width or height; see Table 5-4)

$f$  = focal length of lens

A relatively narrow angle of view would be provided by a 2/3-inch format camera equipped with a 50-mm lens. In this example, the angles of view would be as follows:

$$\alpha_{horizontal} = 2 \tan^{-1} \left[ \frac{8.8}{(2)(50)} \right] = 10.1^{\circ}$$

$$\alpha_{vertical} = 2 \tan^{-1} \left[ \frac{6.6}{(2)(50)} \right] = 7.6^{\circ}$$

A relatively wide angle of view would be provided by a 1/3-inch format camera equipped with a 5-mm lens. In this example, the angles of view would be as follows:

$$\alpha_{horizontal} = 2 \tan^{-1} \left[ \frac{4.8}{(2)(5)} \right] = 51.3^{\circ}$$

$$\alpha_{vertical} = 2 \tan^{-1} \left[ \frac{3.6}{(2)(5)} \right] = 39.6^{\circ}$$

### 5-5.3 Field of View Calculations.

The following simple ratios shown in Equation 5-3 can be used to perform several types of FOV calculations.

#### Equation 5-3. Field of View Ratios

$$\frac{l_{width}}{W} = \frac{l_{height}}{H} = \frac{f}{D}$$

Where:

$l_{width}$  = width of image sensor

$W$  = width of field

$l_{height}$  = height of image sensor

$H$  = height of field

$f$  = focal length of lens

$D$  = distance from lens

To show the application of these FOV ratios, consider this example. A ½-inch format camera will be mounted on a pole located 30 feet (10 meters) from a pedestrian turnstile on the perimeter of an outdoor restricted area. If the desired vertical FOV is a full-height image of each person entering the restricted area, what lens focal length is needed? Assuming a 7-foot (2.13 meters) height of field at a distance of 30 feet (9.1 meters), lens focal length can be calculated as follows:

$$f = \frac{Dl_{height}}{H} = \frac{(9144)(4.8)}{2134} = 20.6 \text{ mm}$$

In this example, the designer could specify a varifocal lens to allow some fine tuning of the FOV during the installation process or later adjustment to meet a new FOV requirement. A 10 mm to 40 mm varifocal lens set at 20.6 mm would meet the stated objective of providing a full-height image of a person at the turnstile, but the same varifocal lens could be set to 40 mm to provide better facial detail or to 10 mm to cover an adjacent vehicle gate. Supporting calculations for these focal lengths are as follows:

$$H = \frac{Dl_{height}}{f} = \frac{(9144)(4.8)}{40} = 1,097 \text{ mm} = 3.6 \text{ feet (1.1 meters) (Better Facial Detail)}$$

$$W = \frac{Dl_{width}}{f} = \frac{(9144)(6.4)}{10} = 5,852 \text{ mm} = 19 \text{ feet (5.8 meters) (Cover Vehicle Gate)}$$

**Table 5-4 Typical Faceplate Sizes**

<b>Nominal Diagonal Measure</b>	<b>Actual Width</b>	<b>Actual Height</b>
1/4 inch	3.2 mm	2.4 mm
1/3 inch	4.8 mm	3.6 mm
1/2 inch	6.4 mm	4.8 mm
2/3 inch	8.8 mm	6.6 mm
1 inch	12.8 mm	9.6 mm

## **5-6 CAMERA RESOLUTION.**

### **5-6.1 Object Discrimination.**

Camera resolution refers to the “graininess” of images captured and transmitted by a camera and is expressed in terms of picture elements (pixels) for IP cameras. Table 5-5 correlates qualitative resolution descriptions to equivalent camera specifications for IP cameras. For each scene of interest, the VSS designer must determine the camera resolution required to achieve the desired discrimination level for objects in the scene. Visual target discrimination criteria developed by John Johnson in the 1950s, commonly referred to as the Johnson criteria and summarized in Table 5-6, can be used to analyze the impact of camera resolution on object discrimination for any given angle of view. These criteria are based on a 50% probability of accurate discrimination by a person viewing the camera image. The following example applies the Johnson criteria to illustrate the difference in object discrimination performance between a high-resolution camera and a megapixel camera.

**Table 5-5 Typical Camera Resolution Specifications**

Qualitative Description	Equivalent Camera Resolution Specification
High resolution	720 x 480 pixels
HD 720p (1 MP)	1280 x 720 pixels
Megapixel resolution	1,280 x 1,024 pixels
HD 1080p (2 MP)	1920 x 1080 pixels
3 MP	2048 x 1536 pixels
5 MP	2592 x 1944 pixels
4K (8 MP)	3840 x 2160 pixels

**Table 5-6 Object Discrimination Levels Based on Johnson Criteria**

Discrimination Level	Meaning	Pixels Required Across Minimum Dimension	Example
Detection	An object of a specified size is present.	2	An object with a minimum dimension of 5 feet (1.5 meters) in the vertical orientation is present in the scene.
Recognition	The class to which the object belongs can be determined.	8	The object is a vehicle, not people or animals.
Identification	The type of object within the class can be determined.	16	The vehicle is a sedan, not a truck, SUV, or van.

A 2/3-inch format camera with a 25-mm lens will be used to visually assess outdoor perimeter intrusion alarms along a restricted area. The camera will be aimed parallel to the fence line to view objects in the clear zone. The objective is for the camera to provide recognition level discrimination for a person crawling through the clear zone. This level of discrimination will allow a human crawler to be distinguished from objects of similar size such as animals and wind-blown debris. The minimum dimension for a human crawler is 12 vertical inches (305 millimeters) and applying the Johnson criteria suggests that this 12-inch (305 millimeters) vertical profile must be “painted” by 8 vertical pixels on the image collected by the camera. Given the properties of the

camera, lens, and object to be viewed, Equation 5-4 can be used to calculate the maximum range for “recognizing” the human crawler.

**Equation 5-4. Object Discrimination**

$$D = \frac{hfR_{vertical}}{p_{vertical}l_{height}}$$

Where:

$D$  = distance from lens to object

$h$  = height of object

$f$  = focal length of lens

$R_{vertical}$  = vertical resolution of the camera in pixels

$p_{vertical}$  = vertical pixels required on object

$l_{height}$  = height of image sensor

Converting the height of the human crawler from 12 inches to 305 mm and solving this equation yields the following result for a high-resolution (720 x 480 pixels) camera:

$$D = \frac{(305)(25)(480)}{(8)(6.6)} = 69,318 \text{ mm} = 227 \text{ feet}$$

A megapixel camera (1,280 x 1,024 pixels), by comparison, provides a maximum “recognition” range of:

$$D = \frac{(305)(25)(1,024)}{(8)(6.6)} = 147,879 \text{ mm} = 485 \text{ feet}$$

In this illustration, even though the angles of view are the same for both cameras (20° horizontal and 15° vertical), the megapixel camera has two times the effective range of the high-resolution camera.

## 5-6.2 Maximum Effective Range.

For objects having a minimum dimension equal to their width (such as a person walking), Equation 5-5 can be used in conjunction with the Johnson criteria to calculate maximum effective range.

### Equation 5-5. Maximum Effective Range

$$D = \frac{wfR_{horizontal}}{p_{horizontal}l_{width}}$$

Where:

*D* = distance from lens to object

*w* = width of object

*f* = focal length of lens

*R<sub>horizontal</sub>* = horizontal resolution of the camera in pixels

*p<sub>horizontal</sub>* = horizontal pixels required on object

*l<sub>width</sub>* = width of image sensor

## 5-7 VIDEO FRAME RATE.

Video frame rate is an important VSS design parameter that affects video transmission, storage, and display. A video frame rate of 30 frames per second (fps) is generally considered to be “full motion video” based on the Society of Motion Picture and Television Engineers (SMPTE) video standard. However, the transmission and recording frame rates for digital video can be set for a range of values between 1 and 30 fps, and some IP cameras and network video recorders support frame rates up to 60 fps. For most security applications, including alarm assessment and evidentiary archives, frame rates between 7 and 15 fps are fully adequate. Higher frame rates are appropriate for surveillance applications in which a smooth video stream is beneficial to the operator, especially when using a PTZ camera. Frame rates of 24 fps and higher will be perceived as “smooth” when viewed by an operator for extended periods of time. In most digital VSSs, transmission and recording frame rates can be programmed to automatically change in response to an external event such as an intrusion alarm or an internal video motion detection trigger.

## 5-8 DIGITAL VIDEO BANDWIDTH.

### 5-8.1 Bandwidth Calculations.

The VSS designer must coordinate closely with the appropriate network designer or administrator to ensure that network bandwidth will support digital video transmission. The designer must also coordinate with the video manufacturer and video management system (VMS) provider to get the most accurate calculations of bandwidth needed to ensure full understanding of how the system will work once implemented. This includes such factors as constant bitrate, variable bitrate, and what happens at the set limit (such as, is frame rate or resolution scaled back or both).

Most camera and VMS vendors can offer the VSS designer calculation tools to help determine the bandwidth requirements. Estimating bandwidth requirements using Equation 5-6 will aid in this coordination.

#### Equation 5-6. Bandwidth Requirement

$$b = krz$$

Where:

*b* = bandwidth required for a single video stream

*k* = network overhead factor, typical value is 1.4

*r* = video frame rate

*z* = average compressed file size of a single video frame

#### 5-8.2 Example.

The average file size for a single frame is dictated by the video resolution and compression, and typical values are given in Table 5-7. The following example illustrates the use of Table 5-7 and Equation 5-6.

Four IP cameras will be installed in an administrative building as part of an access control upgrade. One fixed camera will be installed at the main entry door and the other three fixed cameras will be installed at doors designated for emergency exit only. Each camera has megapixel (1280 x 1024) resolution and H.264 video compression. Video from the administrative building will be transmitted via network at 5 fps to a headquarters building for recording and viewing. How much network bandwidth is required to support these four cameras? Assuming that the main entry camera will have high scene activity, a single video frame will have an average compressed file size of 72 kB. The other three cameras will each have low scene activity and a corresponding file size of 36 kB. Using these file size values from Table 5-7, along with the specified frame rate of 5 fps, the following bandwidth estimates can be made, with the results expressed in units of megabits per second (Mbps):

Entry door camera:

$$b_{\text{entry}} = (1.4)(5)(72) = 504 \text{ kBps} = 4.03 \text{ Mbps}$$

Exit door camera:

$$b_{\text{exit}} = (1.4)(5)(36) = 252 \text{ kBps} = 2.02 \text{ Mbps}$$

Total for all cameras:

$$b_{\text{total}} = b_{\text{entry}} + 3b_{\text{exit}} = 10.09 \text{ Mbps}$$

(Note: 1 Mbps = 125 kBps)

Based on this calculation, the four IP cameras will require approximately 10 Mbps of network bandwidth to transmit video from the administrative building to the headquarters building.

**Table 5-7 Single-frame File Size for Various Resolution Values and Compression Schemes**

Resolution (H x V pixels)	Average Compressed File Size (kB) for a Single Video Frame				
	H.264 - Low Scene Activity	H.265 - Low Scene Activity	H.264 - High Scene Activity	H.265 - High Scene Activity	MJPEG - High Quality
720 X 480	12	9	24	18	60
1280 X 1024	36	27	72	54	180
1920 X 1080	50	38	100	75	250

## 5-9 DIGITAL VIDEO STORAGE.

The VSS designer must plan for digitally storing (i.e., recording) video from all cameras. Several technology options are available. The following paragraphs provide a brief overview of two of the most common video recording methods followed by an explanation of how to estimate video storage requirements.

### 5-9.1 Edge Storage.

Several camera models have the capability for onboard memory card storage, which allows video to be recorded at the edge of the VSS. This ensures uninterrupted recording even when the connection between the camera and the central system is lost. Edge storage capacity is typically more limited than network storage. An onboard secure digital (SD) card, for example, can have a capacity of up to 2 TB. The speed class of the SD card must also be considered. SD card speed class indicates the minimum write speed of the card, which is very important for capturing video. Selecting the proper speed class ensures the video can be written to the card in sufficient time. Use of memory cards must be verified by the manufacturer as applicable and optimized for the purpose needed.

### 5-9.2 Network Video Recorder.

A network video recorder (NVR) records digital video from multiple IP cameras and video encoders to one or more internal hard drives. NVR can be machines that are purpose built or can be off-the-shelf servers meeting manufacturer requirements with appropriate NVR software. The capacity and sophistication vary greatly within this category of video recording technology. A low-end NVR can record between 8 and 32 cameras with recording resolution typically no greater than HD 720 (1280 x 720). High-end NVR camera capacity is based on individual camera resolution, frame rate, average motion factor, bit rate, and camera codecs with capacities in the 32, 64, 128 and 512 range at HD 720 (1280 x 720). Advanced NVR can support multiple different camera

configurations at the same time. Hybrid NVR can accommodate both network and analog cameras on the same recording device for special applications. All NVRs have an internal network interface card to receive and distribute IP video streams, and high-end units have two or more gigabit Ethernet ports.

A video server can be designed with essentially unlimited storage capacity. Hard drive selection is a consideration for the video management system. Both hard disk drive (HDD) and solid state drive (SSD) are a viable option for video archive. There are pros and cons for each type of drive. The VSS designer must work closely with the VMS vendor to determine the best choice based on cost and performance. In general, SSDs are used for the operating system and HDD is used for video storage. NVR storage capacity ranges from 1 TB at the low end of the category to greater than 64 TB for high-end units. The VSS designer must ensure that each network path connecting an IP camera with its associated recording node is adequate in terms of both availability and bandwidth. An important factor to consider is that some cameras are capable of supporting multiple video streams.

### **5-9.3 Required Storage Capacity.**

#### **5-9.3.1 Determine Capacity.**

Once all cameras have been specified for a project by the VSS designer, use Equation 5-7 to estimate the required storage capacity for each video storage device.

#### **Equation 5-7. Storage Capacity**

$$s = trz$$

Where:

$s$  = required video storage capacity for a single camera

$t$  = required video storage duration

$r$  = video frame rate

$z$  = average compressed file size of a single video frame

#### **5-9.3.2 Example.**

The following example illustrates the methodology and calculations needed to estimate required video storage capacity for a single storage device.

The VSS for an access control point will be upgraded to IP cameras. The new system will consist of two PTZ cameras, five fixed, and an NVR. The security manager has stated that the fixed cameras will be recorded at 4 fps with a resolution of 1280 x 1024 and the PTZ cameras will be recorded at 10 fps with a resolution of 720 x 480. The security manager also stated that there is a seven-day video storage requirement for all access control point cameras. The IP cameras will all use MJPEG compression. How much video storage is required for the NVR?

Converting seven days to 604,800 seconds, the storage required for a single fixed IP camera can be calculated as follows:

$$s_{\text{fixed}} = (604,800 \text{ s})(4 \text{ fps})(180 \text{ kB}) = 435,456,000 \text{ kB} \cong 415 \text{ GB}$$

The storage required for a single PTZ camera can be calculated in a similar manner:

$$s_{\text{ptz}} = (604,800 \text{ s})(10 \text{ fps})(60 \text{ kB}) = 362,880,000 \text{ kB} \cong 346 \text{ GB}$$

Taking into account the quantity of fixed and PTZ cameras, the total storage required for all cameras can be calculated as follows:

$$s_{\text{total}} = (5)(415 \text{ GB}) + (2)(346 \text{ GB}) = 2,767 \text{ GB} \cong 2.7 \text{ TB}$$

(Note: 1 TB = 1024 GB = 1,073,740,000 kB)

## **5-10 VIDEO WORKSTATION.**

To allow viewing live and recorded video, the designer must specify at least one workstation for each VSS; multiple workstations may be required for a large distributed system. Because of the computational demands associated with processing and displaying digital video streams, a “gaming” computer is a good choice for a video workstation. These computers generally have high-speed processors, large amounts of random access memory (RAM), fast graphics cards with high-resolution output, and network interface cards supporting Gigabit Ethernet speed. For a single-operator workstation, a graphics card feeding one or two monitors will usually be sufficient for video viewing and management. If three or four monitors are needed for a workstation, two dual-output graphics cards or a single quad-output graphics card must be specified for the workstation. The graphics card and monitor must provide display resolution equal to or greater than the highest resolution camera in the system. Any workstation that will be used to control PTZ cameras must be equipped with a joystick. Video management software that is compatible with all cameras, encoders, and recording devices must be installed on each workstation.

## **5-11 ANALYTICS.**

### **5-11.1 Video Analytics.**

If surveillance is an important security objective for a VSS, the designer must consider including video analytics as part of the system specification. Video analytics software allows the user to input a specific set of rules for each scene of interest, which, if violated, generate visual cues on the monitor, thus drawing the operator’s attention to suspicious objects or behaviors. This capability to automatically prioritize scenes and highlight suspicious areas for the operator maximizes the effectiveness of surveillance activities. Video analytics can be especially beneficial when a single operator is required to perform surveillance with a large number of cameras. Video analytics algorithms can be embedded in IP cameras, encoders, and recording devices or they can run on dedicated file servers. Common rule violations programmed to alert the operator include

crossing a virtual tripwire, loitering in a prohibited area, moving in the wrong direction, leaving an unattended object, and removing an object.

### **5-11.2 Audio Analytics.**

Many IP cameras feature a microphone, either built-in or with an external microphone interface. Similar to video analytics, audio analytics can be used to detect certain sounds and intensity levels. This capability can be used to identify aggressive situations, distress calls, glass break, gunfire, and audible alarm signals. Audio analytics can enhance a VSS by providing an extra level of situational awareness to help the security team quickly identify threat scenarios and respond accordingly.

## **5-12 VSS DESIGN PROCESS SUMMARY.**

### **5-12.1 Define Security Objectives for VSS.**

Begin by evaluating specific project requirements, considering the four most common VSS functions: alarm assessment, access control, surveillance, and evidentiary archives. Concisely state objectives with enough detail to facilitate camera selection and layout. Example objectives are as follows:

- Visually assess perimeter intrusion alarms for seven bistatic microwave sensor zones around the satellite communications facility.
- Visually identify the driver and vehicle prior to opening the gate at the test area.
- Perform surveillance of four exhibit areas in the museum and maintain a 30-day video archive for evidentiary purposes.

### **5-12.2 Develop Camera Layout to Meet Security Objectives.**

Indicate camera locations on site plans and building floor plans, identifying each camera as fixed or PTZ. Specify the mounting configuration (such as wall, ceiling, pole, and roof) for each camera, and select the appropriate camera and lens for the intended FOV.

### **5-12.3 Verify Illumination is Sufficient for Each Scene of Interest.**

Ensure that camera specifications for faceplate illumination are met and that uniformity ratios are within acceptable limits. Specify lighting upgrades as needed.

### **5-12.4 Specify Workstation Locations.**

Indicate workstation locations on building floor plans and describe the basic configuration of each workstation, including quantity and size of monitors. Identify any special furniture or console requirements.

**5-12.5 Specify Recording Locations and Capacity.**

Indicate recording locations on building floor plans and describe the type and quantity of video storage devices required at each location. Calculate the required video storage capacity for each storage device.

**5-12.6 Define Network Architecture.**

Develop a block diagram to illustrate connectivity for all cameras, video storage devices, workstations, and networking devices. Specify cables required for equipment interconnection and calculate bandwidth requirements for all network connections.

**5-12.7 Define Power Requirements.**

Determine the power requirements for each component. Specify all power circuits and the location of all power supplies. Consider PoE capacity. Include midspans as required.

**5-12.8 Describe Software and Integration Requirements.**

Specify features and functions required for camera control, video management, and analytics. State alarm assessment requirements for integration with intrusion detection and access control software.

*This Page Intentionally Left Blank*

## CHAPTER 6 DATA TRANSMISSION

### 6-1 INTRODUCTION.

Data transmission enables the components in an ESS to communicate with each other. Data transmission media (DTM) transmits information from sensors, access control devices, and video components to display and assessment equipment. A DTM link is a path for transmitting data between two or more ESS components and back to the central monitoring station. Procurement of telecommunications equipment must comply with FAR 52.204-25. An effective DTM link ensures rapid and reliable data transmission, is resistant to compromise, has redundancy, and is conducive to rapid fault detection and repair. A number of technology issues are relevant to implementing the DTM, such as bandwidth analysis, secure communications, network topology, communication redundancy, transmission modes or protocols, and transmission media. These issues are discussed in the following paragraphs.

### 6-2 BANDWIDTH ANALYSIS.

With any data-intensive transmission network, such as an ESS network, it is important to determine the amount of bandwidth consumed by the system under normal and high-traffic conditions. This can affect network cost, reliability, and transmission speed. Of the three ESS subsystems, the VSS generally requires the most bandwidth and IDS requires the least. ACS bandwidth requirements are generally low, but bandwidth usage will spike during database synchronization cycles. Also, bandwidth requirements will vary based on the way the ACS is wired and the manufacturer's design. For the DTM, design a system capable of handling the total bandwidth (plus contingency) for each link required in the system. Table 6-1 presents bandwidth usage values for some common ESS components.

**Table 6-1 Bandwidth Usage Values**

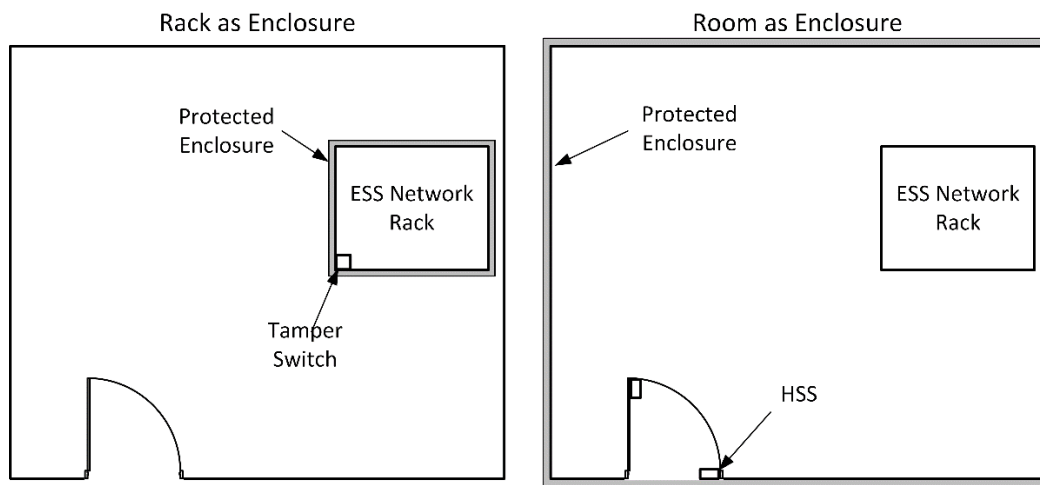
Component	Bandwidth Usage Range (kilobits per second)		
	Low	High	High Bandwidth Usage Results From:
IDS local processor	1	3	High alarm rate, encryption
ACS local processor	5	50	High-volume portal traffic, large database synchronizations
IP camera	100	70,000	High frame rate and resolution, low compression ratio
ESS workstation	100	100,000	Large number of simultaneous video streams

### 6-3 SECURE COMMUNICATIONS.

No matter what transmission mode or media is selected, it is important that a method for securing communications be included. This includes physical protection, such as providing conduit for all conductors, as well as electronic protection, such as encrypting

communication transmissions and supervising alarm circuits. For tamper protection, refer to paragraph 10-6.6 and Appendix A, which includes a discussion on physical protection of conductors as well as more general information on encryption requirements. In general, DTM connections must be done within a tamper-protected enclosure, such as an enclosure with a tamper switch reporting to the ESS. When the use of a tamper-protected enclosure is not possible, design consideration must be made to alarm the room where DTM terminations are made. The preferred method of doing this is by securing doors to the room by HSSs, treating the room as an enclosure. See Figure 6-1 for an illustration of adequate ways to secure ESS DTM.

**Figure 6-1 Enclosures for Secure Communications**



## **6-4 NETWORK TOPOLOGY.**

One of the initial steps in designing and evaluating a security DTM is to identify the topology to be used. Additionally, the designer must coordinate network requirements with installation security and the communications office. Typically, networked security systems are a proprietary security network. See Chapter 8 for more information.

### **6-4.1 General Network Topologies.**

Five general network topologies are possible: star, ring, fully meshed, bus, and hybrid. These concepts apply to intra-site system architectures as well as inter-site regional configurations. A brief description of each topology follows.

#### **6-4.1.1 Star.**

The star, or “hub and spoke,” network involves a central monitoring station (or head-end) and single communication lines out to individual sites (or field panels). The disadvantage to a star topology is that if one of the links is disabled or severed then communication is lost to that node. The unconnected node may still operate through distributed intelligence but will be unable to receive updates from and transmit alarms to the rest of the system. For example, if a new credential holder were added to the

access list, this information could be downloaded to a remote site or panel from a central location. With a severed link, these updates are not available unless the information was uploaded at the local site/panel. Conversely, if a credential holder were deleted from the access database, a “severed” site/panel would continue to allow access until communications were re-established or a local upload made. Figure 6-2 shows a star topology for both an inter-site architecture and an intra-site architecture. Generally, this is the most cost-efficient solution for ESS.

#### **6-4.1.2 Ring.**

The ring topology communicates through a loop. This topology is slightly more robust than a star topology in that if a link fails, communications can still be maintained through the “backside” direction on the loop. Communications may be slower in this backup mode of operation but would be sustainable. Figure 6-3 shows a ring topology for both the inter-site and intra-site scenario.

#### **6-4.1.3 Fully Meshed.**

The most robust topology is a fully meshed topology depicted in Figure 6-4. This topology has backup means of communication, such that if any one link is disabled or severed, data has an alternate path to communicate directly between nodes. This is the preferred ESS network topology, although the costliest.

#### **6-4.1.4 Bus.**

The bus topology communicates use of a computer or server addressing and polling all ESS devices individually. In essence, this acts as an expensive way of daisy-chaining device cabling, reducing the amount of physical wiring required. Due to this configuration, no redundancy is possible and a failed cable segment results in all devices downstream losing communications with the computer or server monitoring the devices. Figure 6-5 depicts an example of a bus topology.

#### **6-4.1.5 Hybrid.**

Dependent on design requirements, the aforementioned topologies can be combined, resulting in a hybrid topology.

Figure 6-2 Star Topologies

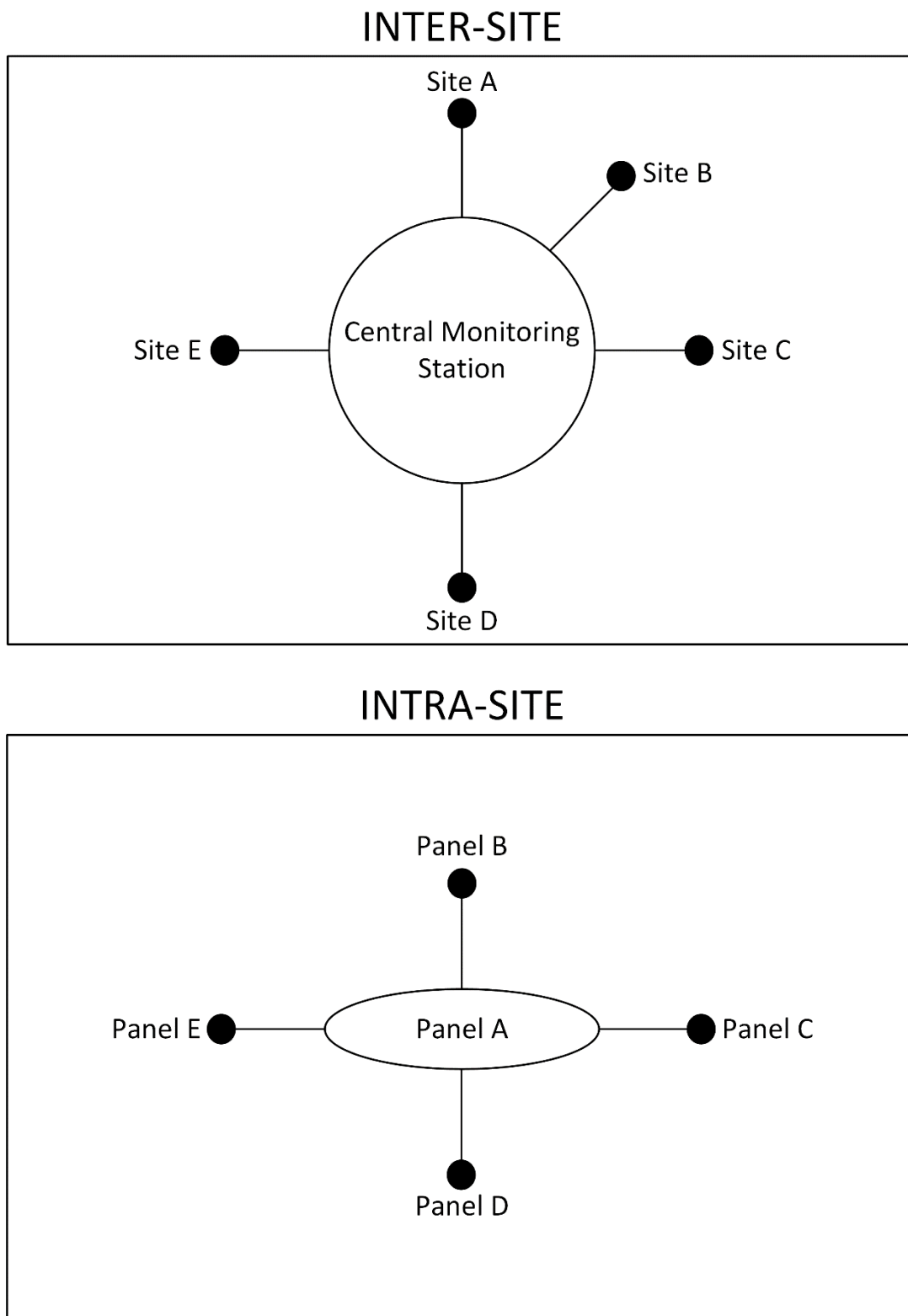
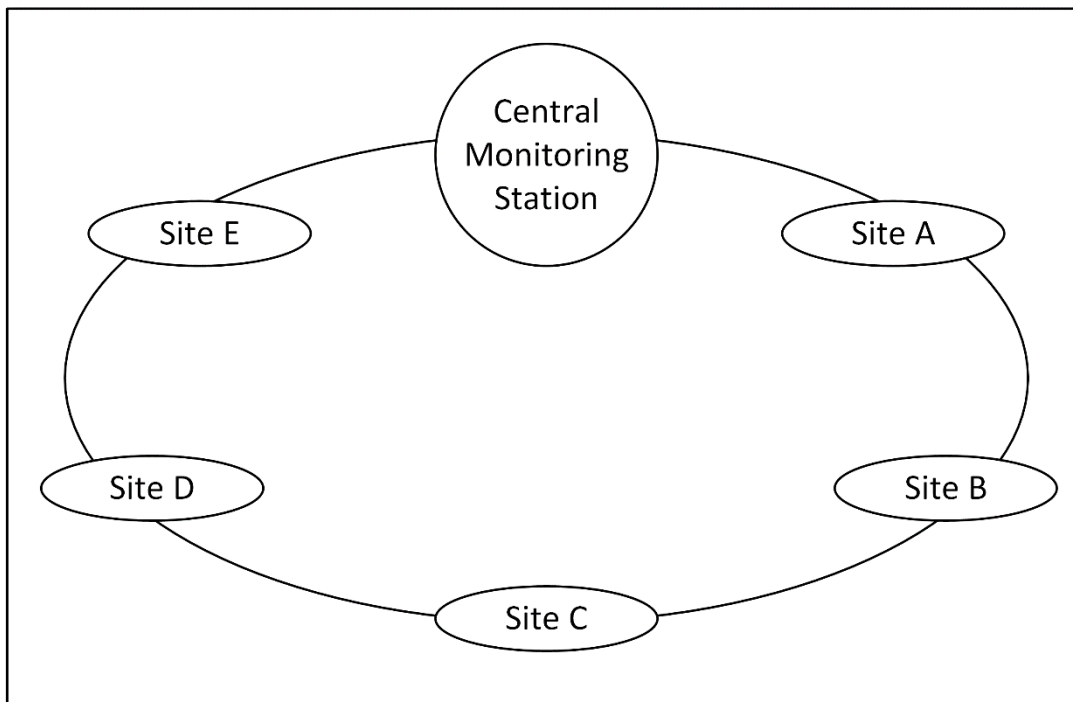


Figure 6-3 Ring Topologies

### INTER-SITE



### INTRA-SITE

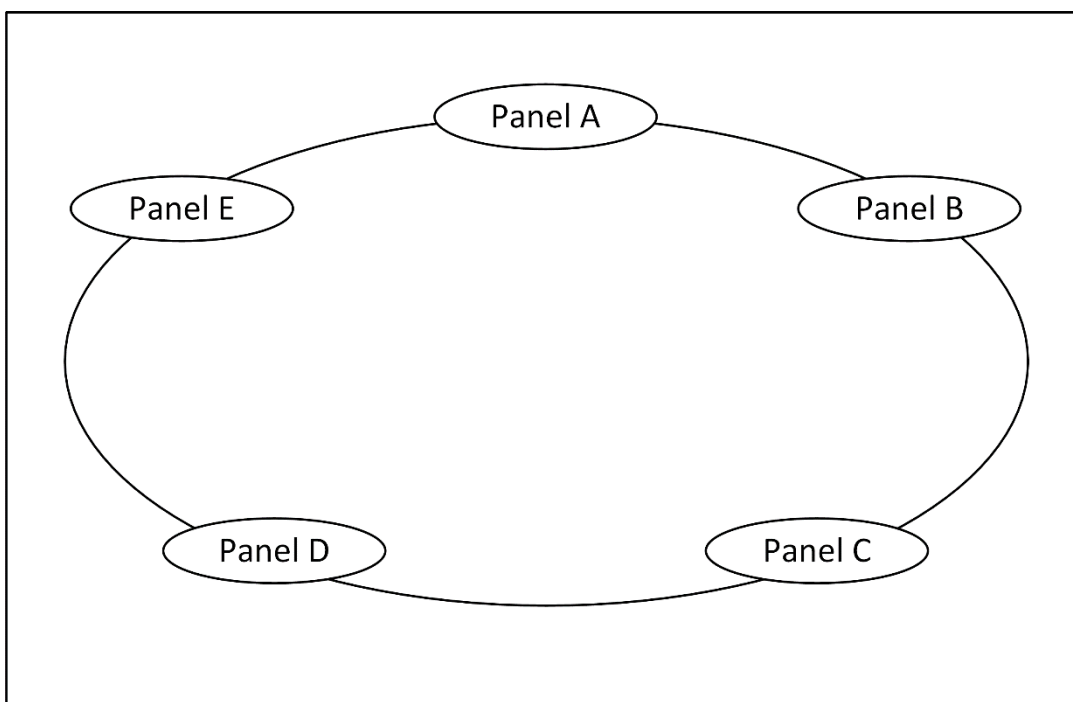
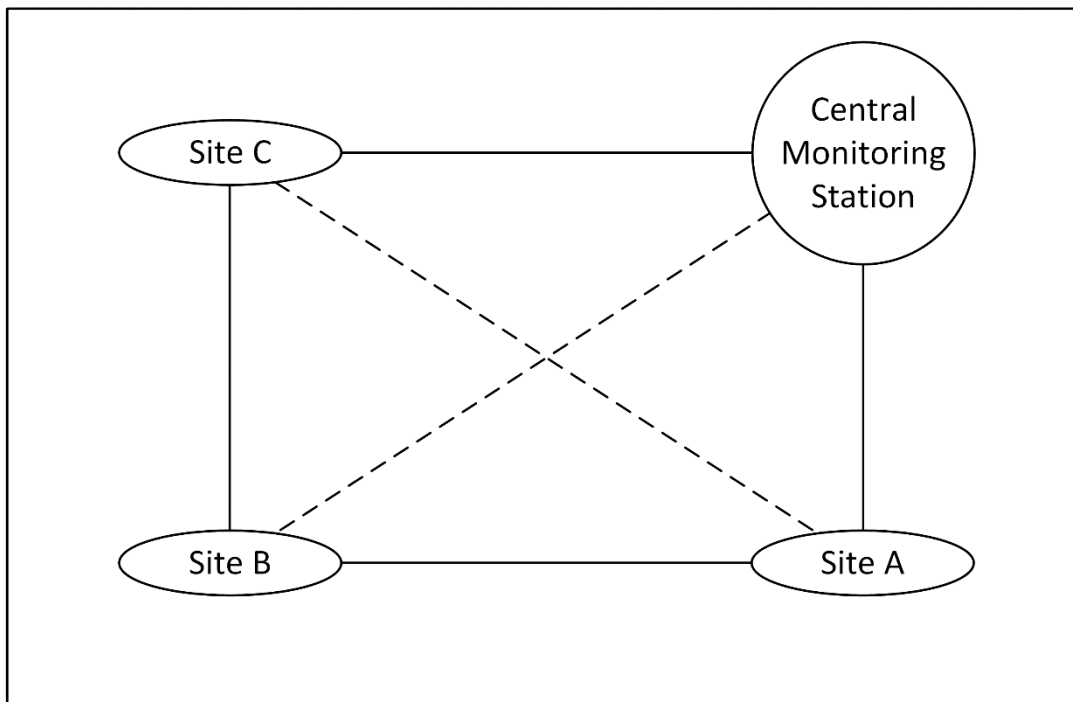
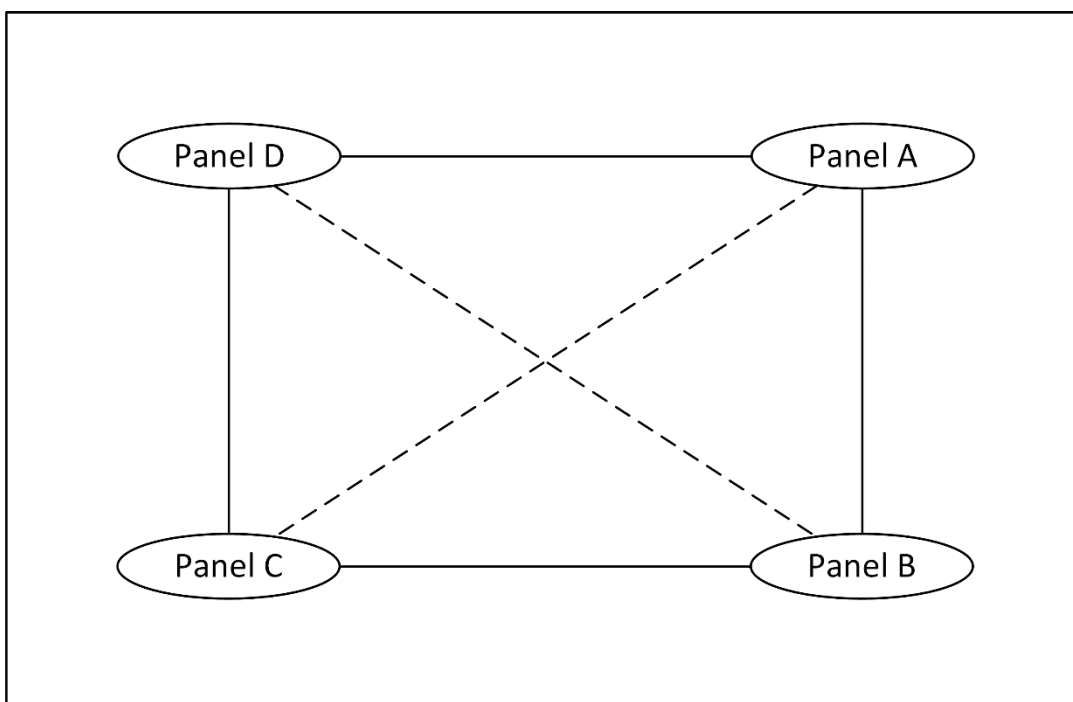


Figure 6-4 Fully Meshed Topologies

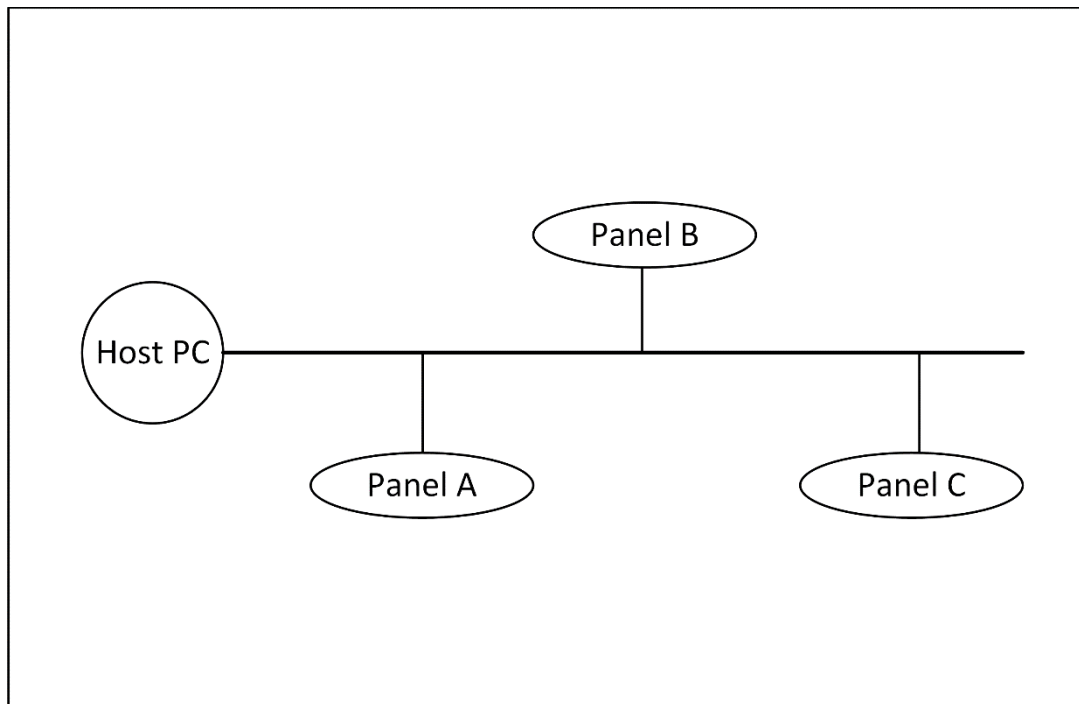
### INTER-SITE



### INTRA-SITE



**Figure 6-5 Bus Topology**



## **6-5 COMMUNICATION REDUNDANCY.**

Typically, the only communication redundancy made is between subsystem field panels and the system head-end. Redundancy between field panels and devices is cost prohibitive. A common method of achieving communication redundancy is running primary as well as backup RS-485 lines. If this is done, it is best to use different raceway routing schemes.

Protocols such as TCP/IP and improved design configurations increasingly harden communication system redundancy and allow monitoring of the DTM. TCP/IP guarantees data delivery, checks receiving device status, verifies the message is correct and complete, and resends data as needed. Redundant communication paths are established so if a component or link goes down, communication is maintained through an alternate communication path. While some people refer to these designs as “self-healing,” the term is a misnomer because the failed component is still a failed component. Alternate communication paths are employed until the fault can be corrected.

## **6-6 TRANSMISSION MODES/PROTOCOLS.**

Several modes and protocols exist for electronic security data transmission, including serial communication (RS-485, RS-232), network communication using TCP/IP, modem, and wireless. The designer must consider protocol compatibility as well as data rate and distance requirements when selecting the appropriate data transmission methods for a project. The information in Table 6-2 will aid in this selection process.

This information is discussed in the following section as part of an overview of the data transmission media commonly specified for ESS projects.

## **6-7 TRANSMISSION MEDIA.**

### **6-7.1 Hardwired.**

Hardwired refers to using dedicated proprietary (DoD-owned) circuits to transmit data/video between DTM nodes. Dedicated circuits can be copper or fiber-optic, both of which are discussed below.

#### **6-7.1.1 Copper Circuits.**

Copper circuits can meet most ESS data transmission needs from alarm circuits transmitting a simple state change to network links operating at speeds up to 1 GB/s. As shown in Table 6-2, copper circuits are capable of supporting lower data rates out to distances of 1,000 feet (305 meters) and greater, but copper Ethernet links are generally limited to 328 feet (100 meters). Single-Pair High-Speed Digital Subscriber Line (SHDSL) technology is a good option for achieving moderately high data rates at fairly long distances over a single copper pair. Disadvantages of copper circuits include susceptibility to electromagnetic interference, radio-frequency interference, and damage from lightning strikes.

#### **6-7.1.2 Fiber-Optic Cable.**

Fiber-optic cable allows transmission over longer distances by using light, which does not have the higher resistance loss over distance like copper circuits. Furthermore, fiber-optic cable is not affected by electromagnetic interference or lightning. As seen in Table 6-2, fiber optic cable, when compared to copper, allows high data rate links to be established over much greater distances. For example, a gigabit Ethernet link of 6.2 miles (10 kilometers) is possible with fiber, compared to only 328 feet (100 meters) with copper. Since the cost of a data transmission system can be a significant component of overall ESS cost, the designer must evaluate the advantages of fiber links in light of their higher cost compared to copper circuits. Other considerations to be considered when utilizing fiber optic cable are the limitations of manufacturer-recommended installation bend radius and the environment in which the cabling will be installed. Generally speaking, fiber-optic cable is far less durable than various forms of copper DTM. Consider providing additional physical protection measures when using fiber-optic media. Of the two varieties of fiber-optic cable, single-mode fiber offers greater distance capabilities than multi-mode fiber but is more expensive to implement.

#### **6-7.2 Direct Subscriber Lines (T1 Lines).**

Direct subscriber lines, also called T1 lines, are commonly used in data transmission media systems for connecting remote sites. T1/DS1 lines are permanent point-to-point links through public networks. The bandwidth capacity of a T1 line is 1.544 Mbps. The cost of the leased line is dependent on distance and existing capacity or infrastructure.

T1 lines are uniquely assigned to a customer, such that only DoD information would be transmitted over the assigned point-to-point link.

### **6-7.3 Wireless.**

For security reasons, only use wireless if other media cannot be used. Wireless broadband networks make use of radio frequency transmission between towers. Wireless LANs make use of radio frequency transmission between wireless network bridges/switches/routers. Some ESS devices have built in wireless networking capabilities for easier installation. Wireless systems have high data transmission rates and do not require installation of cable nor rely on existing copper infrastructure. Wireless communications are affected by line-of-sight topography and extreme weather conditions (such as rain, snow, or fog). Some radio modem units can provide data transmission rates of several Mbps at ranges up to 10 or more miles (16+ kilometers) between modems. One disadvantage of wireless systems is the systems are susceptible to jamming. Cryptography methods must be used to the greatest extent possible to protect information and communications from possible interception. To increase reliability of service, consider utilizing frequency-hopping spread spectrum (FHSS) methods when transmitting radio signals at high rates. Wireless links are typically configured as dedicated circuits for purposes of ESS.

#### **6-7.3.1 Wireless Security.**

Security can be achieved by vendor encryption and decryption at each node. The design and cost estimate must consider equipment and software for authentication servers and encryption systems.

#### **6-7.3.2 Frequency Allocation.**

Frequency allocation or radio frequency spectrum planning is a critical issue and must be an early project design consideration. Frequency allocation is a long lead-time item. Employment of radio frequency transmitting equipment outside of the continental United States (OCONUS) may require approval by the host nation. Refer to Service policies for frequency allocation. Coordinate all frequency allocation efforts with the command-designated frequency allocation manager.

### **6-7.4 Free-Space Optics (FSO).**

FSO, also called free-space photonics (FSPO) or optical wireless, refers to the transmission of modulated visible or IR beams through the atmosphere to obtain broadband communications. Most frequently, laser beams are used. LED technology is also an option. FSO operates similar to fiber-optic transmission, except that information is transmitted through space rather than a fiber-optic cable. FSO systems can function over distances of several kilometers, but each link requires a clear line-of-sight unless mirrors are used to reflect the light energy. FSO systems offer advantages of reduced construction cost in that fiber-optic lines do not have to be installed, but there are limitations. Rain, dust, snow, fog, or smog can block the transmission path and shut down the network. Another advantage of using FSO over other wireless technologies is that it does not require frequency allocation/licensing for use.

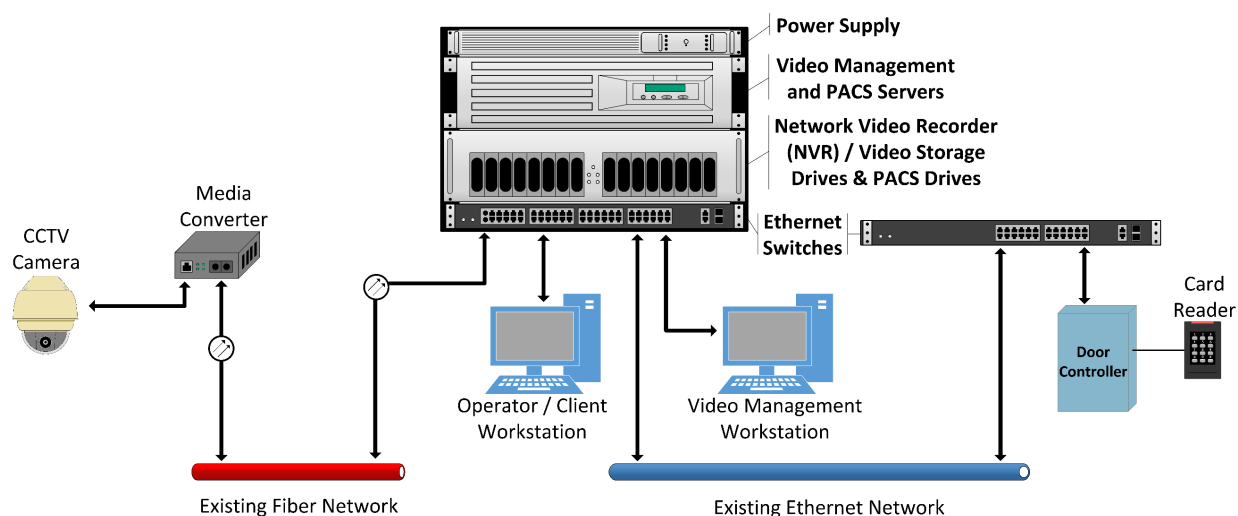
**Table 6-2 Data Transmission.**

Protocol / Media	Data Rate @ Distance
Supervised alarm circuit / copper, single pair	State change @ 1,000 feet (300 m)
RS232 / copper	19.2 kb/s @ 50 feet (15 m)
	9.6 kb/s @ 500 feet (150 m)
	4.8 kb/s @ 1,000 feet (300 m)
	2.4 kb/s @ 3,000 feet (900 m)
V.35 / copper	1.5 Mb/s @ 50 feet (15 m)
	56 kb/s @ 102 feet (31 m)
	19.2 kb/s @ 513 feet (156 m)
	9.6 kb/s @ 1,025 feet (312 m)
	4.8 kb/s @ 2,050 feet (625 m)
	2.4 kb/s @ 4,100 feet (1250 m)
RS422 / copper	10 Mb/s @ 40 feet (12 m)
	1 Mb/s @ 200 feet (61 m)
	100 kb/s @ 4,000 feet (1220 m)
RS485 / copper	10 Mb/s @ 40 feet (12 m)
	1 Mb/s @ 200 feet (61 m)
	100 kb/s @ 4,000 feet (1220 m)
SHDSL / copper, single pair	256 kb/s @ 21,980 feet (6,700 m)
	1.5 Mb/s @ 16,404 feet (5,000 m)
	2.3 Mb/s @ 13,780 feet (4,200 m)
10BASE-T Ethernet / copper, two pairs	10 Mb/s @ 328 feet (100 m)
Fast Ethernet / copper, two pairs	100 Mb/s @ 328 feet (100 m)
Fast Ethernet / multi-mode fiber, two fibers	100 Mb/s @ 1,804 feet (550 m)
Fast Ethernet / single-mode fiber, two fibers	100 Mb/s @ 32,808 feet (10,000 m)
Gigabit Ethernet / copper, four pairs	1 Gb/s @ 328 feet (100 m)
Gigabit Ethernet / multi-mode fiber, two fibers	1 Gb/s @ 1,804 feet (550 m)
Gigabit Ethernet / single-mode fiber, two fibers	1 Gb/s @ 32,808 feet (10,000 m)

## 6-8 NETWORK DEVICES.

Network devices provide interconnection between various DTM types and allows devices to communicate. The most commonly used network devices in ESS consist of routers and switches. Switches are used to connect multiple devices on the same network (typically IP based). Routers connect multiple switches or separate networks together. The designer must select switches and routers listed on the U.S. Department of Defense Information Network Approved Products List (DoDIN APL). Figure 6-6 depicts a simple ESS network using network devices.

**Figure 6-6 ESS Network**



## 6-9 TECHNOLOGY COMPARISON.

Table 6-3 provides a comparison matrix of different DTM technologies for ESS.

Dedicated conductors are highlighted for on-base applications and T1 lines are highlighted for inter-base applications as a general guide. Whichever method is used, initial calculations have to be made on the data rate and distance requirements.

**Table 6-3 DTM Technologies for ESS.**

	<b>Hardwired</b>	<b>Leased T1 Lines</b>	<b>Wireless</b>	<b>Free Space Optics</b>
<b>Suitability on Base</b>	Recommended application.	Does not make sense when base level information infrastructure can be used.	Generally requires line of sight.	May make sense; can be used when there is line of sight.
<b>Suitability Inter Base</b>	Rarely achievable, because of property line boundaries.	Recommended application. Can cross property lines.	A workable application	May make sense.
<b>Initial Cost</b>	Dependent on distance. Principle cost is per linear foot of trenching/ conductors.	Low, which is good. Must provide interface to site's demarcation point for supplier.	Construction costs of towers and tie-ins have to be computed.	Reduced initial cost because conductors are not used. Need transmit/receive equipment.
<b>Recurring Cost</b>	Low, which is good. Minimal maintenance cost of installed conductors.	One T1 line at 1.544 Mbps can be estimated at \$500/month. Obtain vendor quote.	Relatively low, which is good if DoD-owned. Otherwise obtain vendor quote.	Low if DoD equipment. Leased equipment requires vendor quote.
<b>Considerations</b>	Best technology. Not affected by line of sight.	Reasonable alternative to hardwired. Not affected by line of sight.	Generally, requires line of sight. Approved frequencies must be used.	Requires line of sight or mirrors.
<b>Security</b>	Very good, especially if totally contained on DoD property and encrypted.	Second- or third-best choice. Usually dedicated conductors are used from one provider.	Not recommended by CIA studies, but may make sense on DoD property if there is little chance of interception.	Signals can be blocked. Hard to transmit forged signals.
<b>Weather Effects</b>	Not affected. Best technology from weather consideration.	Not affected. As good as hardwired.	Not as bad as free space optics but can be affected by heavy rain and snow.	Rain, dust, snow, fog, or smog can block transmission and shut down network.

## 6-10      ENCRYPTION.

An ESS designer is responsible for reviewing applicable security policies and consulting with cybersecurity personnel to determine data transmission encryption requirements and methods on a project-by-project basis. Two details must be addressed when making this determination: the types of data being transmitted and the data transmission techniques being used. As a general guideline, ESS data associated with very high security assets (such as SCIFs) or containing personally identifiable information (such as biometrics) must be encrypted. Encryption will generally be required when any ESS data is transmitted using techniques such as wireless links and shared or public networks that are inherently more susceptible to interception than hardwired circuits and closed, restricted ESS networks. Encryption provides the benefit of protecting information and communications through use of codes, so that only those for whom the information is intended can read and process. For ESS, the most commonly used encryption type is advanced encryption standards (AES). AES NIST encryption is covered under FIPS 197, *Advanced Encryption Standard (AES)*, or FIPS 140, *Security Requirements for Cryptographic Modules*. ESS encryption standards must comply with guidelines governed by NIST. Encryption requirements are based on the type of asset and governing policy for that asset. In general the encryption standard and certificate for the implementation must be current. Validate current NIST certificates via the NIST cryptographic module validation program to ensure proposed products are compliant.

*This Page Intentionally Left Blank*

## CHAPTER 7 COMMAND AND CONTROL DISPLAY EQUIPMENT

### 7-1 INTRODUCTION.

Command and control display equipment (CCDE) provides authorized users the ability to interact with an ESS to perform a variety of system-level tasks, including monitoring, enrollment, management, and administration. Workstations and file servers along with associated software are the primary elements of CCDE. Design guidance for these elements is provided in this chapter. A simple workstation and file server configuration are shown in Figure 7-1. Implement cybersecurity controls in accordance with the risk management framework (RMF) process to ensure logical protection of ESS workstations and file servers.

**Figure 7-1 ESS Workstation and Lockable File Server Rack**



### 7-2 WORKSTATION.

An ESS workstation consists of a computer and all required peripheral devices. End-user input must be obtained early in the design process to identify all workstation locations. Tasks to be performed at each workstation must be clearly defined as this will impact final equipment selection and software licensing. Once established, workstation requirements must be coordinated with other design disciplines to ensure appropriate space allocation, furniture selection, and network and power connections. Common workstation categories are: 1) operator workstation, 2) administrator (or supervisor) workstation, and 3) enrollment workstation. An operator workstation is used to perform routine ESS tasks such as alarm monitoring and video surveillance. Generating system reports and changing system settings are typical tasks performed at an administrator

workstation. An operator workstation is used on a frequent or continuous basis, while use of an administrator workstation may be intermittent. An enrollment workstation is configured to enter personnel into the access control database. These workstation categories may be helpful in discussing intended functionality with end-user representatives during the planning and design process.

### **7-2.1 Computer.**

Ensure each workstation computer meets or exceeds minimum hardware requirements established by operating system and application software providers. Also consider the type and quantity of concurrent tasks to be performed at a workstation when developing computer performance specifications. The computer hardware configuration must support all required peripheral devices, including multiple monitors as needed. Provide physical protection for each computer; two good options are a lockable console bay as shown in Figure 7-2 and a lockable equipment rack. Physical protection may be enhanced if the equipment rack is in a secure location, separated from the console. If a remote rack is used, a keyboard-video-mouse (KVM) extender is needed to connect the rack-mount computer to the console.

**Figure 7-2 Lockable Console Bay for ESS Workstation Computer**



### **7-2.2 Keyboard and Pointing Device.**

Each computer must be furnished with a keyboard and pointing device. Wired devices are preferred over wireless devices.

### **7-2.3 Joystick.**

Provide a joystick if requested by an end-user. Some end-users prefer a joystick over a pointing device for PTZ camera control.

### **7-2.4 Microphone.**

Provide a microphone if the workstation will be used to communicate with intercom door stations or broadcast audio messages via a distributed speaker network.

### **7-2.5 Speaker.**

Provide a speaker with each workstation. Ensure speaker output is sufficient for audible alarms to be heard clearly over ambient background noise. An output of a least 75 dB is recommended.

### **7-2.6 Enrollment Equipment.**

Provide specialized peripheral devices for an enrollment workstation. These may include a card reader, keypad, camera, and biometric devices. IDS may be required for a room housing an enrollment workstation; check individual Service or agency policy for applicability.

### **7-2.7 Monitors.**

Specify quantity, size, and resolution of monitors based on the tasks to be performed at the workstation. One or two monitors are generally sufficient for administrator and enrollment workstations. Two to four monitors are recommended for operator workstations. Monitors in the 24-inch to 32-inch size range are adequate for most ESS workstations. Recommended minimum monitor resolution is 1920 x 1080 pixels.

### **7-2.8 Printer.**

Provide a printer for each workstation. A shared network printer is an option for a co-located group of ESS workstations. An enrollment workstation requires a specialized badge printer if local badges will be issued.

### **7-2.9 Uninterruptible Power Supply.**

Consider the criticality of tasks performed at a workstation when assessing the need for a UPS. If a need is established, size the UPS based on the reliability of primary power and the availability of a backup generator. A small UPS with a run time in the range of three to five minutes is an economical and effective option for many workstations. Mission-critical workstations must be connected to emergency power circuits to ensure continuous operation.

## 7-3 FILE SERVER.

A file server performs essential system-level functions related to data processing, storage, and transmission. A large ESS may have several file servers, each dedicated to a specific function. The essential nature of ESS file servers dictates that special consideration be given to hardware requirements, physical protection, and backup power as discussed in the following paragraphs.

### 7-3.1 Hardware Requirements.

Hardware requirements are driven by the scale of the ESS and minimum standards established by operating system and application software providers. Consult with software providers to specify hardware that will ensure the desired level of system performance. To enhance reliability and availability, a redundant array of inexpensive disks (RAID) configuration with hot-swappable capability is generally preferred. Enterprise ESS deployments may require a multi-tiered configuration consisting of central servers, regional servers, and site servers. Equip ESS file server racks with a pull-out monitor-keyboard-touchpad console as illustrated in Figure 7-3.

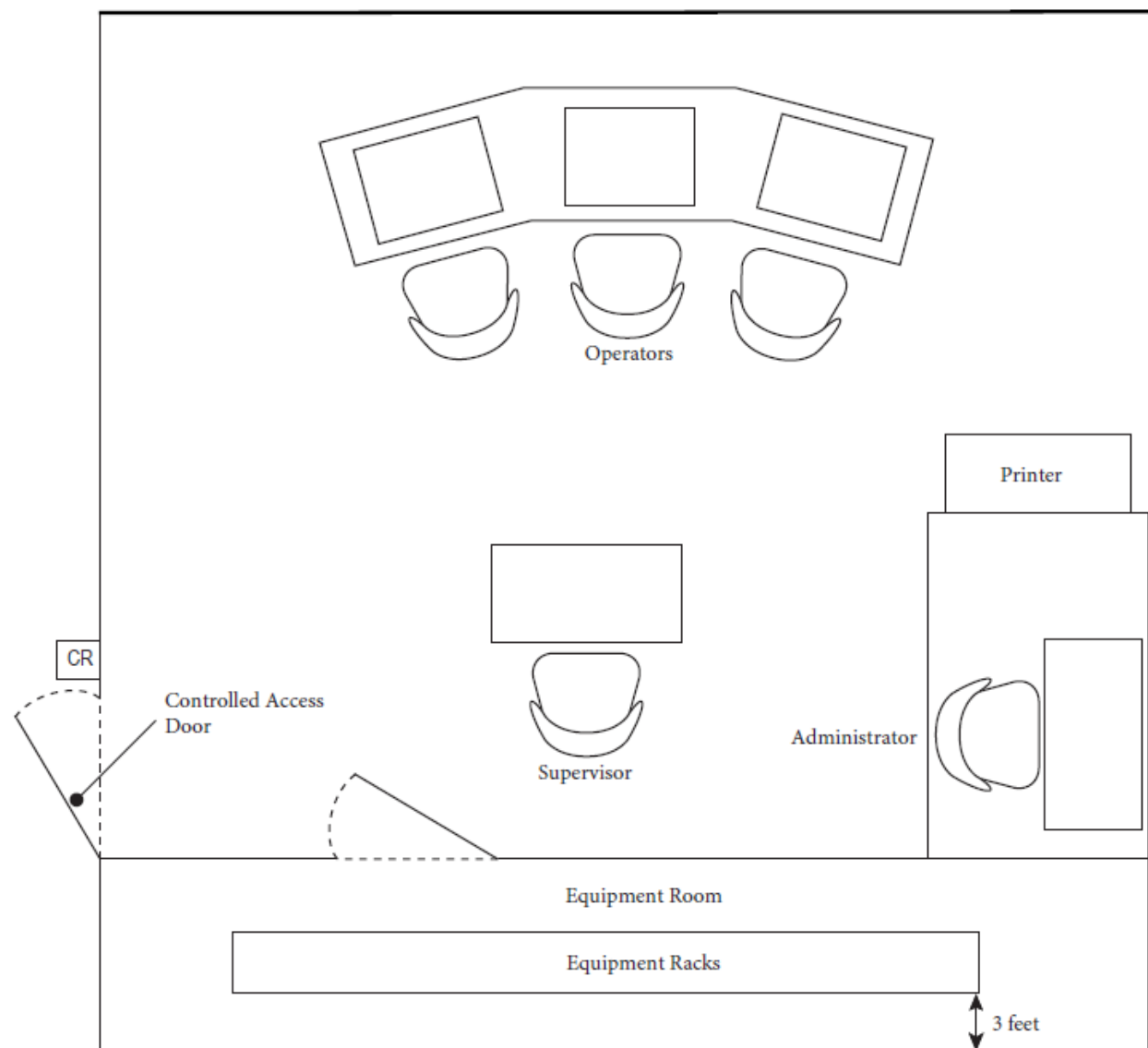
**Figure 7-3 Monitor-Keyboards-Touchpad Console**



### 7-3.2 Physical Protection.

The best option for housing ESS file servers is a data center where physical security, environmental controls, backup power, and network infrastructure are key elements of the facility design. If a data center is not available, a dedicated equipment room is a good option, provided the aforementioned facility design elements are addressed. Figure 7-4 illustrates a central monitoring station with a separate equipment room for housing ESS file servers and network equipment. Do not install ESS file servers in uncontrolled spaces

**Figure 7-4 Central Monitoring Station with Separate Equipment Room**



### **7-3.3 Backup Power.**

Backup power is required for ESS file servers, with UPS run time no less than five minutes. Mission-critical file servers must be connected to emergency power circuits to ensure continuous operation.

### **7-4 SOFTWARE.**

ESS functionality is enabled through specialized application software. Address all required features when developing software requirements as some advanced features may require additional licensing beyond the basic software license. Ensure all file servers and workstations are addressed in the software requirements. A software support agreement is recommended to stay current with software versions.

## **CHAPTER 8 ESS SUBSYSTEM INTEGRATION**

### **8-1 OVERVIEW.**

Since the different subsystems of a facility's total ESS are drawn from a number of different technologies, the manufacturers of subsystems tend to be diverse and, in many cases, not readily compatible. As a result, system integration or making the subsystems and components "talk to each other" reliably and consistently is a major goal of an ESS design. The purpose of this chapter is to briefly consider some of the system integration issues associated with an ESS.

### **8-2 COMMUNICATION FROM THE IDS TO THE ACS.**

As covered in Chapter 2, the IDS may already be an integral part of the ACS. In these systems (depicted in Figure 2-1), basic intrusion detection devices are brought into a combined ACS/IDS system as digital inputs on local security panels. All that is required is to allocate digital input points in the closest security panels and program the ACS to provide an alarm on event.

For some facilities, however, the IDS and ACS will be separate. This is a fairly common scenario in which each IDS zone within a facility is equipped with an IDS local processor connected to the central monitoring station for the sole purpose of IDS alarm monitoring and doors/portals within the facility are controlled by a local ACS administered and monitored by the owner/tenant. In facilities where the two systems are separate, the IDS and ACS often share a common need to monitor the position of certain doors. Rather than having two position sensors on a door (one for IDS and the other for ACS), the designer may specify a single door sensor that has two independent outputs. This allows one output to be wired to the IDS local processor and the other to the ACS local processor. This approach reduces the cost and eliminates the clutter associated with having two sensors on a single door.

### **8-3 COMMUNICATION FROM THE IDS (OR COMBINED ACS/IDS) TO THE VSS.**

Once an intrusion is detected (for example, door forced open or perimeter fence or microwave alarm), it is generally the practice to make sure the event is being viewed and recorded by the VSS. Interface of the IDS to the VSS can occur through several different means: hardwired conductors, serial communications, and networked connections, as discussed below. Activation of an intrusion detection alarm results in an audible alarm that gets the operator's attention.

#### **8-3.1 Hardwired Conductors.**

This is older technology but still effective for simple installations. In this case, copper wiring is taken as digital outputs from the IDS or combined ACS/IDS and connected as inputs to the VSS to initiate camera recording and, if required, panning to a pre-set location (see Chapter 5 for additional information). In the most basic approach, this design requires a pair of wires for each alarm notification output signal.

### **8-3.2 Serial Communications.**

In theory, this is the same principle of operation as the hardwired method, with an improvement in that a single serial data link can handle several camera control signals. It is most easily done when the video and IDS (or combined ACS/IDS) are made by the same vendor but can be done with different vendors if appropriate software drivers are available. While more complicated than the hardwired approach, this method has the advantage of reduced wiring costs.

### **8-3.3 Software-Based Integration for Networked ESS.**

This approach provides flexibility in the initial system setup and allows the user to make configuration changes via software with no additional hardware or wiring investment. For this reason, software-based integration is preferred for most projects, but it requires a networked ESS in which all subsystems are connected to a common IP network. In this approach, all file servers, workstations, video recording devices, cameras, and local processors are connected to the same network via Ethernet cables and switches. This network configuration allows communication between the remote equipment and a server or desktop PC, usually located in the central monitoring station. The desktop PC will have a security program that accesses remote equipment through IP addresses provided during setup. The security program allows the user to access video and ACS information. When using this approach, having adequate bandwidth is important due to the large amount required for video information. Network security is also of paramount importance, and for DoD projects a dedicated security network is recommended. Cost savings of reduced point-to-point wiring have to be compared to possible new costs of installing a dedicated network. A drawback to this approach is that typically the manufacturer of both the video and ACS has to be the same vendor unless compatible software drivers or a software development kit (SDK) is available, allowing both systems to communicate in a common language.

## **8-4 COMMUNICATION FROM THE VSS TO THE ACS.**

Cameras may be used to visually assess access control alarms in the same way they are used to assess intrusion alarms. Cameras may also be used to visually confirm the identity of a person requesting entry into a secure area before releasing the portal (referred to as video verification by some ACS vendors). The IDS/video integration techniques described above also apply to ACS/video integration.

## **8-5 COMMUNICATION FROM THE ACS TO THE CENTRAL MONITORING STATION.**

ACS alarms may be transmitted from a facility to the central monitoring station. The designer must determine for each project whether a facility owner/tenant will monitor ACS alarms locally or will rely on the central monitoring station to provide ACS monitoring services. If the central monitoring station will monitor ACS alarms, the monitored facility must be equipped with a local processor that is compatible with the existing central monitoring system.

## **8-6 DESIGN GUIDANCE ON IT SYSTEM COORDINATION.**

Fiber optic cables typically come in multiples of twelve strands, with 12-strand and 24-strand fiber optic cable being very common. While there are no technical limitations on combining ESS with other base systems, such as IT or instrumentation and control, it is standard engineering practice to keep ESS communication dedicated for security purposes only. If other unrelated systems are on a common fiber, other vendors or organizations will have closer access to the security network. Plan for future expansion (provide a minimum of 20% spare capacity (fibers)).

## **8-7 INTEGRATING ESS AND OTHER SYSTEMS.**

For some projects, it may be beneficial to integrate ESS and other systems based on end-user preferences for monitoring and managing system information. Software integration is generally the preferred method for these projects. Consult with the end-user to achieve the proper balance between operational efficiency and system complexity, recognizing that just because a system can be integrated with ESS does not mean that it is allowed or desired. The following is a partial list of other systems that may be considered for ESS integration:

- Duress
- Intercom
- VoIP telephone
- Infant protection (medical facilities)
- Visitor management
- Key management
- Computer-aided dispatch
- Gunshot detection
- Mass notification
- Fire alarm
- Utility monitoring

## **8-8 COMMON CONSIDERATIONS FOR ESS DESIGNERS.**

There are several questions that must be answered early in any ESS project, whether supporting MILCON or SRM projects.

- Most ESS are proprietary, with very limited compatibility of software and hardware between vendors. A basic question that must be answered early in the design process is: “Who will be monitoring the ESS?” Typically, IDS is monitored by a Military Police or security forces central monitoring

station. The local security panels must be compatible with the central monitoring station IDS receiver software and equipment.

- ACS and VSS may be monitored by the Military Police or security forces but are more often monitored within the building or by a local command. The same above requirements for compatibility exist.
- The DoD Components, Military Departments and local Commands often have programs for their ESS requirements, identifying specific manufactures and components.
- Coordination with the Command and/or organizational security manager will ensure the ESS design is compliant with applicable security policy and supports the building owner's local security plan.
- Reducing the variation of ESS hardware will simplify future maintenance cost and complexity, e.g., the use of only two or three camera types from the same manufacturer to satisfy VSS requirements.
- All ESS require detailed "as built" drawings to support future expansion, maintenance, and service of the system after installation.

## **CHAPTER 9 DESIGN PROCESS SUMMARY**

### **9-1 INTRODUCTION.**

This chapter presents a process summary on how to design an ESS. Other documents provide guidance or directives on design and construction of DoD facilities. The intent of this chapter is not to set new directives, but rather to communicate a process that works well.

Two principal project approaches are design-bid-build and design-build. The design process summary outlined in this chapter is applicable to both approaches.

### **9-2 PROJECT PLANNING.**

As discussed in Chapter 2, ESS is a portion of the overall physical security scheme for a facility and must be integrated into the overall physical protection plan. Table 9-1 includes a list of agency requirements for ESS. The list is not all-inclusive; however, it provides the designer with agency-specific requirements and top-level references.

#### **9-2.1 Balance Project Funding and Project Scope.**

Heightened levels of a security system provide increased resistance to intrusion and attack. Increased security brings increased construction costs and complexity. The more complex the system, the more the cost of operation and maintenance will increase. The level of security elements and security requirements need to be identified and reconciled with project funds early in a project. The challenge for the design team is to balance security requirements with life safety, convenience, operation, maintenance costs, and life-cycle costs.

#### **9-2.2 Existing Site Plans and Building Plans.**

Locate and obtain existing site plans and building plans for associated buildings during the planning stage. Include plan drawings for electrical infrastructure, communications infrastructure, riser diagrams, as well as floor plans, installation/base public works, related existing as-built drawings, and structural diagrams. Obtain plan drawings prior to soliciting bids for any ESS work. Computer Aided Design (CAD) drawings are preferred. See appendix C for example CAD Drawings. Conduct site surveys early in the design process to verify the accuracy of the existing plans with regard to current site conditions.

#### **9-2.3 Multi-Organizational Interfaces.**

Meetings with end-users, facility managers, installation/base public works, and security specialists need to be held. Additionally, determine facility and security forces operational requirements.

**Table 9-1 Agency Requirements for Electronic Security Systems**

Agency	Standard	Applies to
U.S. Department of Homeland Security (DHS)	Homeland Security Presidential Directive 12 (HSPD-12)	All government entities (mandatory)
National Institute of Standards and Technology (NIST)	FIPS 201, <i>Personal Identity Verification (PIV) of Federal Employees and Contractors</i>	All government entities (mandatory)
Federal Identity, Credential, and Access Management (FICAM), also known as FIPS 201, <i>Evaluation Program</i>	FIPS 201, <i>Evaluation Program Approved Products List (APL), Physical Access Control System (PACS) Components</i>	All government entities (mandatory)
NIST	SP 800-116, <i>Guidelines for the Use of PIV Credentials in Facility Access</i>	Any government entity
DHS	<i>The Risk Management Process: An Interagency Security Committee Standard</i> , November 2016/2nd Edition	Any government entity
DHS	<i>The Risk Management Process for Federal Facilities</i> , Appendix A: Design-Basis Threat Report (FOUO), 2018 Edition	Any government entity
DHS	<i>The Risk Management Process for Federal Facilities</i> , Appendix B: Countermeasures (FOUO) 2018 Edition	Any government entity
Department of Defense (DoD)	DoDI 5200.08, <i>Security of DoD Installations and Resources and DoD Physical Security Review Board (PSRB)</i>	Any government entity
DoD	DoD Manual 5100.76, <i>Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (AA&amp;E)</i>	Any government entity
Office of the National Director of National Intelligence	Intelligence Community Standard Number (ICS) 705-1, <i>Physical and Technical Standards for Sensitive Compartmented Information Facilities</i>	Any government entity
National Counterintelligence and Security Center	<i>Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, IC Tech Spec – for ICD/ICS 705</i>	Any government entity
DoD	UFC 4-021-02, <i>Electronic Security Systems</i>	Any government entity
DoD	UFC 4-010-03, <i>Security Engineering: Physical Security Measures for High-Risk Personnel</i>	Any government entity
DoD	UFC 4-010-05, <i>SCIF/SAPF Planning, Design, and Construction</i>	Any government entity
DoD	UFC 4-010-06, <i>Cybersecurity of Facility-Related Control Systems (FRCS)</i>	Any government entity
DoD	UFC 4-020-01, <i>DoD Security Engineering Facilities Planning Manual</i>	Any government entity
DoD	UFC 4-020-02FA, <i>Security Engineering: Concept Design</i>	Any government entity
DoD	UFC 4-020-03FA, <i>Security Engineering: Final Design</i>	Any government entity
DoD	UFC 4-022-01, <i>Security Engineering: Entry Control Facilities/Access Control Points</i>	Any government entity
DoD	UFC 4-022-03, <i>Security Fences and Gates</i>	Any government entity
DoD	UFC 4-024-01, <i>Security Engineering: Procedures for Designing Airborne Chemical, Biological, and Radiological Protection for Buildings</i>	Any government entity
DoD	UFC 4-025-01, <i>Security Engineering: Waterfront Security</i>	Any government entity
DoD	UFC 4-141-04, <i>Emergency Operations Center Planning and Design</i>	Any government entity
DoD	UFC 3-501-01, <i>Electrical Engineering</i>	Any government entity

#### **9-2.4 Space Planning.**

The ESS designer must interact early to reserve space requirements in a new building (square footage area) for ESS components such as equipment racks, consoles, operator workstations, and administrative workstations.

#### **9-2.5 ESS Site Surveys.**

Conduct the site survey early in the design process in order to validate existing drawings as well as gather data for any new requirements.

It is important for the design team to collect detailed information about any existing systems. A site survey checklist is included in Appendix B. The items included in the site survey checklist are not all-inclusive; however, it does provide the framework for the user to have general guidance while conducting an ESS site survey. It is up to the user to tailor the checklist to the specific job site and the type of assets to be protected. In general, site surveys include a capacity assessment of existing systems to include, but is not limited to, the following issues:

- IDS: Any expansion capability?
- ACS: How many unused card reader slots are available at what panels?
- What type of access credential is used?
- Is there existing badging (issuing new badges) capability?
- VSS: Is there spare capacity?
- Is there spare video archiving capacity available?
- ESS maintenance: Is the system currently maintained?
- Cybersecurity: Does the system have a current authorization to operate (ATO)?
- Data transmission system type and bandwidth availability
- Approval of radio frequency emitters by local jurisdiction or host nation

#### **9-2.6 Central Monitoring Station.**

Appropriate square footage for the ESS central monitoring station must be allocated early in the design process. If sufficient space does not exist for the current project, the location for the central monitoring station needs to be identified and a scheme for central monitoring made (e.g., a new central monitoring station is required). Determine requirements for central monitoring station connectivity and DTM. Connectivity requirements refer to bandwidth and pathway considerations. Additionally, distance issues and availability of points of connection need to be reviewed. There will be additional project costs if new pathways, additional bandwidth, and new connections are required.

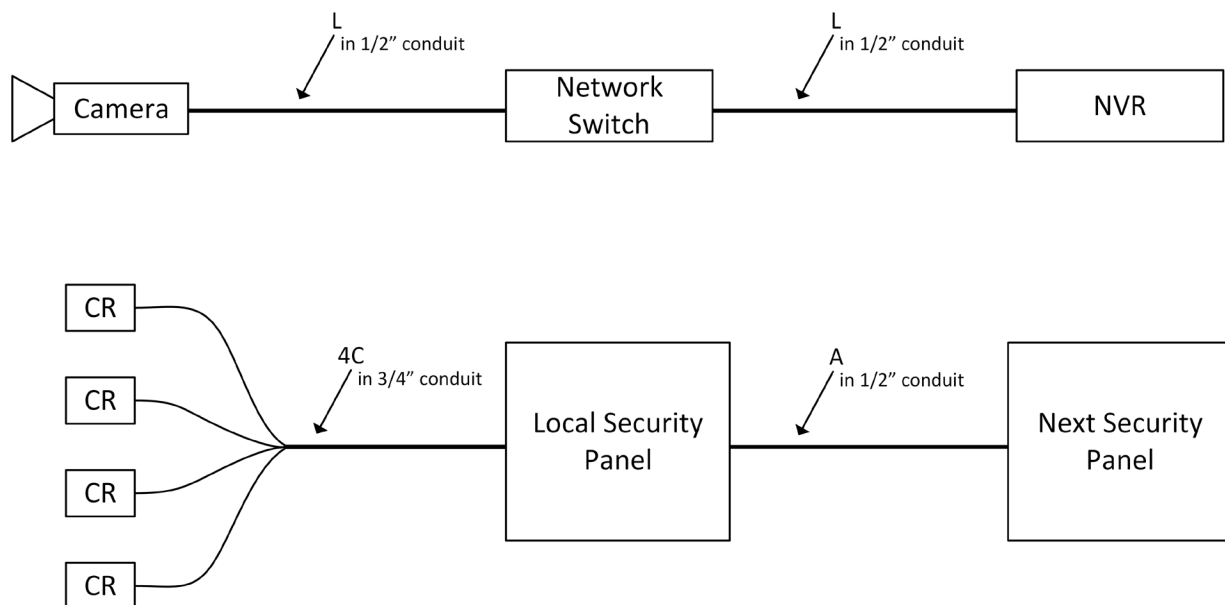
### 9-3 INITIAL DRAWING PREPARATION.

A good start for drawing production is to begin with security plan drawings and a system block diagram.

#### 9-3.1 Cable Schedule.

For identifying different cable types required for a project, a good approach is to use a cable schedule and show the conductor count and cable legend on riser diagrams. This approach is illustrated in Figure 9-1 and Table 9-2.

**Figure 9-1 Cable Counts on Riser Diagrams**



**Table 9-2 Sample Cable Schedule**

<b>Cable Legend</b>	<b>Style</b>	<b>Type</b>	<b>Use</b>
A	#16/1 TSP	Communication Cable Plenum Rated (CMP)	RS-485
C	#20 AWG/3 TSP	Communications Cable Riser Rated (CMR)	Card reader cable
E	#18 Solid/shield	RG-6U	Video
F	2 #12 w/1 #12 ground	THHN	120 VAC wiring
G	#18/1 TP	Communications Cable General Purpose (CMG)	Video
L	8-C	CAT6	Ethernet cable
U	24-strand	50 micron	Fiber-optic cable
W	-----	50 ft HDMI	Workstation to display

### 9-3.2 Functional Matrix.

A document defining the functionality to the system is a useful tool (see example in Figure 9-2).

**Figure 9-2 Functional Matrix**

ACTION		Signal sent to security system at Dispatch Center NVR records camera image Guard verifies alarm with camera UPS system or batteries engage Local door sounder to alarm PTZ Camera focuses on preset location Door unlocks until fire alarm panel is reset Door unlocks Motorized gate opens Response force mobilized									
		A	B	C	D	E	F	G	H	I	J
1	Valid card reader attempt	●							●		
2	"Lost card" attempt	●	●	●							
3	Outdoor microwave sensor alarm	●	●	●			●				
4	Local security panel power loss	●			●						
5	Door held open alarm	●	●	●		●	●				
6	Door forced entry alarm	●	●	●		●	●				
7	Tamper switch activated on local security panel	●									
8	Fixed camera video motion detection activated	●	●	●							
9	Interior motion sensor alarm	●									
10	Tamper notification activated on security device	●									
11	Glass break sensor alarm	●									
12	Fence sensor alarm	●	●	●			●				
13	Fire panel alarm	●						●			
14	Remote door access activated	●							●		
15	Remote gate access activated	●	●							●	
16	Emergency exit door opened	●				●					

### 9-4 BASIS OF DESIGN.

The basis of design (BOD) or design narrative is prepared in the early phases of the design process. It is developed from the project requirements. The BOD presents the technical factors and design parameters required for the project. Typically, a BOD is

done as a report and includes a functional description of systems, a narrative of system requirements, some base drawings such as the functional matrix, and documentation of factors affecting the ultimate design and functionality of a system.

## **9-5 DESIGN DEVELOPMENT PHASES.**

ESS design features include components and software for protecting the assets, as well as physical protection of the components of the ESS. Security systems may store administrative and response procedures to protect the assets in case of an attack. ACS store personnel information, such as credentials, and other personal information needed for authentication. Stored information must be managed in compliance with DoD regulations as well as the specific requirements imposed by the respective Service, DoD agency, or federal agency.

### **9-5.1 Concept Design (35%).**

The 35% design indicates the level of construction and general location of sensor cabling and data transmission cabling from controllers, sensors, and workstations. Sensors, door closures, magnetic or electric locks, and any unique requirements for control and access to areas, spaces or rooms must be called out in the design analysis and drawings. Architectural and electrical drawing schedules for power, door locks, and interior and exterior camera locations must be addressed for coordination of the trades involved.

#### **9-5.1.1 Legends and Abbreviations.**

Provide legends and abbreviations associated with the security system design.

#### **9-5.1.2 Floor Plans.**

Provide representative floor plans.

#### **9-5.1.3 Site Plans.**

Provide site plans showing all exterior camera poles and exterior light fixtures, site utilities, cable/conduit/duct plans for the site as well as exterior system components, panels, and devices.

#### **9-5.1.4 Elevation Drawings.**

Security system drawings will include plan and elevation drawings. Site plans and layouts will show new and existing utilities. Plans will show locations of video cameras, controllers, panels, IDS sensors, fences, and camera poles. If building service equipment and exterior architectural and structural features affect camera view or conflict with controlled ingress and egress requirements for security or life safety, these issues will be addressed as a part of the design. The plans will be coordinated with other utility plans concerning scale, landmark references for proximity, and interference management. The plans will be separate from water, sewage, and other utility plans.

Elevation views of security system equipment, such as camera poles, panels, and fenced areas and gates, will be scaled and will identify each item of equipment.

#### **9-5.1.5 Building Floor and Ceiling Plans.**

Building floor and ceiling plans for interior security systems will include layouts for cameras, sensors, locks, card readers, door controllers, conduits, cable trays, communication equipment, and data transmission systems (video and data) cables. For renovation and modification projects, plans will depict the work and “Work Not in the Contract, or Task Order, or Delivery Order” on all drawings and plans. Where work is extensive, use separate drawing sheets to show existing-to-remain, demolition, and new work.

#### **9-5.1.6 Single-Line Diagrams.**

Single-line diagrams of IDS, VSS, and ACS subsystems must be developed as a part of concept design. Include the over-arching security system block diagram showing the integrated subsystems (for example, ACS, IDS, VSS, CCDE workstations/servers and peripherals, data transmission system components and interfaces). The single-line diagrams for each subsystem must show workstations, controllers, perimeter sensors, panels, and sensor and data transmission conduits and cables.

#### **9-5.1.7 Power.**

Design drawings must depict proposed power sources and devices, controllers, card readers, and communication system interface schemes (interior and exterior). Ensure electrical panel board schedules include power requirements and dedicated circuits for ESS. The diagrams will include existing and proposed overvoltage and surge protection device types in sufficient detail to demonstrate security system protection philosophy. For exterior panels and equipment, lightning protection must be designed and specified. Include grounding, grounding electrode system, and lightning protection system in security system riser diagrams.

#### **9-5.1.8 Affected Systems.**

Drawings will contain nameplate data for components of existing systems that are affected by the new design or that affect the new equipment or systems.

### **9-5.2 Intermediate Design (65%).**

The 65% design must be sufficiently complete to demonstrate design compliance with regulations and applicable criteria. The drawings developed as concept design drawings must include additional detail and requirements.

#### **9-5.2.1 Legends and Abbreviations.**

Include legends and abbreviations throughout the drawings.

#### **9-5.2.2 Scale.**

The floor plans must be drawn to scale.

#### **9-5.2.3 Site Plan.**

Site plans include all camera poles, video equipment panels, exterior lighting fixtures, site utilities, and point of entry of security system cables and sensor wiring, and cable/conduit/duct plans for the site.

#### **9-5.2.4 Exterior Security System Components, Panels, and Devices.**

Provide plan and elevation drawings of security systems. Include new and existing utilities on plans and layouts. Show locations of cameras, lighting fixtures, gate and door controllers, panels, IDS sensors, fences, and exterior pole or building mounting requirements on plans and drawings. Coordinate security system plans with other utility plans concerning scale, landmark references for proximity, and interference management. Provide security system plans separate from water, sewage, and other utility plans. Scale and identify each item of security system equipment in elevation views. Ensure building or site features do not obscure the FOV of camera or conflict with security or life safety requirements. .

#### **9-5.2.5 Building Floor and Ceiling Plans for Interior Security System.**

Include layouts for video cameras, sensors, locks, card readers, door controllers, and conduits, cable trays, communication equipment, and data transmission systems (video and data) cables. For renovation and modification projects, plans will depict the work and “Work Not in Contract” requirements. Where work is extensive, use separate sheets to show existing-to-remain, demolition, and new work.

#### **9-5.2.6 Single-Line Diagrams.**

Add details of components and appropriate features to the concept single-line diagrams for IDS, VSS, and ACS subsystems.

#### **9-5.3 Pre-Final Design (95%).**

The level of detail in the 95% design demonstrates the entire security system and the data transmission systems requirements, including interfaces with other design disciplines. All coordination efforts with other design disciplines will be incorporated before completion and submittal. With the exception of completing minor details, this submittal could be used to obtain fair and competitive bids from contractors and used for construction.

#### **9-5.3.1 Previous Content.**

Content of the 65% design submission and all design progress up to the point of the pre-final submission must be included. All conflicts and all prior approved comments issued prior to the pre-final design submittal are resolved.

#### **9-5.3.2 General Notes.**

Include general notes that provide criteria for general contractor instructions, design criteria for security system and the data transmission systems, construction materials and equipment, and inspections, performance verification and endurance testing, and verification of system(s) intended function. Identify systems or component parts of the security system and the data transmission systems where the DOR is delegating the design responsibility to a qualified delegated engineer.

#### **9-5.3.3 Pertinent Information.**

95% drawings will show all pertinent plans, elevations, sections, details, locks, card readers, controllers, communication interfaces, field distribution panels, door and camera schedules, and notes to present a complete description of the construction/installation required. Properly annotate, locate, and dimension all elements to be constructed/installed.

#### **9-5.3.4 Exterior Security.**

The 95% exterior security system drawings will include:

- Details that clearly depict the installation requirements of overhead and underground data transmission system cables, underground or above-ground exterior sensors, power sources, distribution panels, gate controllers, door controllers, and pole- and building-mounted cameras and lighting fixtures.
- Exterior security systems power and communication cable clearances based on NEC and for over 600-volt power lines as required by IEEE C2, *National Electrical Safety Code(R)* (NESC(R)).
- Lighting levels for exterior areas and equipment, and placement of light fixtures to provide the light to dark ratio based on criteria.
- Plans and details that clearly distinguish new from existing construction and define their interfaces.
- Equipment schedules for all equipment included in the design will be complete.

#### **9-5.3.5 Interior Security.**

The 95% interior security system drawings will include:

- Camera schedule.
- Door schedule for doors controlled with card reader or security locks.
- Electrical power wiring details for all electronic security equipment requiring normal power. Include uninterruptible and/or emergency power and their sources.
- Riser diagram communication network connectivity and interfaces, showing routers, switches, and cables.
- Mounting details for card readers, sensors, electric/security locks, and security system equipment.
- Designation of all rooms and areas as shown on architectural and other drawings.
- Internal and external equipment wiring diagrams, including interconnections between related items of equipment.
- Cable and conduit schedules.
- Security system equipment plan, elevation, side views, sectional views, and details (interior and exterior).
- Interface drawings between existing security systems/equipment and new security systems/equipment.
- Nameplate data for components of existing systems that are affected by the new design or that affect the new equipment or systems.
- Complete schedules for all equipment included in the design.

#### **9-5.4 Final Design (100%).**

The 100% design must be complete in detail to demonstrate the entire security and data transmission systems requirements by including the 95% design submission with the addition of minor details, and resolution of approved review comments provided as a part of the 95% design review. Incorporate all valid comments made on previous submittals into the final submittal. The drawings must be complete in detail to provide for fair and competitive bids from contractors and provide for construction of the project without additional drawings.

### **9-6 BIDDING.**

The bidding phase of a project is a critical part of the ESS lifecycle. If done properly, it will ensure the end-user gets what they need within the timeframe and budget allotted. A number of constraints must be considered for the bidding phase. The more complex a system, the more details need to be provided in the bid package. More information can

reduce the number of questions and potential change orders. Work with the contracting team to develop a proposal response time and a procurement strategy that is consistent with the level of complexity of the system. Include procurement act requirements such as the Buy American Act and Trade Agreements Act (TAA) for country of origin requirements related to the procurement of electronic security products. This can encourage more bidders to participate and increase the quality of responses.

In addition to technical references, provide a concept of operations document. This will help the bidders understand how the systems will be used, give bidders a better understanding of intent, and facilitate more accurate responses. Installers and integrators must be an approved vendor for the system, experienced in the installation, calibration, and programming of ESS. Require a minimum of three years of documented experience for the types of systems the project includes.

## **CHAPTER 10 CROSS-DISCIPLINE COORDINATION**

### **10-1 GENERAL COORDINATION.**

Throughout the planning and design process the designer(s) must coordinate closely with the end-user and their command, physical security and antiterrorism officers, base communications officer, fire and safety personnel, and the installation facilities engineering office. The design team lead must ensure that all security requirements (both physical and electronic) are coordinated between security and other disciplines, which primarily include civil, architectural, electrical, telecommunications (information technology and cybersecurity), and safety. Historically the biggest disconnect in project design and high construction cost is due to a lack of adequate coordination between key stakeholders and engineering disciplines.

The following paragraphs provide examples of areas where cross-discipline coordination is required to properly address security requirements.

### **10-2 END-USER/CUSTOMER.**

Although many design requirements are specified in standard codes and regulatory requirements, the designer(s) must coordinate closely with the end-user to fully understand the end-user's specific operational, functional, and mission-specific security and operational needs. The designer needs to understand how the facility will be used and whether or not the end-user or their higher headquarters utilizes or requires any standard or proprietary ESS equipment to manage, monitor, and control access to their facilities. Understanding what standard equipment, the end-user, site, or command uses is particularly important in relation to cybersecurity standards and existing system accreditations as this information could determine the final design solution required for ESS.

### **10-3 HOST INSTALLATION/BASE.**

The designer(s) must coordinate closely with the end-user's host installation physical security and antiterrorism officers, base communications officer, fire and safety personnel, and the installation facilities engineering office. The designers must understand what site-specific requirements, codes, and constraints may affect the design. Understanding what standard equipment the host installation uses may be particularly important in relation to interoperability, monitoring, cybersecurity standards, and existing system accreditations as this information could also determine the final design solution required for ESS.

### **10-4 CIVIL COORDINATION.**

#### **10-4.1 Gate Control (Vehicle/Pedestrian Gates and Sally Ports).**

Vehicle gates and pedestrian gates, booths, or turnstiles may be equipped with electronic access controls and gate operators/motors. Access controlled gates are often

equipped with a card reader pedestal or mount with a card reader and, in many cases, an intercom system and other associated access control and safety devices.

A sally port is a secure controlled entry and exit portal used for inspections and prevent tailgating. Sally ports may require control hardware for interlocking gates. Refer to UFC 4-022-01, *Security Engineering: Entry Control Facilities/Access Control Points*, for more information on sally ports and entry control points.

#### **10-4.2      Underground Site Work.**

Interbuilding DTM communications are often made by direct buried conductors. Underground site work needs to coordinate with existing civil drawings and known buried utility locations. Coordination with local authorities to receive all approvals and required dig permits is an important step to avoid major damage to existing underground utilities and causing potential catastrophic delays to on-site operations.

#### **10-4.3      Outdoor Perimeter Security Features.**

Perimeter security projects often involve clearing, grading, drainage improvement, erosion control, and paving. These design elements must be coordinated with local site development and environmental representatives. Civil engineering input must be solicited when designing above-ground perimeter security features such as fences, passive vehicle barriers, towers, and poles.

### **10-5      ARCHITECTURAL COORDINATION.**

It is imperative that all ESS (IDS, ACS, VSS, and security intercom) device locations and equipment space requirements be identified early in initial design and planning stages in order to coordinate mounting locations (ceiling, walls, doors), and requirements for electronic access controlled door hardware and locks. Detailed door-by-door coordination reviews must be conducted during design development and creation of construction documents. Require doors with security hardware and sensors to be factory prepped with all required American National Standards Institute (ANSI) cutouts and internal recessed wire ways for security sensors and electronic hardware. Door hardware schedules must be coordinated with security and the designer of record to ensure the door hardware is compatible with the planned ACS and devices. Examples of door hardware items that may be required include, but are not limited to an electrified mortise or push bar exit device with built in REX switch, hinge transfer device, lock power supply, electric strike, magnetic lock, and recessed DPS or HSS. An important benefit of early close coordination with security is the ability to conceal supporting conduit infrastructure and devices within the walls to the maximum extent possible, thus eliminating the need to retrofit and surface-mount conduit and security devices after construction is completed.

Door control impacts (door hardware needs or changes) are sometimes overlooked in project construction cost estimates. Inventory of doors and assessment of door and hardware suitability must be an early design consideration for assessing project door

interface requirements. Door coordination is one of the most frequent (and costly) problem areas on security projects. It is important that the ESS designer coordinate with the project architect to ensure the proper door hardware is specified and installed.

#### **10-5.1 Balance Security with Convenience.**

Other architectural issues that need to be considered include balancing security with convenience, entries and exits, life safety code considerations, space planning, doors, and door locks.

There is a natural conflict between making a facility as convenient as possible for operation and maintaining a secure facility. Security requirement must not be sacrificed for convenience. Proper security controls will reduce the flow rate and ease of ingress and egress for a facility. These issues must be addressed in initial planning to facilitate additional entry points or administrative requirements.

### **10-6 ELECTRICAL COORDINATION.**

Electrical is one of the most important disciplines that must be coordinated with when designing an ESS. Electrical issues that need to be coordinated are discussed in the following paragraphs.

#### **10-6.1 Power.**

When possible, feed the ESS loads from distribution panels within the protected area. A good practice is to use distribution panels with dedicated security system breakers that can be locked. ESS loads must be placed on dedicated circuits.

#### **10-6.2 Backup Power.**

##### **10-6.2.1 Battery Backup.**

Minimum requirements for battery backup are dependent on the type of facility or asset being protected. Some services or assets have minimum independent battery/UPS requirements. Backup power may be provided by batteries, UPS, or generators, or combinations of these devices that meet the minimum requirements for backup power duration, including minimum battery requirements. If a generator or UPS is not available for backup, provide backup with batteries. Space for batteries and UPSs must be provided in communications rooms where the ESS will be located. If a generator is used to provide portions of the backup power, the protected circuits must automatically transfer to the emergency electrical power source.

##### **10-6.2.2 Backup Power for VSS.**

Depending on criticality of an asset and the availability of security forces to assess alarms, consider providing backup power for VSS used for assessing alarm conditions. Where VSS are used for IDS alarm assessment; use backup time in accordance with IDS backup requirements and/or per applicable requirements documents. Backup

power must be provided for VSS that employ video analytics as the primary means of intrusion detection in accordance with IDS power backup requirements and must also be considered when used for surveillance around critical assets. Space for batteries and UPSs must be provided in communications rooms where the ESS will be located to support VSS backup power.

### **10-6.3 Grounding, Bonding, and Lightning Protection.**

Refer to the following documents, as applicable, for specific ESS issues:

- UFC 3-520-01, *Interior Electrical Systems*
- UFC 3-575-01, *Lightning and Static Electricity Protection Systems*
- ANSI/TIA-STD-607, *Telecommunications Bonding and Grounding (Earthing) for Customer Premises*
- NFPA 70, *National Electrical Code (NEC)*
- NFPA 780, *Standard for the Installation of Lightning Protection Systems*

### **10-6.4 Surge Protection.**

Provide surge protection devices for all ESS communications identified in NFPA 780 in accordance with UFC 3-520-01. Ensure space in communications rooms where ESS is housed to provide such surge protection.

Provide surge protection devices for UPS and generators in accordance with UFC 3-520-01. Ensure space in communications rooms where ESS is housed to provide such surge protection.

### **10-6.5 Electromagnetic Interference (EMI).**

Interference can be introduced to unprotected communication lines that are in close proximity to electrical power wiring, radio frequency sources, large electric motors, generators, induction heaters, power transformers, welding equipment, and electronic ballasts. Protection from EMI includes avoiding the sources of the interference by physical separation; shielding wire lines by means of specialty wiring (coaxial, twisted shielded [foil] pairs, and metal sheathed cables); and metallic conduit systems.

### **10-6.6 Tamper Protection.**

Tamper protection is required for all sensors, card readers, and enclosures containing a splice or connection. Tamper protection for ESS can be physical protection, line supervision, encryption, and/or tamper alarming of enclosures and components. All tamper alarm signals must be continuously monitored, whether the system is in the access or secure mode of operation.

### **10-6.7 Cable Type.**

Data communication signals are sensitive to changes in capacitance and resistance associated with different cable types. Digital “1s” and “0s” trigger on sharp LRC (inductance, resistance, and capacitance) time constants. Specify the cable type that meets the equipment manufacturer’s minimum specifications, DoD and/or Service-specific technical standards, and NEC requirements (for example, riser-rated and plenum-rated). Where standards conflict, the designer must use the most stringent standard regarding electrical safety and performance.

#### **10-6.7.1 Cable Routing.**

Install all conduit and cabling associated with the ESS within the perimeter of the protected area to the greatest extent possible. A communications link from a protected area to a central monitoring system is an obvious exception to this guideline.

#### **10-6.7.2 Signal and DTM Supervision.**

Line supervision is a term used to describe the various techniques designed to detect or inhibit manipulation of communication networks. All signal and DTM lines must incorporate some level of line supervision. Line supervision for ESS must detect and annunciate communication interruptions or compromised communications between field devices, workstations, and the associated central system. Field device signals must be supervised by monitoring the circuit and initiating an alarm in response to opening, closing, shorting, or grounding of the signal. DTM supervision must initiate an alarm upon any manipulation or disruption of the signal.

#### **10-6.7.3 Encryption.**

ESS encryption requirements may be affected by the security network architecture. Coordination may be required with the network designer/owner to ensure proper encryption of the ESS data and ensure compatibility.

#### **10-6.7.4 Physical Protection of Exterior ESS.**

All exterior intrusion detection sensors and access control readers must have tamper-resistant enclosures and integral tamper protection switches. All enclosures, cabinets, housings, boxes, and fittings having hinged doors or removable covers that are protected by employed sensors must be locked, welded, brazed, or secured with tamper-resistant security fasteners and be tamper-alarmed. Route exterior ESS sensor communication and power cables that are not directly protected by sensors by the following methods:

- In rigid or intermediate metal conduit as defined by NFPA 70
- In concrete-encased duct
- In conduit buried a minimum of 2 feet (0.6 meter) below finished grade

- Suspended at a minimum of 15.5 feet (4.5 meters) above finished grade

#### **10-6.7.5 Physical Protection of Interior ESS.**

Coordinate between security and electrical disciplines to ensure all intrusion detection sensors, access control readers, and assessment equipment located outside controlled areas have tamper-resistant enclosures. At a minimum, coordinate the following design criteria

- Install all ESS cabling within the protected area to the greatest extent possible.
- All enclosures, cabinets, housings, boxes, and fittings having hinged doors or removable covers must be locked, welded, brazed, or secured with tamper-resistant security fasteners and be tamper-alarmed.
- Metallic conduit that leaves a SCIF, SAPF, or other locations with TEMPEST requirements necessitates a decoupling (such as an insert of nonmetallic conduit or a dielectric break) when exiting the area.
- For ordnance facilities, metallic conduit must be run underground for at least 50 feet (15 meters) from the structure. Refer to UFC 3-575-01 for additional requirements.
- Comply with applicable security policy requirements for installing IDS communications wiring in conduit. Apply security policy for the specific asset being protected. For example, security policy for SCIFs requires the following: "IDS-associated cabling that extends beyond the SCIF perimeter must be installed in rigid conduit or must employ line security and meet other security requirements." There is no universal requirement for IDS wiring to be installed in conduit.

#### **10-6.8 Radio Frequencies (RF).**

Designers planning or proposing the use of RF devices must coordinate with the frequency manager and host nations for frequency allocation to verify the devices are approved for use.

RF systems must employ some form of tamper protection, such as the following:

- The security system must use dedicated frequencies to transmit ESS alarm data.
- The system must detect and report intentional and unintentional jamming attempts.

#### **10-6.9 Voltage Drop Considerations.**

Standard voltage drop calculations need to be made by the designer for calculating ESS conductor size. This is especially important for VSS cameras, which may be located

some distance from interior termination cabinets and may be located outside. The system designer must meet voltage drop requirements in accordance with NEC.

#### **10-6.10 Harmonics.**

Harmonics in a power system are typically the odd multiples of 60 Hz, such as 180 Hz and 300 Hz, and are generated by switching power supplies such as in a computer, by adjustable frequency motor drives, by lighting ballasts, by UPS systems, by electric welders, and by other rectifier type equipment. Harmonics in a system are measured in total harmonic distortion (THD).

##### **10-6.10.1 Impacts in a Power System.**

Harmonics in a power system can cause overheating of cables and equipment along with false operations. NFPA 70 requires designs to consider harmonics and IEEE 519 is a reference standard. When a neutral of a multiphase feed has significant harmonics, it is to be oversized. UL and IEEE have methods for de-rating standard transformers for harmonics.

##### **10-6.10.2 Mitigation.**

Mitigation of harmonics involves either isolating the harmonic source from the rest of the power system or isolating sensitive equipment from the harmonics. Methods of mitigation involve oversized/de-rated standard transformers or harmonic K-rated transformers (K4 or K13 being common), oversized neutrals in distribution systems (full size is adequate for feeds to individual equipment), input line reactors or output filters (usually on motor drives), and surge suppressors at panelboards, wall receptacles, power bars, or built into the input of end loads, such as a security panel.

##### **10-6.10.3 Electrical Noise Reduction.**

To further reduce electrical noise, a copper equipment ground sized per NFPA 70 (unless the cable is already shielded) and copper grounding electrode conductors sized per NFPA 70 may be run in raceways in addition to bonding metallic raceways and enclosures together.

#### **10-6.11 Raceway.**

All conduit, wire way, and raceway must meet the requirements of NFPA 70.

Conduit runs may have a maximum of three 90-degree bends or any combination of bends not to exceed 270 degrees.

#### **10-6.12 Labeling.**

Cables must be labeled at origination, termination, and entry into and exit from enclosures with permanent labels.

### **10-6.13 Shielding.**

When required, shielded cable must only be grounded at one end, typically back at the local security panel to prevent open loop grounds.

### **10-6.14 Intercom System.**

While not a requirement, site-specific factors may require provision of an intercom or similar auxiliary communication system at entry portals (such as motorized gates) to facilitate communication between personnel requesting entry and the monitoring station or other answering location.

### **10-6.15 Lighting.**

While not an official part of ESS, lighting is an effective part of the overall physical protection design. Refer to UFC 3-530-01 for additional guidance. Lighting may be considered as a countermeasure for protection of each critical asset. Coordinate with the electrical/lighting engineer for placement of lighting to enhance viewing of VSS, as discussed in Chapter 5.

Lighting at guard checkpoints must be sufficient to clearly allow a guard to verify the picture ID on access badges. Some installations may provide a fixed camera at an automatically operated gate for both surveillance and verification of a visual credential for access. In these cases, lighting must similarly be sufficient to allow accurate verification of the picture ID.

## **10-7 LIFE SAFETY AND FIRE PROTECTION COORDINATION.**

Applicable life safety and existing codes/standards must be met. In the event of an emergency, building occupants must be able to follow emergency procedures quickly and safely. The ESS designer must coordinate with the DFPE, as defined in UFC 3-600-01 (for items such as exit plan considerations and fire alarm system integration) to implement security without comprising life safety code standards. Physical security system designs need to be coordinated with and comply with NFPA 101, *Life Safety Code*, and *Architectural Barriers Act (ABA) Accessibility Standard for Department of Defense Facilities*.

### **10-7.1 Fire Alarm System.**

In the United States, most egress doors are required to unlock (in the path of emergency egress) in the event of a fire emergency. (**Note:** Certain institutional facilities are exempt from this automatic door-unlock requirement, for example, prisons, hospitals, and other high-security facilities). Methods vary on how this may be accomplished. The designer must coordinate with the DFPE, as defined in UFC 3-600-01 to ensure the design meets the requirements of NFPA 101. If free egress hardware is supplied (which is possible when electric locks or electric strikes are used), then that is all that is required. If magnetic locks are supplied, this life safety function

has to be achieved by interfacing the ACS with the fire alarm system. The ESS design needs to include the elements identified below for system interface:

- Wire and conduit from the fire alarm system to the security system. It is required that the power and communication lines not be placed in the same conduit.
- Assignment of fire alarm input/output addresses. The fire alarm system sends a signal (fire alarm system output) to each individual door controller in the event of a fire alarm signal.
- Assignment of security system input/output addresses.
- Termination of the fire alarm/security system interface on the fire alarm system.
- Termination of the fire alarm/security system interface on the security system.
- Programming of the fire alarm system to achieve door unlock signals in the event of a fire alarm signal.
- Programming of the security system to achieve door unlock signals in the event of a fire alarm signal.
- Door access control hardware all needs to be “home run” to a local junction box for ease of troubleshooting and repair.

#### **10-8 MATERIAL ENTRY CONTROL.**

Other mandates will dictate specific requirements, but the following are typical considerations for material entry control as it relates to ESS and physical security:

- Separate material entry control circulation from general facility traffic.
- Loading docks are typically monitored by fixed cameras.
- Rollup doors are typically monitored by an interior point sensor, such as a DPS.
- Shipping and receiving areas are typically caged or secured with a restricted access scheme, such as a higher card access hierarchy level.

*This Page Intentionally Left Blank*

## **CHAPTER 11 SYSTEM TESTING, TRAINING, AND FINAL DOCUMENTATION**

### **11-1 OVERVIEW.**

The purpose of this chapter is to provide guidance ensuring effective execution of the final stages of an ESS procurement and installation project. Although this is not always the case, ideally at this point all of the equipment is fully installed and the remaining requirements will ensure an effective transition from the installation contractor to the end-user and allow for efficient transition into a maintenance and services contract if one is to be implemented. This section consists of three major components: training, system acceptance testing (SAT), and final documentation. The details of each component are further described below.

### **11-2 TRAINING.**

Training is an important part of the system installation process, not only for the user of the system but also for the contractor. An otherwise perfectly installed and highly capable system is rendered worthless if the end-user can't perform simple configuration and maintenance tasks on the system. Without sufficient training, the system will not serve its purpose, but will also become resource heavy as it requires frequent service calls to make simple changes. In an ideal case, the system will have been fully pre-acceptance tested (PAT) by the contractor, and training will be performed just before SAT such that the system operator (or maintainer) is fully trained before the system is in full-time operation. The system designer must take into account the following considerations when planning for system training: accommodation for multiple sessions due to guard shifts or other details; provisions for how training is provided such that it can be easily re-taught in cases where system operators may be highly dynamic due to military reassignments; special requirements for specific training timelines (for example, require system training after the system receives a successful SAT, due to no personnel on-site in new construction build). Careful planning throughout the entire design and installation process will produce a higher quality end-product.

#### **11-2.1 Training Types.**

There are three typical types of training, including operator, administrator, and maintenance training. General requirements for each training type are described below. The specification must clearly define which types of training are required; the quantity of people for which the training is required; the quantity of sessions (if more than one) required; and any specific details required to be included in each type of training.

### **11-2.1.1 Operator Training.**

Operator training provides the trainee the skills they need for day-to-day use of the system as a full-time system operator. Training is normally separated into modules (and potentially separate training sessions if deemed necessary by the designer) by disciplines of ESS to include IDS, ACS, and VSS. Typically, making changes to the system is limited, and training tends more toward the lines of acknowledging alarms, manipulation of camera views, or monitoring personnel who pass through ACS portals.

#### **11-2.1.1.1 IDS/ACS Operator Training.**

IDS/ACS operator training includes, but is not limited to:

- System operation procedures
- System configuration orientation
- Alarm acknowledgment
- Alarm response logging
- Graphics functionality
- Any special information required for operation with integrated systems

#### **11-2.1.1.2 VSS Operator Training.**

VSS operator training includes, but is not limited to:

- System operating procedures
- Limited system configuration
- Video call-up operation
- Camera and monitor control
- Graphics functionality
- Basic device terminology and troubleshooting
- Any special information required for operation with integrated systems

### **11-2.1.2 Administrator Training.**

Administrator training is typically held for a limited number of people who will have the highest access level to the system. Training is normally separated into modules (and potentially separate training sessions if deemed necessary by the designer) by disciplines of ESS to include IDS, ACS, and VSS. It includes all the training from the operator training but also more advanced training to make higher level system modifications. It will include, but not be limited to, the following.

#### **11-2.1.2.1 IDS/ACS Administrator Training.**

IDS/ACS administrator training includes, but is not limited to:

- System operation and configuration procedures
- Operator functions
- Database functions and setup
- Card holder input and deletion procedures
- Report generation
- Applications programs (as applicable)
- Graphics generation and manipulation
- Items unique to the ACS and IDS interfaces with other systems
- System backup and restore
- Any special information for operation or configuration with integrated systems

#### **11-2.1.2.2 VSS Administrator Training.**

VSS administrator training includes, but is not limited to:

- Modification to camera's associated with camera call-up
- Addition of new cameras
- Setting of home location for PTZ cameras
- Setup for any video analytics
- Any configuration between integrated systems

#### **11-2.1.3 Maintenance Training.**

The system maintenance training is intended to provide training on the basic tasks required to keep the system(s) in proper operation. The course may be provided for government-employed system maintainers where no maintenance contract is in place, or a government-contracted maintainer in the case that the installation contractor is not the same contractor who will be providing maintenance services. It may also be useful for the end-user, such that they have better awareness of the duties their contracted maintainer will be performing. The course is typically taught at the project site after endurance test completion for a period of five training days, but can be adjusted as necessary. The training includes:

- Physical layout of each piece of hardware
- Troubleshooting and diagnostics procedures

- Component repair and replacement procedures
- Maintenance procedures and schedules, including system testing after repair
- Calibration procedures; upon course completion, the students will be proficient in system maintenance
- Review of site-specific drawing package, device location, communication, topology, and flow

### **11-2.2 Training Plan.**

Tailor the ESS specification (UFGS 28 10 05) to require the submittal of a training plan to ensure the contractor fully understands the training required to be provided. At a minimum, the plan must include a narrative description of all training being provided; an overall training schedule (to include all training that is to be provided); specific course agendas for each module being taught and aligning with major topics within the training manuals (for example, ACS administrator training and IDS operator training); and a full text copy of all training materials to be used in each course (include electronic copies of videos or other documents if they are part of the training content). Submittal of the training plan well before the actual training is to take place, ensuring sufficient time is given for revisions in cases where the submission is inadequate. This will also allow for proper schedule coordination with the end user or stakeholders.

### **11-2.3 Training Content.**

The training will be oriented to the specific systems being installed. Training content will include training manuals and audio-visual materials as needed. Early coordination with system users is again important. If it is known that there will be frequent turn-over of operator personnel, it may make sense to specify the entire training be constructed such that it can be initially documented through video or electronic presentation, allowing the content to be easily re-taught to new personnel. Typically, training manuals will be delivered for each trainee with two additional copies (normally hard and electronic copies) delivered for archiving at the project site. The manuals will include an agenda, defined objectives for each lesson, and a detailed subject matter description for each lesson. The manuals will also include any manufacturer's product data or literature needed to supplement the description and training narrative, whether by physical inclusion or by referencing the documents in the manual. The contractor will furnish audio-visual equipment if required and other training materials and supplies to the trainees as needed. The contractor will also provide copies of the audio-visual materials to the end user such that the training manuals are a complete representation the actual training provided and can be provided to future staff as a training aid. This is typically done by including a compact disc (CD) or digital video disc (DVD) that also includes electronic copies of the manuals, or a separate CD or DVD when delivering printed manuals.

#### **11-2.4 Training Personnel Requirements.**

The ESS specification will include requirements of personnel that will be performing the role of training instructor, and typically also provide a means for the contractor to provide confirmation that these requirements will be met. At a minimum, it is good practice to require the instructor to be certified to work on the systems they are instructing on, as well as have had some level of past experience in doing so.

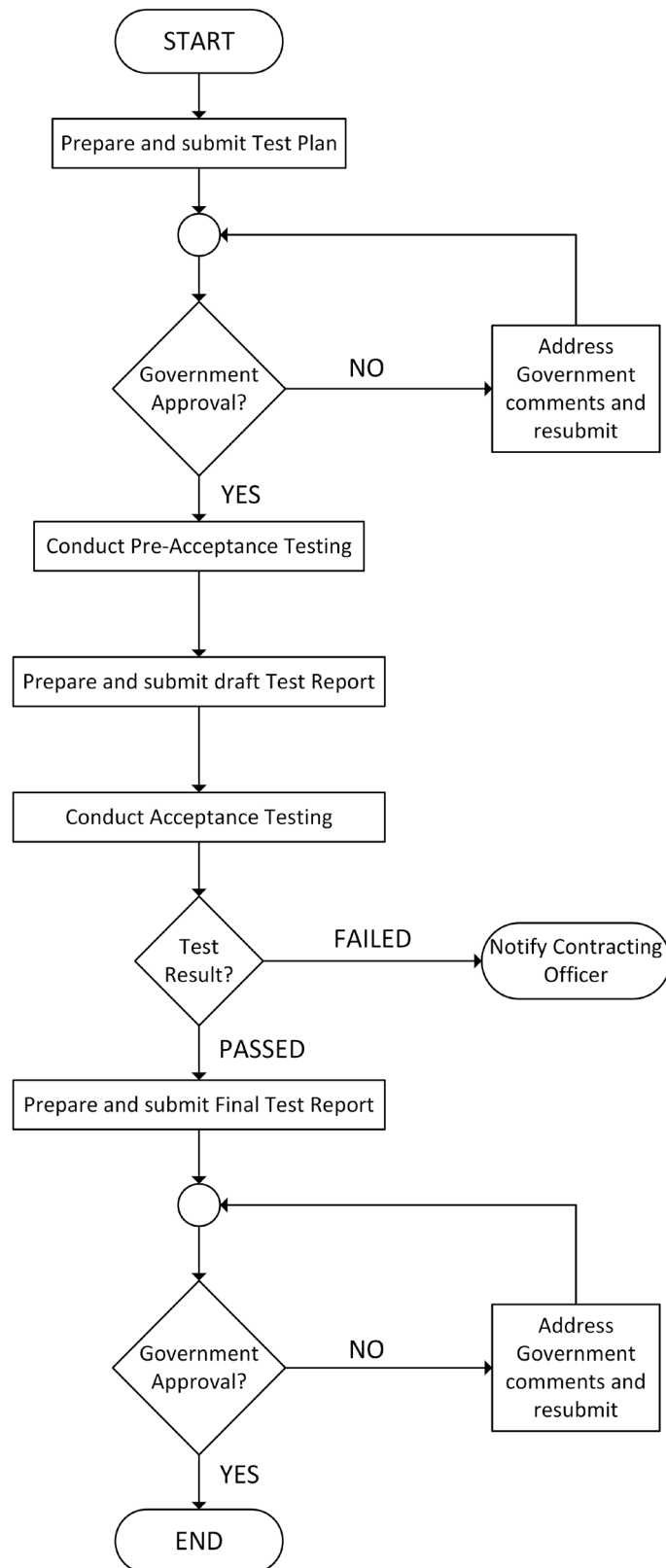
### **11-3 SYSTEM ACCEPTANCE TESTING (SAT).**

#### **11-3.1 General.**

The process for SAT is a critical element of the contract execution that ensures operational readiness and contract compliance, while also ensuring the end-user receives a product that meets their expectations and the applicable requirements of the respective agency or department. A full assessment of the system operation and expected behavior ensures a 100% tested and fully operational system at the time of system turn-over and commencement of the warranty period. This is beneficial to both system owner and the installation contractor. A general outline of the process can be seen in the Figure 11-1 flowchart. System testing components include:

- Test plan
- PAT
- SAT
- Final test report
- Government acceptance

Figure 11-1 SAT Process Flowchart



### **11-3.2 Test Plan.**

The ESS technical specifications or scope of work must include requirements for the ESS installation contractor to conduct comprehensive testing of every component and feature in order to demonstrate acceptable system performance to the government. This section discusses SAT process and procedures. The plan will be a tool for both the contractor in PAT and the government in SAT, ensuring proper contract execution. It must be submitted to the government for review and acceptance prior to any testing being completed on the system. To avoid delay to contract execution, care needs to be taken to submit the plan with ample time allotted for government review, comment resolution and correction, and acceptance before testing commences (including contractor pre-acceptance testing).

#### **11-3.2.1 General Description.**

The first section of the test plan outlines the basic roles and responsibilities of all participants in the collective SAT and lays out the outline of how the tests and test phases will be executed. It also describes how the sub-parts listed below will be incorporated and used within the testing.

##### **11-3.2.1.1 Personnel Roles and Responsibilities.**

The intent of SAT is for the contractor to successfully demonstrate to the government representative that they have met the requirements of the contract. This typically means that the contractor will be performing all test functions and executing the test. The government's purpose as a participant is to witness the SAT and facilitate coordination at the site such that testing is allowed to proceed as necessary. This may require coordination with on-site personnel for awareness, to request assistance in completion of testing activities, or clearing personnel from test areas to allow the contractor to successfully complete the testing. The roles of all participants of the SAT must be clearly stated in this section of the test plan, and may include test director, operator, technician, test intruder, and any other personnel that will be performing test activities.

##### **11-3.2.1.2 Test Equipment/Personnel.**

The test plan must clearly identify who is responsible for providing materials, personnel, or equipment required to successfully complete a 100% test of the system. Typically, any materials, equipment, or test personnel required are the responsibility of the contractor to provide. This may include equipment such as volt or light meters, ladders, screwdrivers, man-lifts, and/or any personnel/equipment to perform tasks such as crawl, climb, run, or jump tests for exterior sensors or observe workstations for proper alarm initiation. When the contractor is the responsible party, then they must not rely on the government to provide any resources for testing the system.

### 11-3.2.2 Test Procedures.

The contractor must provide test procedures for every component of the ESS. These procedures will be detail and specifically tailored to the site and equipment being tested. For example, do not state that an exterior fence sensor will be tested by manufacturer's recommendations (too vague), but state the specific test to be performed, the steps required to perform that test, and the quantity of iterations required to be completed where applicable (such as, validating probability of detection or confidence rates). At a minimum, the test procedures will provide the following:

- Provide a step-by-step procedure for conducting each functional test.
- Describe actions to be performed and the expected results from each step of the procedure.
- Ensure performance standards described in contract specifications are addressed.
- Ensure any specific requirements from the contract-specified criteria are met.

A sample test procedure can be seen in Figure 11-2 or visit [https://www.wbdg.org/FFC/NAVGRAPH/example\\_test\\_procedures\\_logs.pdf](https://www.wbdg.org/FFC/NAVGRAPH/example_test_procedures_logs.pdf) for a full listing of previously generated sample procedures. If a previously generated procedure doesn't fit the equipment to be tested, the contractor must modify an existing procedure or create a new procedure as needed.

Figure 11-2 Sample Test Procedure

PVT PROCEDURES		SITE NAME
<b>TEST NO:</b>	70	<b>OBJECTIVE:</b> To verify that this feature performs in accordance with the manufacturer's specifications.
<b>TITLE:</b>	Gate Access Control & Safety Devices	
<b>REFERENCE:</b>	UFGS 28 20 01.00 10 (13720), Section 2.8.5.10	
INITIAL CONDITIONS		
Real-time communication is established with the operators at the primary and remote stations. Gate shall be closed and operational.		
TEST EQUIPMENT		
a. If the gate is equipped with a bumper detector, a small hammer shall be provided. b. Passenger car / truck or large metal object to test the safety loops. c. Door magnet to simulate gate forced open. d. Gate Emergency Release Pull Station Reset Key.		
<u>EVENT</u>		<u>EXPECTED RESULTS</u>
70.1 <u>Access Request</u>		
a. Direct the test subject to initiate a valid access request.	•	The gate card reader shall indicate a valid card read and the gate shall open. Access granted will appear at the operator console. The gate shall close after the internal time limit has expired.
b. Direct the test subject to initiate an invalid access request.	•	The gate card reader shall indicate an invalid card read and the gate shall remain closed. Access denied will appear at the operator console.

### 11-3.2.3 Test Logs.

The test logs are an important part of system acceptance. Not only do they provide records for system acceptance to the end-user at the system turnover stage but can also heavily influence the efficiency in execution during the functional testing phase of both the PAT and SAT. When properly constructed, the logs can provide guidance and direction on a logical path of progression through the various sensors or equipment to be tested, while reducing redundant trips back to the same piece of equipment to test different functions. When the logs are lackadaisically constructed without thought given to a logical flow, testing may require the expenditure of unnecessary effort searching several pages for tests on a single device and reducing overall testing efficiency, when some forethought could easily avoid the issue and concisely depict the complete test logs for that device on a single page. Other important items to consider are validation for proper documentation of serial numbers and IP addresses, accurately listed equipment location and enclosure information (for example, Building 2, IDB #2, and door controller #2), and ensuring that there is enough space provided in the log page to record all test data for each test, as well as the inclusion of some space for taking notes. Sample test logs are included at [https://www.wbdg.org/FFC/NAVGRAPH/example\\_test\\_procedures\\_logs.pdf](https://www.wbdg.org/FFC/NAVGRAPH/example_test_procedures_logs.pdf) and serve as a basic outline. For a more detailed version of an example test log, which tends toward proper planning as described within this section, see Figure 11-3.

Figure 11-3 Example Test Log

SENSOR / ALARM POINT INFORMATION							LINE OF DETECTION TESTS				SENSOR ONLY TESTS				CAMERA CALL UP			
LOC	DEV	INPUT	ALARM POINT #	VICADS	LOCATION DESCRIPTOR	TYPE	WALK	RUN	JUMP / CUT	CRAWL / CLIMB	PASS	FAIL	TAMPER	SUPERVISION	ALARM MONITOR 1	ALARM MONITOR 2	ALARM MONITOR 3	ALARM MONITOR 4
FDB 1	Vindicator AES-1500-A SN = aaaa 1:131 - IP ADDR = xxx.xx.xxx.xxx	N/A																
		1	13102		Perimeter Zone 1 R1	Microwave												
		2	13103		Perimeter Zone 1 R2	Microwave												
		3	13106		Perimeter Zone 2 R3	Microwave												
		4	13107		Perimeter Zone 2 R4	Microwave												
		5	13201		Perimeter Zone 1 T1	Tamper												
		6	13202		Perimeter Zone 1 T2	Tamper												
		7	13203		Perimeter Zone 2 T3	Tamper												
		8	13204		Perimeter Zone 2 T4	Tamper												
		AUX 1	13205		Perimeter Pole 1 CCTV Box	Tamper												
		AUX 2	13206		Perimeter Pole 2 CCTV Box	Tamper												
		AUX 3																
		AUX 4																
		AUX 5	13210		Perimeter FDB 1 IDS PS	AC Fail												
		AUX 6	13211		Perimeter FDB 1 IDS PS	Low Batt												
	Vindicator AES-1500-B SN = aaaa 1:132 - IP ADDR = xxxxx	N/A																
		1	13104		Perimeter Zone 1 IR1	PIRAMID												
		2	13108		Perimeter Zone 2 IR2	PIRAMID												
		3	13101		Perimeter Zone 1	Fence												
		4	13105		Perimeter Zone 2	Fence												
		5	13212		Perimeter FDB 1 APU 1	Fault												
		6	13207		Perimeter FOPP	Tamper												
		7	13109		Perimeter Maxiris Tx	IR												
		8	13110		Perimeter Maxiris Rx	IR												
		AUX 1																
		AUX 2																
		AUX 3																
		AUX 4	13208		Perimeter FDB 1	Tamper												
		AUX 5	13209		Perimeter FDB 1 CCTV PS	AC Fail												
		AUX 6																

#### **11-3.2.4 Schedule.**

A schedule must be provided that outlines the contractor's projected timeline for completing testing. Including the PAT, SAT (including any endurance testing), and timeframe for submission of the final test reports. This allows for proper scheduling of resources for both the contractor and government personnel participating in the overall acceptance testing.

#### **11-3.3 Pre-Acceptance Testing.**

The contractor must conduct a complete test of all field equipment, workstations, and central system hardware and software in accordance with the approved test plan. This ensures that when the government representative arrives to witness the SAT, all system anomalies have already been discovered and remediated as necessary, facilitating an efficient acceptance test without failure. The test director must be on site to conduct a pre-test inspection and oversee all testing activities. Prior to testing, the test director will visually inspect all ESS components and correct deficiencies in workmanship and neatness as needed. Verify equipment to ensure all that was proposed is on-site, installed, and documented with accurate locations, as well as model and serial numbers recorded. During the pre-test inspection, the accuracy of red-line drawings will be verified and updated as needed. Failure to complete all the steps as outlined herein greatly increases the probability for a failed SAT, resulting in potential credits due to the government. PAT will be conducted in two phases: functional testing followed by burn-in testing. The ESS technical specifications or scope of work must include requirements for the ESS installation contractor to perform PAT and provide the results of the test in a draft test report.

##### **11-3.3.1 Functional Pre-Acceptance Testing.**

During the functional pre-acceptance testing (FPAT) phase, the system performance is verified by proceeding through each of the test procedures for each piece of equipment, as approved in the test plan. If a failure occurs, take corrective action and retest the item until the expected result occurs. Record the results in the test logs, including a written explanation of each failure, stating the cause, corrective action, and results of the retest. Continue functional testing until all tests have been successfully completed with no unresolved failures.

##### **11-3.3.2 Burn-In Testing.**

The purpose of burn-in testing is to allow time for observation and discovery of any deficiencies or anomalies that were not apparent during the functional testing phase; hence, burn-in testing may only begin after successful completion of all functional testing. A frequently occurring burn-in testing failure is nuisance or false alarms that are not seen until the system has been running for an extended period of time. For example, a dual-technology PIR and microwave motion sensor is installed and successfully detects all attempts at intrusion during functional testing but fails burn-in testing due to unintended detection of traffic driving on an adjacent road (nuisance

alarm) and at a rate that exceeds what is allowable by the applicable policy documents. Burn-in testing may be performed on all systems, but the duration will be scaled according to system complexity and size. Typical durations of burn-in testing are 24 hours for a small single zone IDS to 120 hours for a multi-zone system with interior and exterior IDS, access control, and VSS integration. It is important to note that when multiple systems are integrated together, the final burn-in test may not commence until all system integration is complete. During the burn-in testing phase, the ESS will be placed in normal operating mode and system performance evaluated for the pre-determined duration. During this time, the ESS must be fully functional and programmed such that all features can be exercised and evaluated through normal use. Record all system anomalies in the approved test logs, including a description of each anomaly and any actions taken in response. Any minor deficiencies observed during the course of testing must be immediately corrected. After a failure is corrected, repeat functional tests for components and features associated with the failure. Once satisfied with the repeated functional testing, repeat full burn-in testing on the failed component and then continue with the remainder of the burn-in test. A properly executed burn-in test will put the contractor in a favorable position for a successful endurance test when required as described in paragraph 11-3.4.4, and result in a well-tuned system delivered to the end-user.

#### **11-3.3.3 Draft Test Report.**

The test director must prepare, sign, and submit a draft test report detailing the results of the PAT and that the system is ready for SAT. Refer to paragraph 11-3.4.4 for required content.

#### **11-3.4 System Acceptance Testing.**

SAT is one of the most important parts of any contract, as it is the final system check witnessed by a government representative before system acceptance and turnover. This phase, when properly executed, ensures the end-user receives a high-quality product, meeting expectations and setting a foundation for a system that will operate efficiently with minimal issues through its lifetime.

##### **11-3.4.1 Notification of System Readiness.**

Require the contractor to provide notification to the contracting officer that all PAT and corrections have been completed and the system is ready for SAT at least 15 days before the expected SAT start date in the case of a typical system. This threshold may be adjusted in the specification as needed, depending on system specifics or other requirements such as complexity of travel for the government representative to system location, complicated access requirements/required preparations to enter the site, or any other projected circumstances where more time is required. This notification is intended as a mechanism to ensure the contractor is confident the system will pass SAT and is in full compliance with all requirements, but also a measure for reducing wasted resources on planning and travel to the site which could be prevented with a properly executed PAT.

#### **11-3.4.2 Visual Inspection and Equipment Verification.**

The contractor must assist the government representative to conduct a visual inspection of ESS equipment and wiring. This is typically completed in conjunction with the initial steps of functional SAT (FSAT) (see paragraph 11-3.4.3) but could be included as a separate phase in large or complicated systems. This inspection will focus on the general neatness, quality of workmanship, and compliance with applicable codes and the manufacturers' recommended installation methods. Assess proper labeling at each end of cables used in installation of the ESS, including communication and power cables. This inspection also serves as a verification that the equipment models and locations previously approved are congruent with what is actually installed on-site. Provide a comprehensive listing of installed equipment and software (including model and serial numbers). Provide a complete set of ESS red-line drawings to be used and marked up as necessary during the inspection. Document any deficiencies identified in the approved test logs or on the red-line drawings as necessary. Provide completed logs and marked-up red-line drawings as a part of their final test report.

#### **11-3.4.3 Functional System Acceptance Testing.**

The contractor must test the ESS in accordance with the approved test plan and begin FSAT upon arrival of the government representative at the project site. Verify the system meets all requirements of the specification and complies with the specified standards. The contractor must execute the approved test plan and comply with requests from the government representative to repeat functional tests previously performed during PAT. The government reserves the right to request the contractor to repeat all functional tests or a representative sampling as a means of performance verification and may elect to adjust the quantity or type of tests they intend to witness at any time during the test. If the PAT has been properly executed and the system exhaustively tested as intended, then the FSAT phase can typically be completed efficiently and with minimal deficiencies discovered. In general, it is beneficial to begin with the intent to fully test the entire system and scale back if a sufficient quantity of tests are passed without failure (this is generally a judgment call for the government representative). If deficiencies arise during testing, discuss possible causes and corrective measures with the government representative and obtain government approval before making any adjustments, repairs, or modifications. Making any changes may require a re-test of the entire system or zone being tested and, at a minimum, requires a complete retest of the affected device.

**Note:** There are Service policy documents that may require an exhaustive 100% testing of system components at the FSAT in order to validate metrics such as probability of detection and/or confidence rate is in compliance with acceptable rates. The contractor must add all test results to approved test logs for inclusion in the final test report.

##### **11-3.4.3.1 Failed Test.**

The government retains the right to terminate testing at any time the ESS is found to be incomplete or fails to perform as specified. Such termination of system testing

constitutes a failed SAT. Consider writing the specification to hold the contractor financially responsible for all government travel, labor, or other costs associated (may include costs for contract modifications if required) with a failed SAT. This will provide a level of assurance that the contractor has indeed done due diligence and fully tested the system for conformance before the government representative arrives at the site.

#### **11-3.4.4 Endurance Testing.**

The purpose of endurance testing (ET) is to demonstrate system reliability and operability under normal operating conditions for an extended period of time. The intent is to flush out any deficiencies that weren't immediately apparent during the FSAT phase. The FSAT is sometimes not representative of normal operating conditions due to constraints or conditions that can't be prevented; for example, a new construction facility with an ACS requiring a certain system throughput, where construction conditions won't allow for a representative number of personnel under normal operating conditions until after the functional testing phase is complete. ET may be required per the applicable policy documents or simply desired for higher confidence that the system will perform as intended under normal operations. Most small and/or less complicated systems will not require an ET but consider an ET in environments more prone to nuisance and false alarms, such as exterior IDS (for example, bi-static microwave sensors, exterior dual-technology systems, fence-mounted IDS, and buried line sensor systems). When ET is required, government approval is required before proceeding from FSAT phase to ET phase. Generally, ET is not done until all specified system training is complete and all outstanding deficiencies have been satisfactorily corrected.

##### **11-3.4.4.1 Testing Duration and Phasing.**

If an ET is specified, the testing duration is generally between five and 30 days. The duration is specified based on system complexity. In some cases, the duration may be specified by a policy document (for example, AR-159 requires a continuous 30-day ET). Historically, there have been two testing phases and two assessment/review phases. When not required to be a continuous test, the default was first a 15-day testing period followed by five days to provide analysis and authorization to proceed to the next phase. Next, another 15-day period is repeated with another five days for presentation of the final analysis and report. Testing durations and phases may be adjusted as desired by the designer with coordination with the system user.

#### **11-3.4.4.2 System Assessment and Analysis.**

During ET, the contractor will monitor the system, gather and analyze data, and provide updated reports to the government in accordance with the specification such that deficiencies can be identified in a timely fashion. Testing plan will include monitoring plan, such as a contractor physically on-site to monitor VSS data collection from system operators/guards. Usually, it is best to have the contractor on-site monitoring the system to theoretically get more accurate results. Sometimes this is not possible due to space requirements or otherwise and collection of information by the guard force must be relied upon. In the latter case, it is important to ensure the guard force is fully aware of their documentation requirements such that a useful report can be presented. The specified requirement for analysis/reporting frequency is determined by system complexity and the site's unique security posture. It may be desirable to have someone from the contractor on-site monitoring the system 24 hours per day with tabulation and report at the end of each day or it may be desirable to simply review system reports and interview system operators once a week to compile data and compute false alarm/nuisance alarm rates for a weekly report. A more frequent requirement for provided analysis will likely result in quicker identification of issues such as high false and nuisance alarm rates and can provide data to allow a decision on whether early ET termination might make sense.

#### **11-3.4.4.3 Endurance Failure and Re-test Requirements.**

Generally, where test termination is required due to a failure, once the repair is complete the component itself must be verified again through the FSAT phase. Once completed, ET can re-commence. In some cases, as directed by the government representative, entire zones or the entire system may have to again pass through FSAT. When a deficiency is discovered, discuss corrective options, depending on the severity of the deficiency. Continued monitoring and assessment may be considered in the case of a borderline deficiency in hopes that the system may still pass. In the case of a major defect or component failure, early termination of the current test phase, with subsequent repair and then restart of testing, may be warranted. As detailed above, an ET failure generally consists of a considerable amount of re-testing. Consider the case where an endurance testing period is required to be 30 days and a failure is identified on day eight. The decision is made to continue with the remainder of the test, yet the end result is still a failed ET. In this case, considerably more time is lost than if the requirement was only for a 10-day ET duration. Thought given to these outcomes may have bearing on the duration of testing selected (when not a hard policy requirement) (see paragraph 11-3.4.4.2), but also in a decision on how to continue when a deficiency is identified.

#### **11-3.4.4.4 Final Test Report.**

To close out the SAT phase, the contractor shall submit a final test report following the successful completion of FSAT (or ET if required), including resolution of all non-compliant items. Address the following topics in the final test report.

#### **11-3.4.4.4.1 Summary.**

Provide a chronological summary of all testing (including PAT). Describe test activities and results in narrative form.

#### **11-3.4.4.4.2 Personnel.**

Provide a list of all contractor and government personnel who participated in the testing.

#### **11-3.4.4.4.3 Test Logs.**

Provide all completed test logs along with a test log verification signed by the test director.

### **11-3.5 Government Acceptance.**

Government acceptance is the point at which the contractor's warranty service begins at the completion of SAT. In cases where an ET is required, the warranty normally begins at the point at which the government representative declares a successful ET and the final test report is approved. When ET is not required, the warranty period begins at the declaration of a successful FSAT phase, including approval of the final test report.

### **11-3.6 System Turn-over.**

System turn-over occurs directly after declaration of government acceptance and marks the final step in the contract or task order completion. It includes the turn-over of final documentation documents as defined in paragraph 11-4. It may include completion of DD Form 1354 to transfer real property, as in cases where buildings or fences were constructed as a part of the ESS contract. It may also include any final documentation stating the system was successfully installed and tested and is formally turned over to the end-user in accordance with any regulations (for example, AR 190-59, *Chemical Agent Security Program*, requires completion of DA Form 4604 be provided to the end-user at the turn-over stage).

## **11-4 FINAL DOCUMENTATION.**

The final documentation consists of all the completed and finalized documents that will be provided to the end-user and intended as a package presenting the entire picture of the ESS. The final documentation submittals are the last submittals provided from the contractor to the government and consist of the final test report, operations and maintenance (O&M) manuals, final as-built drawings, and warranty documentation. Each must be specified as a requirement in any ESS contract.

### **11-4.1 Final Test Report.**

The final test report shall be included as a requirement of the SAT and is fully defined in the SAT section above but is included here for completeness. This report provides the results of system testing to the user. It provides a record showing the system has been

fully tested to ensure proper and correct installation and any deficiencies have been corrected and re-tested. The final report provides a level of confidence that the user will have few or no issues with the system due to quality of ESS installation.

#### **11-4.2 Operations & Maintenance Manuals.**

O&M manuals are vitally important to being able to both fully understand and operate the system but also to keep the system in a fully operating status for the foreseeable future. Unfortunately, they are often overlooked if not provided as a requirement to the contractor. The O&M manuals consist of all manuals published by the manufacturer that relate to installation, programming, configuration, and troubleshooting of all components of the ESS. These are not product data sheets that simply provide the technical specifications of the equipment being installed. The manuals will include information such as how to setup the graphical display on an IDS workstation, how to add or remove users or restrict time zones in an ACS, how to modify or add camera call-ups in an integrated VSS, and how to properly ground a surge suppression device. The O&M manuals are not always easily obtainable for the general public; hence, it is very important the end-user receives these from the contractor providing the ESS. Generally, a hard copy will be stored in an easy-to-find area, such as a server room or under a system console, and also an electronic copy so it can be viewed on a device and hard copies can be printed.

#### **11-4.3 Final As-built Drawings.**

The final as-built drawings are the visual representation of the entire system. They must include all details of the system down to the specific landing of wiring to the individual panels. The full details of the system or specific component of the system must be able to be determined from the drawings without having to be physically present at the actual device. "Typical" type wiring diagrams will be limited unless supplemented with a wiring matrix listing the end-to-end connections of all equipment. A complete set of drawings will greatly simplify the job for personnel performing maintenance duties, result in reduced down-time and quicker resolution for system issues, and result in a likely reduction in maintenance work order calls due to an overall better-maintained system. Ensure that all as-built drawings are accurate and correct before final approval, as this is likely the tool to be used most heavily by the system user.

#### **11-4.4 Warranty Documentation.**

The contract specification will provide a minimum warranty of one year on parts and labor for all components installed during contract execution. As part of the final documentation, the contract specification must require a letter of warranty, which provides all pertinent information in regard to the warranty being provided. Include contractor points of contact (POC) information and phone numbers for warranty calls, terms of warranty, and a list of all equipment installed under this task order. In addition, this list of equipment must include vendor, model number, serial number, warranty start date, contractor's warranty expiration date, and equipment manufacturer's warranty expiration date.

*This Page Intentionally Left Blank*

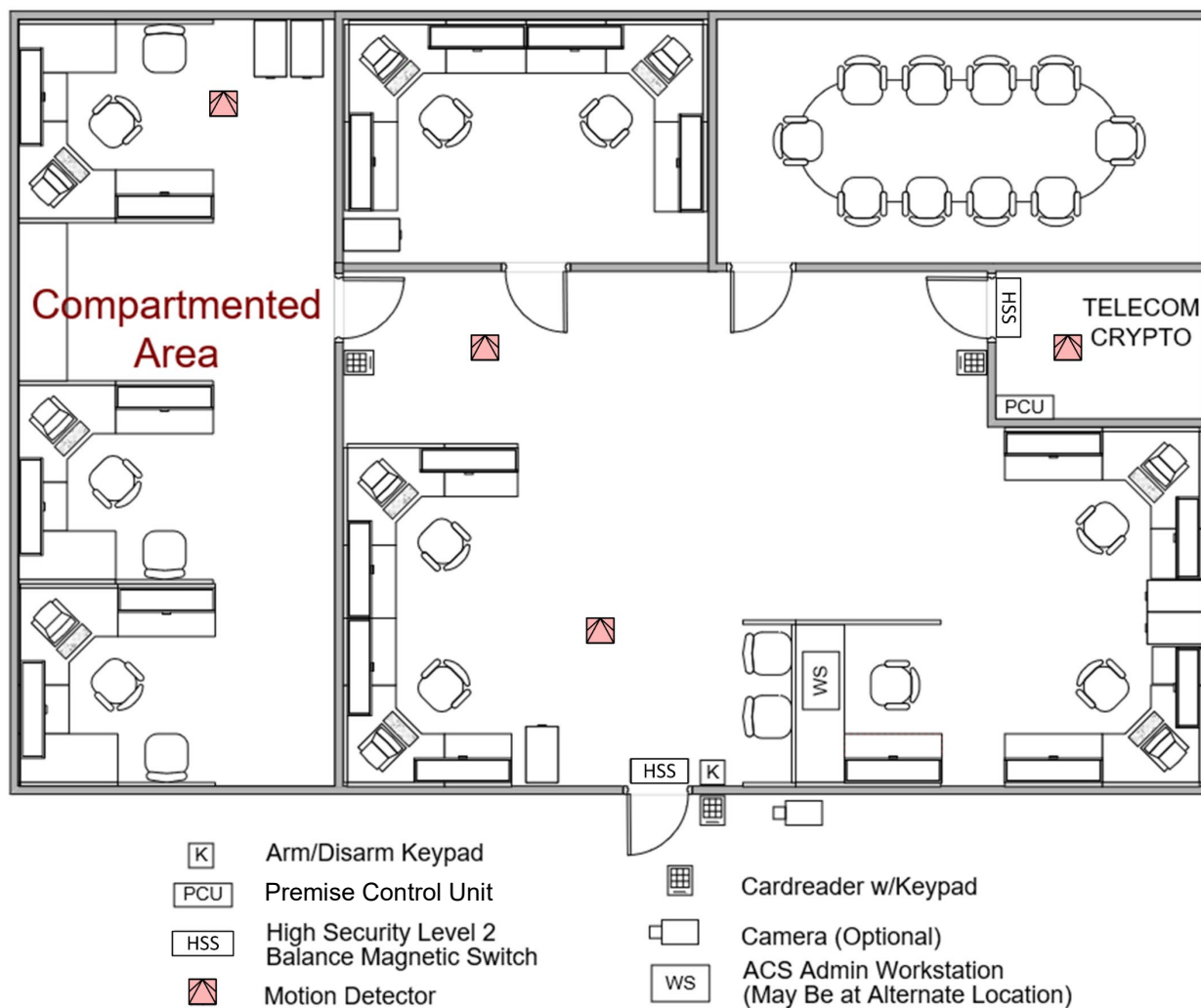
## APPENDIX A INTERIOR IDS ZONE EXAMPLES

The best practices appendix is considered to be guidance and not requirements. Its main purpose is to communicate proven facility solutions, systems, and lessons learned, but may not be the only solution to meet the requirement.

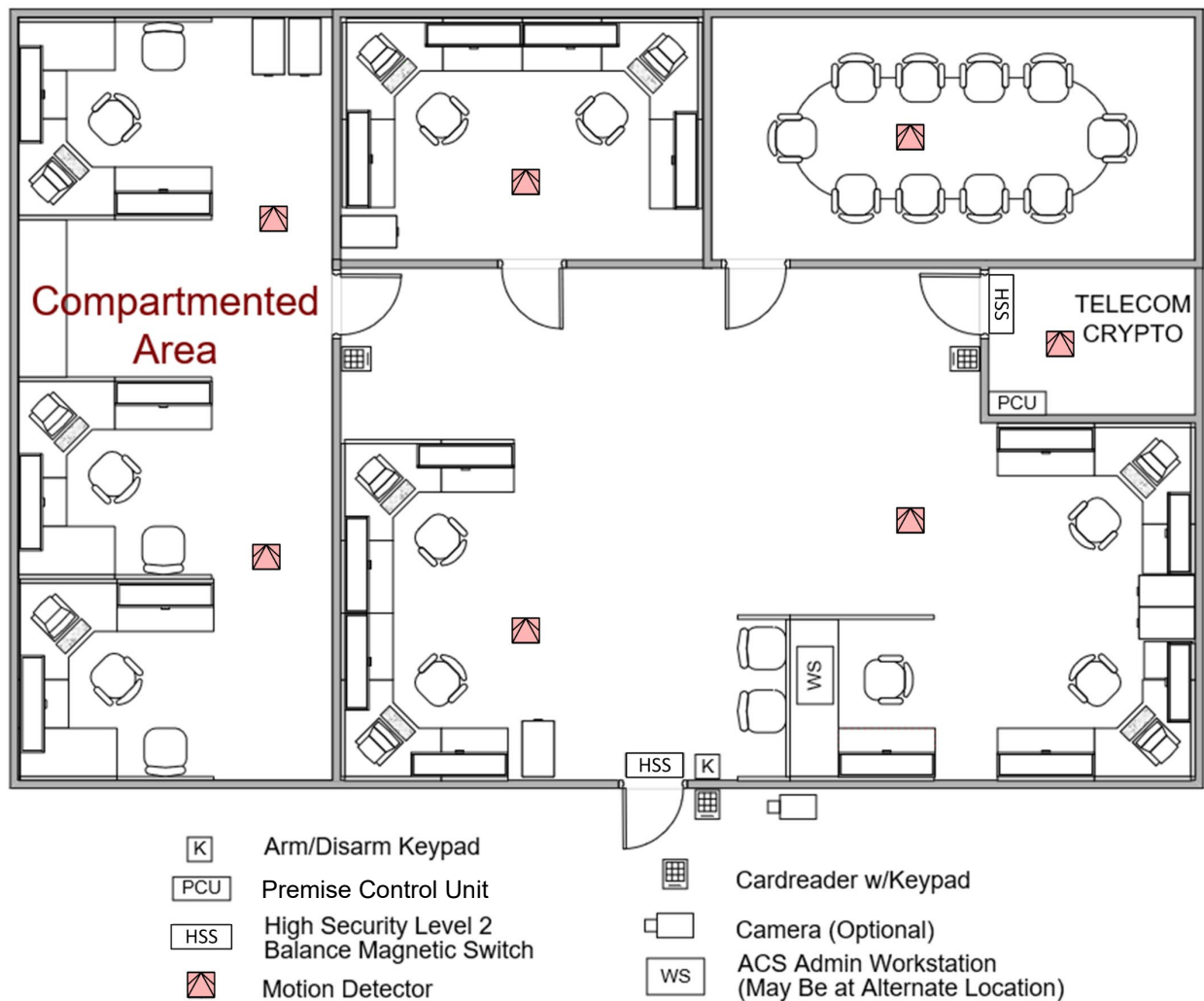
The information in this appendix is intended to help the designer understand and apply policy-directed IDS requirements. It is not comprehensive, as it addresses only a few high-security assets and summarizes only the most critical technical requirements. Using this information as a starting point, the designer must identify all security policies that pertain to each project and ensure all IDS requirements are addressed in the design.

### A-1 SENSITIVE COMPARTMENTED INFORMATION FACILITY AND SPECIAL ACCESS PROGRAM FACILITY.

#### A-1.1 Coverage Based on Cognizant Security Authority Written Designation of Security-In-Depth



## A-1.2 Coverage Based on No Written Designation of Security-In-Depth



## A-1.3 DoD Criteria Document.

- UFC 4-010-05, *SCIF/SAPF Planning, Design, and Construction*

## A-1.4 Policy Baseline.

- Director of National Intelligence, *Intelligence Community Standard (ICS), Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, IC Tech Spec – for ICD/ICS 705*
- DoD Manual 5205.07, Volume 3, *DoD Special Access Program (SAP) Security Manual: Physical Security*
- DoD Manual 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*

#### **A-1.5 Baseline Intrusion Detection System Requirements.**

- Must be protected by an IDS when not occupied.
- Provide sensors on all doors and man-passable openings on the secure perimeter. Provide motion sensors within the secure perimeter to protect all windows (less than 18 feet [5.5 meters] above the ground or from the nearest platform affording access), doors, and man-passable openings and detect movement within to include possibly compartmented areas if required by the SCIF AO or Special Access Program Central Office (SAPCO).
- Provide an IDS arm/disarm keypad at primary entrance.
- For facilities outside the U.S. and in Category I and II countries, motion detection sensors above false ceilings or below false floors may be required by the SCIF AO or SAPCO.
- The plans for IDS, including the extent of coverage, must be approved by the SCIF AO or SAPCO.
- Emergency exit doors must be secured with an FF-L-2890 pedestrian lock and emergency egress device, alarmed, and monitored 24 hours per day.
- Interior areas of a SCIF through which reasonable access could be gained, including walls common to areas not protected at the Sensitive Compartmented Information (SCI) level, must be protected by IDS consisting of motion sensors and Level 2 HSS unless the AO determines that a facility's security programs consist of layered and complementary controls sufficient to deter and detect unauthorized entry and movement.
- IDS must be installed in accordance with UL 2050 Extent 3, which is detailed in UL 681, and consist of:
  - Point sensors that meet UL 634 Level 2 HSS standard.
  - Motion detection sensors must be UL 639 listed. Dual-technology sensors may be used when authorized and when each technology transmits alarm conditions independent of the other technology ("or" configuration).
- PCUs must be located within the perimeter of a SCIF, display alarm status, identify alarms, and display activated sensors.
- SCIF and SAPF utilities (power and signal) distribution on the interior of a perimeter wall treated for acoustics or RF must be surface mounted, contained in a raceway, or an additional wall must be constructed using furring strips.

IDS status is typically monitored outside of the SCIF/SAPF at a centralized alarm monitoring station. Only changes in status (access and secure) and alarm events are reported to the monitoring station. The ability to arm and disarm the IDS zone and to

make administrative changes to IDS PINs and system passcodes and passwords is limited to SCI indoctrinated personnel for SCIFs.

**A-1.6 Tamper Protection.**

- All IDS systems, including any ACS equipment, must be equipped with tamper detection devices that must be monitored continuously, whether the system is in the access or secure mode of operation. Upon detection, an alarm (not fault) condition must be transmitted to the PCU and monitoring station.
- IDE cabling that extends beyond the SCIF perimeter must employ encrypted line security or be installed in a closed and sealed metal conveyance, defined as a pipe, tube or the like, constructed of ferrous electrical metallic tubing (EMT), ferrous pipe conduit, or ferrous rigid sheet metal ducting. All joints and connections must be permanently sealed completely around all surfaces (for example, welding, epoxy, and fusion). Set screws must not be used. The seal must provide a continuous bond between the components of the conveyance. If a service or pull box must be utilized, it must be secured with a GSA-approved combination padlock or AO-approved key lock.
- All system sensors should be located within the perimeter of the SCIF. Cabling between all sensors and the PCU must be dedicated to the system, contained within the SCIF. With AO approval, sensors external to the SCIF perimeter and any perimeter equipment used may be connected to the IDS, provided the lines are installed on a separate zone and routed within grounded conduit.

**A-1.7 External Transmission Line Security.**

- Any system transmission line leaving the SCIF to the monitoring station must meet NIST FIPS for certified encrypted lines. PCUs certified under UL 1610, *Standard for Central-Station Burglar-Alarm Units*, must meet FIPS 197 or FIPS 140 encryption certification and methods. For PCUs certified under UL 1076, FIPS 140 is the only acceptable encryption certification and method. Alternative methods must be approved by the AO.

**A-1.8 Emergency Backup Electrical Power.**

- Twenty-four hours of uninterruptible backup power is required. This may be provided by batteries integral to the ESS, UPS, generators, or any combination thereof. In the event of primary power failure, the system must automatically transfer to an emergency electrical power source without causing alarm activation.
- An audible or visual indicator at the PCU must provide an indication of the primary or backup electrical power source in use. Equipment at the

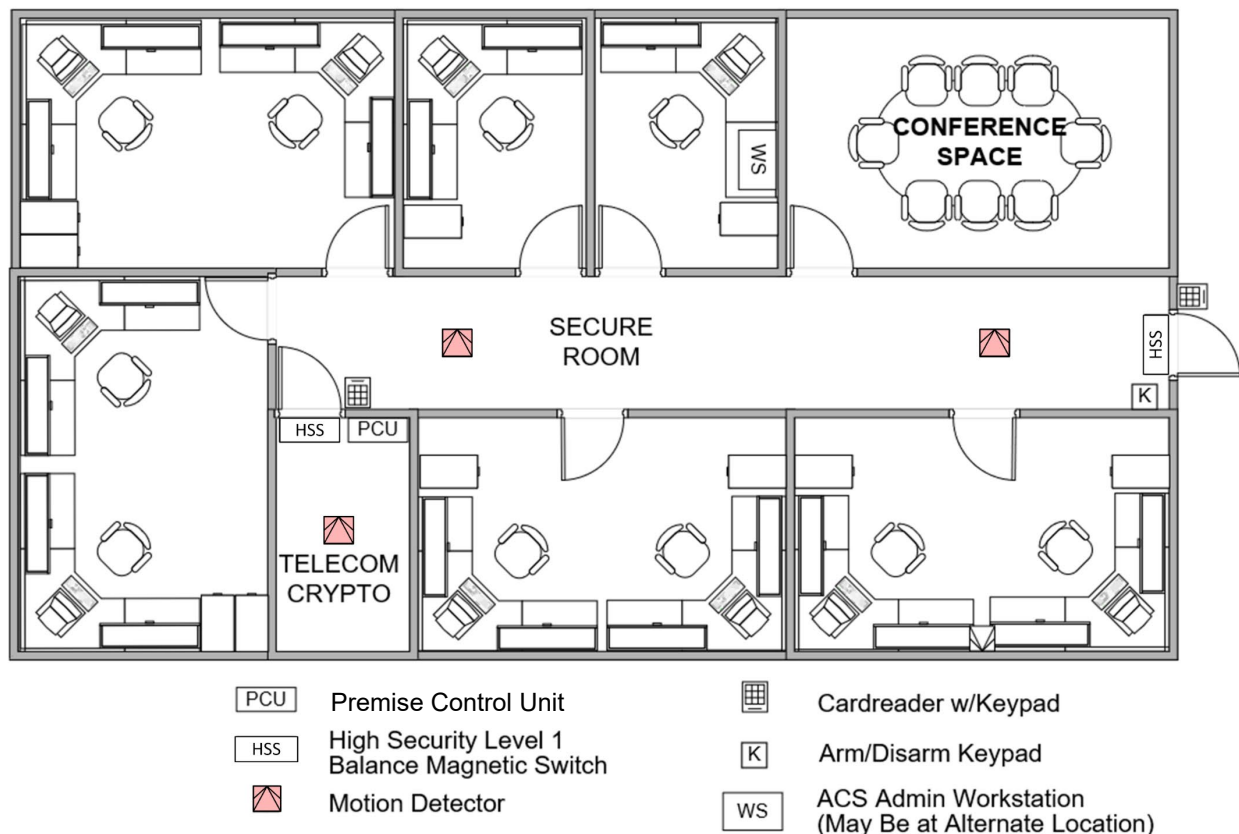
monitoring station must visibly and audibly indicate a failure in a power source or a change in power source. The individual system that failed or changed must be indicated at the PCU or monitoring station as directed by the AO.

### A-1.9 Optional Equipment.

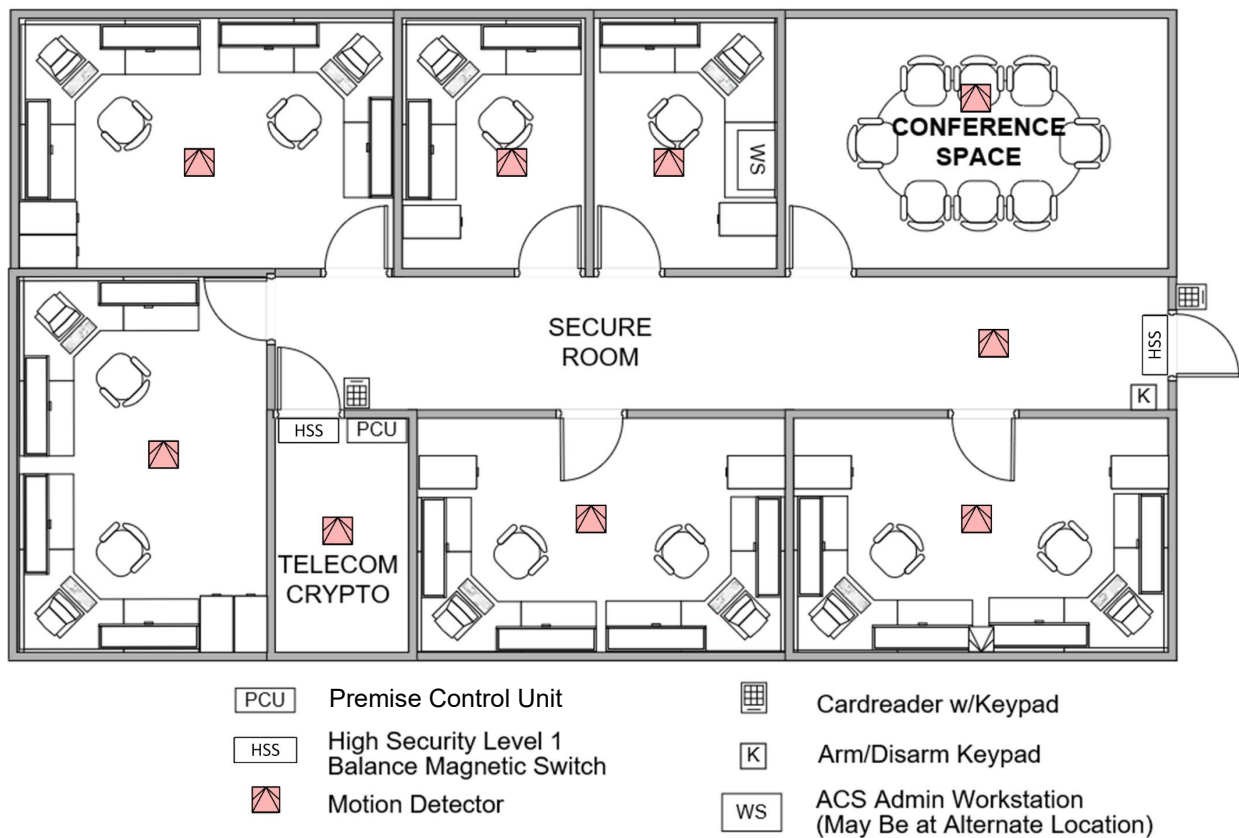
- External VSS camera to monitor primary entrance.
- Access to SCIF/SAPF must be controlled by SCI-indoctrinated personnel or by an approved ACS to ensure physical access is limited to authorized personnel only. While access to more than one SCIF/SAPF may be controlled by a centralized ACS, the computer equipment containing the access-control software program must be located inside the SCIF, inside another approved SCIF within the same command or agency, or inside an approved Secret controlled area. At no time may an ACS located in an unclassified space be used to control entry into a SCIF/SAPF.

## A-2 SECURE ROOM (TOP SECRET OR SECRET OPEN STORAGE)

### A-2.1 Coverage Based on Cognizant Security Authority Written Designation of Security-In-Depth



## A-2.2 Coverage Based on No Written Designation of Security-In-Depth



## A-2.3 Policy Baseline.

- DoD Manual 5200.01, Volumes 1 through 3, *DoD Information Security Program*
- AFMAN16-1404 vol. 1-3, *Department of the Air Force Information Security Program*
- AR 380-5, *Army Information Security Program*

## A-2.4 Baseline Intrusion Detection System Requirements.

- Must be protected by an IDS when not continuously manned or under constant surveillance. If an IDS is not required, a continuously manned secure area should be equipped with an alerting system on all potential entrances into the secure area that cannot be observed by the occupants.
- Secure areas that reasonably afford access to the security container or area where classified data is stored must be protected with motion detection sensors. All readily accessible windows (within 18 feet [5.5 meters] of ground level or from the nearest platform affording access) must be protected by an IDS, either independently or by the motion

detection sensors within the space, whenever a secure room is located within a controlled compound or equivalent and forced entry protection of the windows is not provided.

- All perimeter doors and man-passable openings into the secure area must be protected by a UL 634 Level 1 HSS. A UL 634 Level 2 HSS is preferred due to higher resistance to magnetic tampering.
- IDS arm/disarm keypad at primary entrance.
- Perimeter emergency exit doors must be secured, alarmed, and monitored 24 hours per day.
- IDS must be installed in accordance with UL 681 and consist of Level 1 HSS that meet UL 634 and/or other government-approved sensors.
- PCUs must be located within a secure room.

#### **A-2.5 Tamper Protection.**

- All IDS systems, including any ACS connected, must be equipped with tamper detection devices that must be monitored continuously whether the system is in the access or secure mode of operation. Upon detection, an alarm (not fault) condition must be transmitted to the PCU or monitoring station.
- System associated cabling that extends beyond the protected area perimeter must be installed in conduit and must employ electronic line supervision. Electronic line supervision will entail a polling or multiplexing system or equivalent.
- All system sensors must be located within the protected area.
- Cabling between all sensors and the PCU must be dedicated to the system, contained within the protected area.

#### **A-2.6 External Transmission Line Security.**

- When the transmission line leaves the facility and traverses an uncontrolled area, Class I or Class II line supervision must be used. Class I is highly preferred, which includes encryption standards certified by NIST or another independent testing laboratory.

#### **A-2.7 Emergency Backup Electrical Power.**

- Eight hours of uninterruptible backup power is required. This may be provided by a UPS, batteries integral to the ESS, generators, or any combination thereof. In the event of primary power failure, the system must automatically transfer to an emergency electrical power source without causing alarm activation.

- A visual indicator at the PCU must provide an indication of the primary or backup electrical power source in use. Equipment at the monitoring station must visibly and audibly indicate a failure in a power source or a change in power source.

### A-3 ARMS STORAGE AREA (ARMORY, ARMS ROOM, READY ISSUE ROOM).



#### A-3.1 Policy Baseline.

- DoD Manual 5100.76, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (AA&E)
- OPNAV Instruction 5530.13, *U.S. Navy Conventional Arms, Ammunition, and Explosives Physical Security Policy Manual*
- MCO 5530.14A, *Marine Corps Physical Security Program Manual*
- DAFI 31-101, *Integrated Defense (ID)*
- AR 190-11, *Physical Security of Arms, Ammunition, and Explosives*
- DESR 6055.09, *DoD Explosives Safety Standards*

### **A-3.2 Baseline Intrusion Detection System Requirements.**

- Must be protected by an IDS when not continuously manned or under constant surveillance.
- All perimeter doors and operable man-passable openings into the storage area must be protected by UL 634 Level 1 HSS. A UL 634 Level 2 HSS is preferred due to higher resistance to magnetic tampering.
- The storage area must be protected by interior volumetric sensors.
- Duress alarm at all issue ports.
- IDS arm/disarm keypad at entrance and for all separated (unit-based) interior storage areas that require an independent IDS capability.
- Perimeter emergency exit doors must be secured, alarmed, and monitored 24 hours per day.
- IDS must be installed in accordance with UL 681 and consist of:
  - Level 1 HSSs that meet UL 634 and/or other government-approved sensors.
  - UL 639 listed motion detection sensors.
- AA&E with controlled inventory item codes (CIIC) A through H, K, L, O, S, T, U, 7, and 9 require compliance with DoD 5200.01V3 to house the PCU in the protected space.
- For hazardous locations, refer to DESR 6055.09.

### **A-3.3 Tamper Protection.**

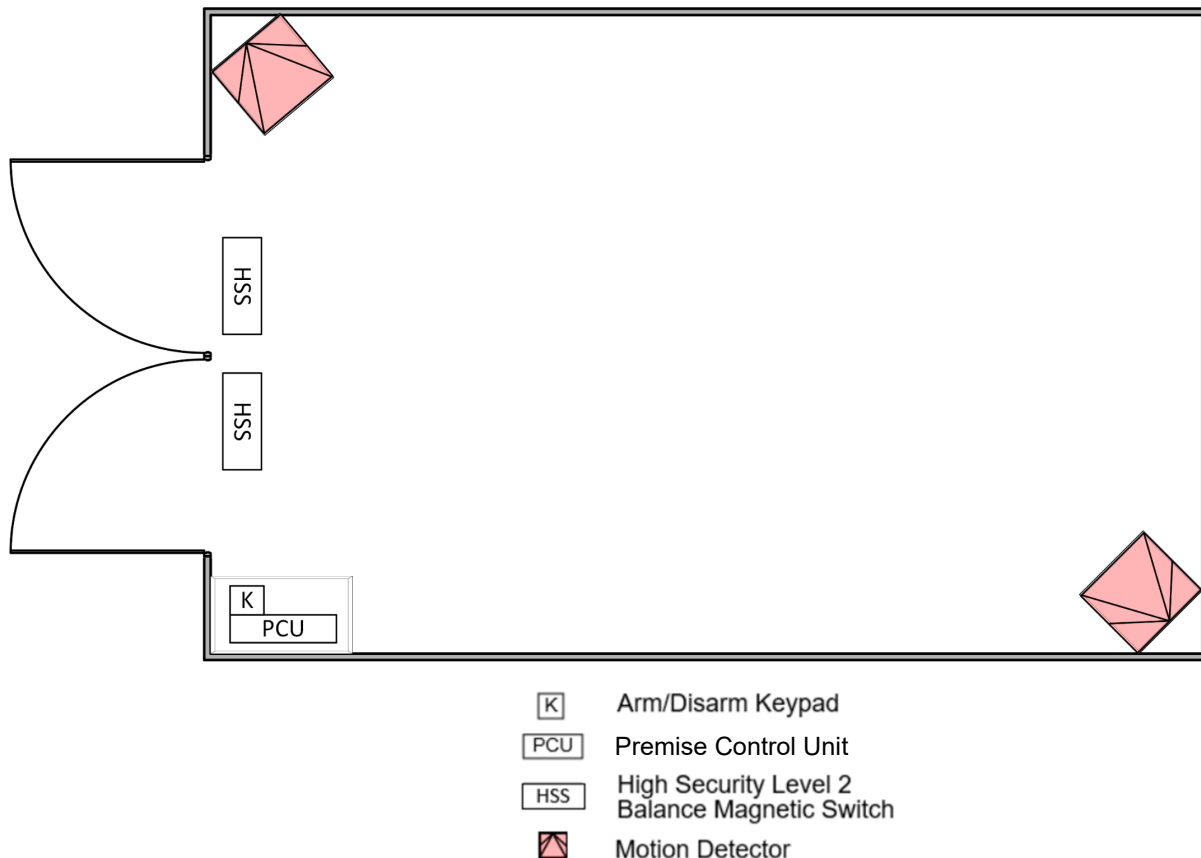
- All IDS systems, including any ACS connected, must be equipped with tamper detection devices that must be monitored continuously whether the system is in the access or secure mode of operation. Upon detection, an alarm (not fault) condition must be transmitted to the PCU or monitoring station.
- IDS transmission lines must have electronically monitored line supervision in order to detect evidence of tampering or attempted compromise. Electronic line supervision will entail a polling or multiplexing system or equivalent. If line security is unavailable, two independent means of alarm signal transmission from the alarm area to the monitoring station must be provided. Where possible, one of the two independent means of alarm signal transmission should be a secure wireless link. The dual transmission equipment must continuously monitor the integrity of communications links. Protect wireless links by means specified in FIPS 140 and have a valid certificate from the NIST Cryptographic Module Validation Program (CMVP).
- All system sensors must be located within the protected area.

- Cabling between all sensors and the PCU must be dedicated to the system, contained within the protected area, and be supervised, typically by an end of line resistor (EOL).
- Enclose cabling between all sensors and the PCU in rigid metal conduit to provide physical protection of the wiring when required by Service policy.

#### A-3.4 Emergency Backup Electrical Power.

- Eight hours of uninterruptible backup power is required. This may be provided by a UPS, batteries integral to the ESS, generators, or any combination thereof. In the event of primary power failure, the system must automatically transfer to an emergency electrical power source without causing alarm activation.
- An audible or visual indicator at the PCU must provide an indication of the primary or backup electrical power source in use. Equipment at the monitoring station must visibly and audibly indicate a failure in a power source or a change in power source.

#### A-4 MAGAZINE (EARTH-COVERED MAGAZINE).



**A-4.1 Policy Baseline.**

- DoD Manual 5100.76, *Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (AA&E)*
- OPNAV Instruction 5530.13, *U.S. Navy Conventional Arms, Ammunition, and Explosives Physical Security Policy Manual*
- MCO 5530.14A, *Marine Corps Physical Security Program Manual*
- DAFI 31-101, *Integrated Defense (ID)*
- AR 190-11, *Physical Security of Arms, Ammunition, and Explosives*
- DESR 6055.09, *DoD Explosives Safety Standards*

**A-4.2 Baseline Intrusion Detection System Requirements.**

- Sensitive conventional AA&E designated Security Risk Categories (SRC) I and II must be protected by an IDS when not continuously manned or under constant surveillance.
- All perimeter doors and man-passable openings into the magazine must be protected by UL 634 Level 1 HSS.
- Provide IDS arm/disarm keypad at entrance and for all separated (unit-based) interior storage areas that require an independent IDS capability
- The storage area must be protected by UL 639 listed interior volumetric sensors.
- IDS must be installed in accordance with UL 681.
- AA&E with CIIC A through H, K, L, O, S, T, U, 7, and 9 require compliance with DoD 5200.01V3 to house the PCU in the protected space.
- For hazardous locations, refer to DESR 6055.09.

**A-4.3 Tamper Protection.**

- All IDS systems, including any ACS connected, must be equipped with tamper detection devices that must be monitored continuously, whether the system is in the access or secure mode of operation. Upon detection, an alarm (not fault) condition must be transmitted to the PCU or monitoring station.
- System associated cabling that extends beyond the protected area perimeter must be installed in conduit and must employ electronic line supervision. Electronic line supervision will entail a polling or multiplexing system or equivalent. If line supervision is unavailable, two independent means of alarm signal transmission to the monitoring location must be provided.
- All system sensors must be located within the protected area.

- Cabling between all sensors and the PCU must be dedicated to the system, contained within the magazine unless the PCU must be outside the magazine for electrical safety reasons.

**A-4.4 Emergency Backup Electrical Power.**

- Eight hours of uninterruptible backup power is required. This may be provided by a UPS, batteries integral to the ESS, generators, or any combination thereof. In the event of primary power failure, the system must automatically transfer to an emergency electrical power source without causing alarm activation.
- An audible or visual indicator at the PCU must provide an indication of the primary or backup electrical power source in use. Equipment at the monitoring station must visibly and audibly indicate a failure in a power source or a change in power source.

**A-4.5 Hazards of Electromagnetic Radiation to Ordnance (HERO).**

- Refer to DA PAM 385-64, *Ammunition and Explosives Safety Standards*, to determine HERO requirements for ESS equipment installed in a magazine.

## APPENDIX B SITE SURVEY CHECKLIST

### B-1 ESS SITE SURVEY CHECKLIST.

The items included in the following checklist are not all inclusive. The intent is for the user to have general guidance to utilize while conducting a site survey. It is up to the user to tailor the list to the specific job site and the type of assets to be protected.

The use of video recording and photography can be useful tools to collect survey data. Information associated with the use of cameras on site must be obtained ahead of time. Survey participants are required to adhere to the camera policy at each site.

Survey Element		Notes
<b>Asset Description</b>		
Mission Description		
	Critical asset(s) description/locations	
Facility Size		
	Occupancy by time and number (Example: M–F, 0700–1630, 250 employees)	
	Demographics	
Threat Assessment (Use caution – may be classified)		
	Vulnerability Assessment (Describe when and who conducted the assessment.)	
	Potential threats (Examples: Adversary individuals/groups, threat capability)	
Adjoining Property		
	Describe direction, owner, boundary	
	Describe how access from adjoining property is controlled. (During normal duty hours; during off-duty hours.)	
	Do these properties pose a threat? (Yes or no)	
<b>Environment</b>		
	Weather conditions (Snow, sand, salt, high winds, fog, etc. Indicate average rainfall, average snowfall, and monthly temperature range.)	

Survey Element		Notes
	History of exposure to natural phenomenon (Examples: Hurricane, forest fire, tidal waves, tornadoes, lightning, extreme temperatures, sandstorms, blizzards)	
	Geographic setting (urban, suburban, rural, military installation, etc.)	
	Point of closest approach from perimeter	
	Number and location of vehicle approaches	
	Number and location of pedestrian approaches	
	Cover/concealment opportunities (Describe location and type)	
	Vehicle approach (Describe anticipated type of vehicle approach. Indicate if chicane is in place.)	
	Response force capabilities and description	
	Type/size of perimeter barriers and obstacles	
<b>Perimeter Barriers</b>		
Fence		
	Type and condition of fence material	
	Gates (Describe location and type.)	
	Dimensions of fence	
	Distance between fence and other structures	
	Type and condition of soil (Examples: sand, clay, eroding or stable)	
	Utility interferences (Describe location and type. Examples: Electrical, gas, water, sewer, telecommunications)	
	Roads, major highways, railroad tracks, or runways close to perimeter (Describe distance and location.)	
	Evidence of burrowing or damage to fence	

Survey Element		Notes
	Vegetation in close proximity to fence (Indicate if it is well maintained or impeding the fence.)	
	Identify any climbing aids in close proximity to the fence.	
	Describe any signage or other items attached to the fence	
Vehicle Barriers		
	Type (Automatic or manual operation)	
	Location	
	Quantity	
	Condition	
	Maintenance (Indicate if maintenance records are kept current)	
<b>ESS</b>		
	DoD-approved system (Examples: Has current ATO. Identify program-specific system of record such as ICIDS.)	
Intrusion Detection System (IDS)		
	Interior IDS	
	Type	
	Location	
	Quantity	
	Condition	
	Number of processors (Describe software licensing and build information.)	
	Exterior IDS	
	Type	
	Location	
	Quantity	
	Condition	
	Potential sources of nuisance alarms (Examples: inductive motors, air conditioning equipment, pumps,	

Survey Element		Notes
	welding equipment, or excavating nearby)	
	Number of processors (Describe software licensing and build information.)	
Access Control System (ACS)		
	Type of credential (access card)	
	Location of enrollment station(s)	
	Type of card readers	
	Condition	
	Quantity	
	Number of processors (Describe software licensing and build information.)	
	Number of ACS portals	
	Locking procedures/control functions (Examples: normal operations, emergency operations, normal duty hours, off-duty hours)	
	ACS integrated with IDS/VSS	
	Visitor controls and procedures	
	Access portals manned/unmanned	
	Access procedures to verify individuals	
	Access procedures followed/enforced	
	Personnel and hand-carried items searched	
	Procedures for vehicle entry (Personal, organizational, and commercial vehicles)	
VSS		
	Video management system (Describe software licensing and build information.)	
	Type (Fixed, PTZ)	
	Location	
	Quantity	
	Condition	
	Number and location of monitoring stations (Describe monitor configuration.)	

Survey Element		Notes
	Recording requirements	
	Archive requirements	
	Storage capacity	
	Integrated with IDS for alarm assessment	
	Topography of exterior assessment zones (Examples: level, uneven, obstructions)	
Central Monitoring Station		
	Effective integration (Example: cameras and alarms are integrated to provide guard forces with alarm assessment capability.)	
	Human factors (Example: ergonomic design of workstation appears to promote well-being of the operator and enhance system performance.)	
	Alarm types (Intrusion, tamper, comm fail, power fail, etc.)	
	Alarm events recorded	
	Trend analyses developed (Examples: Nuisance alarms, false alarms, alarm latency, ACS portal throughput issues)	
Lighting		
	Type of luminaire	
	Location	
	Condition	
	Quantity	
	Photometer reading (Utilize previous lighting study data if available.)	
	Adequately support guards (Meets illumination requirement based on asset type. Evidence of glare.)	
	Adequately supports VSS (Meets illumination requirement based on image sensor)	
Data Transmission System (DTS)		
	Type of DTS (Examples: fiber, copper, wireless. Describe condition and date of initial installation.)	

Survey Element		Notes
	DTS security	
	DTS routing	
	Redundancy	
	Vulnerabilities (Use caution - may be classified)	
<b>System Maintenance</b>		
	Testing intervals (Describe required and actual.)	
	Hardware	
	Software	
	Maintenance records kept current	
<b>Cybersecurity</b>		
	Current accreditation	
	Cybersecurity maintenance	
<b>Power Systems</b>		
	Primary (Describe supplier, type, and condition. Examples: local utility company, 1 Phase, 2 Phase, 50 Ha, 60 Hz, 110v, 220v)	
	Spare capacity	
	Proper grounding	
	Surge protection	
	Backup power	
	Identify critical loads (Describe load shed logic if available.)	
	Type (generator or battery)	
	Automatic or manual transfer	
	Operating time	
	Uninterruptible power source for sensitive loads	
	Operating time	
	Frequency of backup power testing	
<b>Plans and Procedures</b>		
	Security plans effectively support personnel and equipment usage (Indicate	

Survey Element		Notes
	if plans have been validated through exercise or testing.)	
	Maintenance plans effectively support personnel and equipment operation	
Additional Survey Elements		Additional Notes and Comments

*This Page Intentionally Left Blank*

## **APPENDIX C EXAMPLE DRAWINGS**

### **C-1        ESS EXAMPLE DRAWINGS.**

The following pages represent example CAD drawings for an ESS.

# C-1.1 Symbols and Abbreviations.

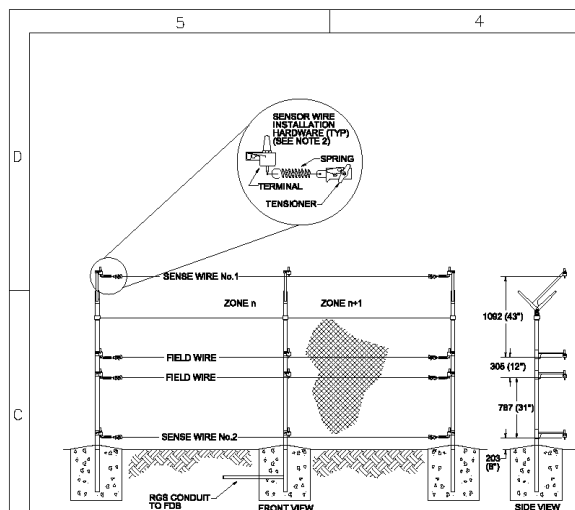
*** SAFETY FIRST ***					
5	4	3	2	1	
ABBREVIATIONS		SYMBOLS			
<p>ACC/SEC ACCESS/SECURE ACS ACCESS CONTROL SYSTEM AI ALARM INTERFACE B BALANCED MAGNETIC SWITCH BMS BISTATIC MICROWAVE SENSOR BOC BASE OPERATIONS CENTER BPC BURIED PORTED CABLE SENSOR C COMMON ACCESS CARD CAM CAMERA, FIXED CCD CHARGE COUPLED DEVICE CCTV CLOSED CIRCUIT TELEVISION CFS CAPACITANCE FENCE SENSOR CLW CLIENT WORKSTATION COTS COMMERCIAL OFF-THE-SHELF EQUIPMENT CPLD COUPLED CPS CAPACITANCE PROXIMITY SENSOR CPU CENTRAL PROCESSING UNIT CR CARD READER CSA COINJUNCT SECURITY AUTHORITY D DURESS ALARM SWITCH DBT DEBUG BASIS THREAT DM DISPLAY MONITOR DTM DATA TRANSMISSION MEDIA DVR DIGITAL VIDEO RECORDER E ENTRY BOOTH EC ENROLLMENT CENTER ECE ENROLLMENT CENTER EQUIPMENT ECF ENTRY CONTROL FACILITY EDB ELECTRONIC DOOR BOLT EDS ELECTRONIC DOOR STRIKE EFDS ELEC. FIELD DISTURBANCE FENCE SENSOR EMI ELECTROMAGNETIC INTERFERENCE EML ELECTROMAGNETIC LOCK EOL END OF LINE EP EDGE OF PAVEMENT ESSC ELECTRONIC SECURITY SYSTEM CONSOLE F FALSE ACCEPTANCE RATE OR FALSE ALARM RATE FAS FINGERPRINT ANALYSIS SCANNER FC FAIL OVER CONTROLLER FDB FIELD DISTRIBUTION BOX FIPS FEDERAL INFORMATION PROCESSING STANDARDS FO FIBER OPTIC FORX FIBER OPTIC RECEIVER MODULE FOTC FIBER OPTIC TRANSCIVER FOTX FIBER OPTIC TRANSMITTER MODULE FOUJ FOR OFFICIAL USE ONLY FOV FIELD OF VIEW FRR FALSE REJECTION RATE GBS GLASS BREAK SENSOR GLC GROUND LOOP CORRECTOR H HIGH DEFINITION HD HARD DISK DRIVE STORAGE HGU HAND GEOMETRY UNIT HVAC HEATING, VENTILATION, AND AIR CONDITIONING HVR HYBRID VIDEO RECORDER IDE INTRUSION DETECTION EQUIPMENT IDS INTRUSION DETECTION SYSTEM IP INTERNET PROTOCOL IR INFRARED IVS INTELLIGENT VIDEO SURVEILLANCE J JUNCTION BOX K KEYBOARD KP KEYPAD L LOCAL AREA NETWORK LCD LIQUID CRYSTAL DISPLAY LDR LINE DRIVER LP LOCAL PROCESSOR M MAGNETIC CONTACT MD METAL DETECTOR MDM</p>		<p>MMS MICROWAVE MOTION SENSOR MMSB MONOSTATIC MICROWAVE SENSOR MMS MULTIPLEXOR MUX MASS NOTIFICATION SYSTEM MVS MASTER VIDEO SYNC GENERATOR P PB PUSH-BUTTON SWITCH PCU PREMISE CONTROL UNIT PIN PERSONAL IDENTIFICATION NUMBER PIR PASSIVE INFRARED MOTION SENSOR PS POWER SUPPLY PTZ CAMERA, PAN-TILT-ZOOM PVC POLY-VINYL CHLORIDE R RCC REDUNDANT CENTRAL COMPUTER RDC REGIONAL DISPATCH CENTER RDTB RADAR DETECTION SYSTEM RFI RADIO FREQUENCY INTERFERENCE RFID RADIO FREQUENCY IDENTIFICATION RGS RIGID GALVANIZED STEEL RK RECEIVER S SCIF SENSITIVE COMPARTMENTED INFORMATION FACILITY SCPS SECURITY CONSOLE POWER SUPPLY SMP SYSTEM MULTIPLEX PANEL SOC SECURITY OPERATIONS CENTER SSV SYSTEM SENSOR SSCS STRAIN SENSITIVE CABLE SENSOR TDR TIME DOMAIN REFLECTOMETRY TS TAMPER SWITCH TWS TAUT WIRE SENSOR TX TRANSMITTER U UMS ULTRASONIC MOTION SENSOR UPS UNINTERRUPTIBLE POWER SUPPLY VGO VEHICLE GATE OPENER VMD VIDEO MOTION DETECTION VS VIBRATION SENSOR VW VAULT WALL WAN WIDE AREA NETWORK X X-RAY ARTICLE SURVEILLANCE/X-RAY</p>	<p>ACCESS CONTROL BIOMETRIC ACCESS CONTROL DEVICE (REFERENCE DOOR SCHEDULE FOR TYPE) CARD READER WITH KEYPAD GENERIC CARD READER (REFERENCE DOOR SCHEDULE OR SPECIFICATIONS FOR TYPE) GENERIC SCREENING DEVICE EXPLOSIVE DETECTOR METAL DETECTOR TAG DETECTOR (EAS) X-RAY TURNSTILE (REFERENCE DOOR SCHEDULE OR SPECIFICATIONS FOR TYPE) ANNUNCIATION: CONSOLE/PANEL CENTRAL PROCESSING UNIT FIELD PANEL GENERAL SECURITY HORN (DIFFERENTIATE FROM FIRE HORN, USE ALSO FOR LOCAL ALARM) POWER SUPPLY FIBER OPTIC MODULE INTERCOM SENSORS CAPACITANCE SENSOR GENERIC BURIED SENSOR GENERIC GLASS BREAKAWAY SENSOR GENERIC FENCE (REFERENCE TYPE IN SPECIFICATION OR SCHEDULE) GENERIC VOLUMETRIC BEAM SENSOR (BI-STATIC) GENERIC VOLUMETRIC MOTION SENSOR (MONO)</p>	<p>SWITCHES GENERIC SWITCH DOOR SPRING LOADED/DEADMAN ROCK L-UP/OVERHEAD DOOR GATE WINDOW/SLIDING DOOR FOOTBALL TAMPER HINGE PLUNGER/ROLLER LEVEL/TIMING CURRY BILLCASH DRAWER REFERENCE DOOR SCHEDULE OR SPECIFICATION FOR GAP, SIZE, MOUNTING, BALANCED, TAMPERED, EOL RESISTOR PUSH BUTTON BELL PUSH DURESS Panic DOOR RELEASE REQUEST FOR EXIT VIDEO GENERIC CAMERA AUTO-PAY CONCEALED OR DOMED PAN PAN-TILT FIXED SPILT REFER TO CAMERA SCHEDULE AND SPECIFICATION FOR TYPE (AO, ETC.) SIZE INSURE (ENVIRONMENTAL, EXPLOSION PROOF, ETC.) MOUNT (WALL, CEILING, FOLD) LENS (TYPE, SIZE) PAN RESETS ASSOCIATED ALARM SWITCHING SIGNAL TRANSMISSION RECORDER AUDIO DIGITAL VIDEO</p>	<p>DESIGNER GUIDANCE NOTES: 1. DRAWINGS SHALL COMPLY WITH THE A/E/C STANDARD LOCATED AT: <a href="http://acadmcenter.dnrc.dnrc.mil">HTTP://ACADMCENTER.DNRC.DNRC.MIL</a>. 2. SECURITY ENGINEERING SYMBOLS SHALL FOLLOW ASTM F967-03. 3. AS A MINIMUM, SYSTEMS INSTALLATION DRAWINGS SHOULD PROVIDE THE LEVEL OF DETAIL AS OUTLINED IN USGS 28 TO 24 PARAGRAPH 1.3.3, SHOP DRAWINGS, UNLESS OTHERWISE REQUIRED BY CONTRACT.</p>
5		4	3	2	
*** SUPPORT VALUE ENGINEERING - IT PAYS ***					
DATE: 03/04/2004					
Sheet reference number: TY-001					
Sheet 1 of 200					



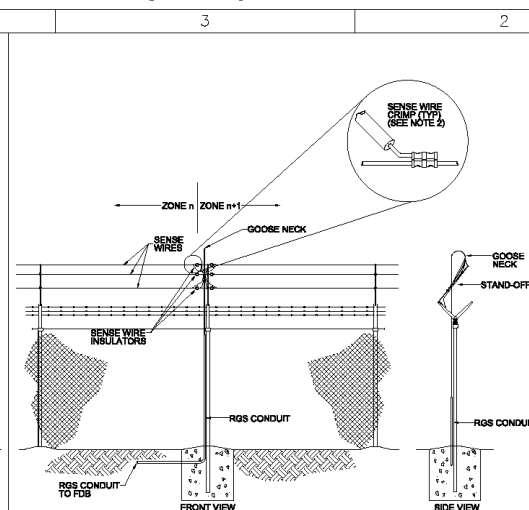
**\*\*\* SAFETY FIRST \*\*\***



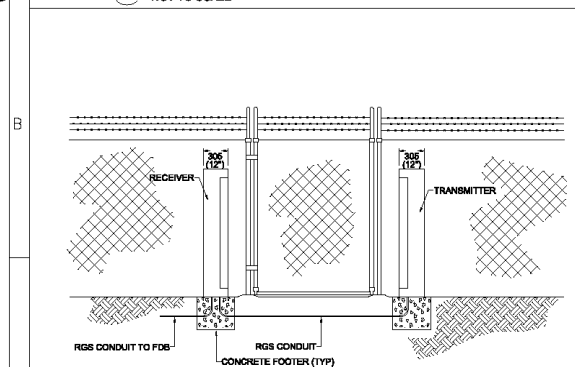
**\*\*\* SAFETY FIRST \*\*\***



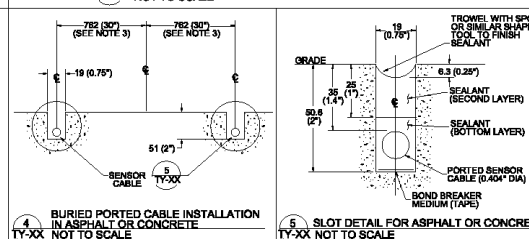
1 ELECTRIC FIELD DISTURBANCE FENCE SENSOR DETAIL  
TY-XX NOT TO SCALE



**2 CAPACITANCE FENCE SENSOR INSTALLATION DETAIL**  
**TY-XX NOT TO SCALE**

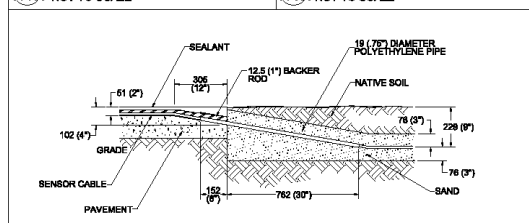


3 PHOTOELECTRIC BEAM ACROSS SWING GATE  
TY-XX NOT TO SCALE



4 BURIED PORTED CABLE INSTALLATION  
IN ASPHALT OR CONCRETE  
TY-XX NOT TO SCALE

5 SLOT DETAIL FOR ASPHALT OR CONCRETE  
TY-XX NOT TO SCALE



**6 BURIED PORTED CABLE SENSOR SOIL-TO-HARD SURFACE TRANSITION DETAIL**  
**TY-XX NOT TO SCALE**

- NOTES:**

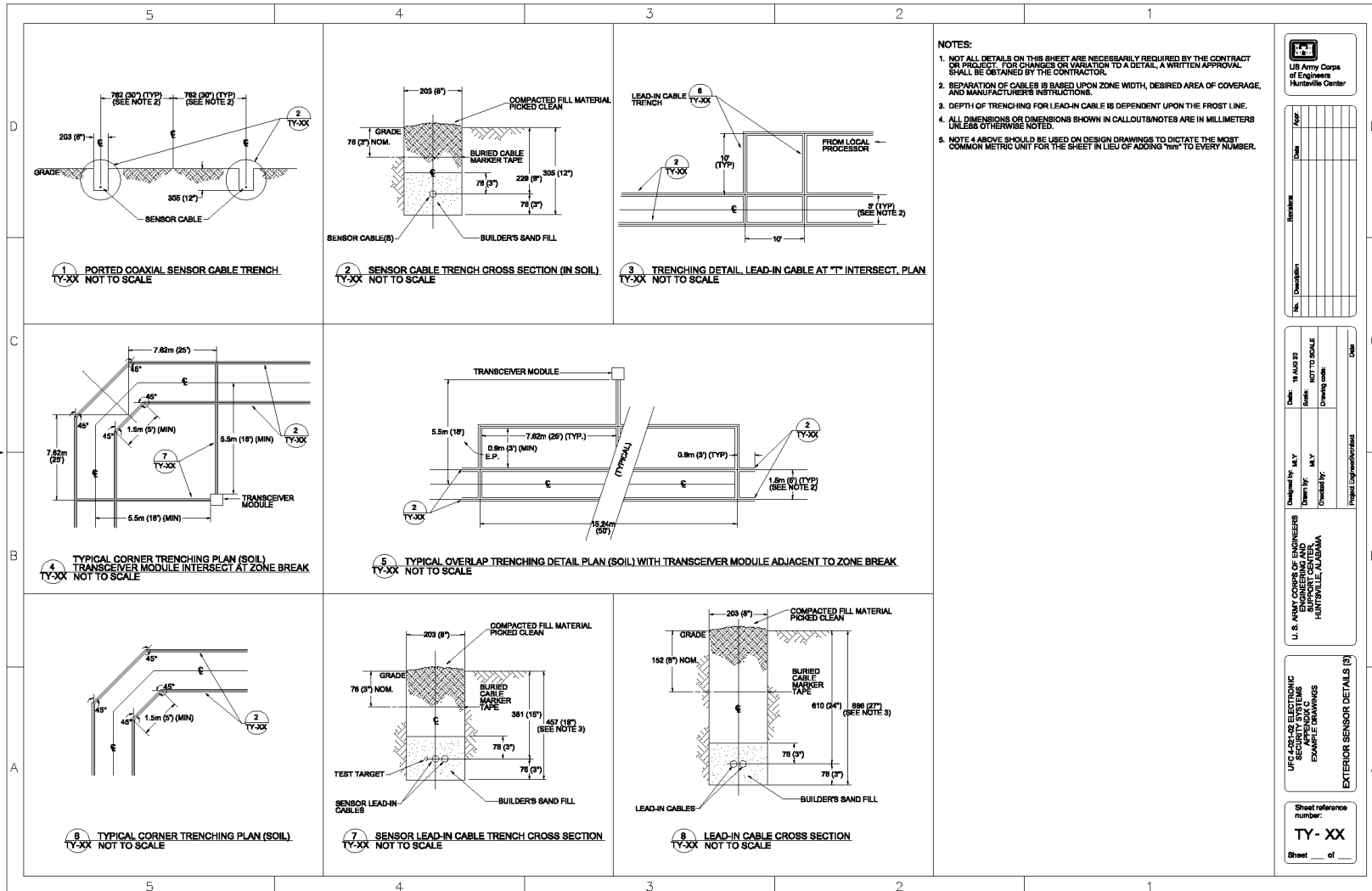
1. NOT ALL DETAILS ON THIS SHEET ARE NECESSARILY REQUIRED BY THE CONTRACT OR PROJECT. FOR CHANGES OR VARIATION TO A DETAIL, A WRITTEN APPROVAL SHALL BE OBTAINED BY THE CONTRACTOR.
2. SENSE WIRE, LEAD-IN WIRE, AND ALL WEATHER-EXPOSED METALLIC HARDWARE MUST BE STAINLESS STEEL.
3. SEPARATION OF CABLES IS BASED UPON ZONE WIDTH, DESIRED AREA OF COVERAGE, AND MANUFACTURER'S INSTRUCTIONS.
4. ALL DIMENSIONS OR DIMENSIONS SHOWN IN CALLOUTS/NOTES ARE IN MILLIMETERS UNLESS OTHERWISE NOTED.
5. ALL SECURITY FENCING SHALL BE IN ACCORDANCE WITH USBC STANDARD DETAILS FOR CHAIN LINK SECURITY FENCING.
6. NOTE A ABOVE SHOULD BE USED ON DESIGN DRAWINGS TO DICTIONATE THE MOST COMMON ABOVE UNIT FOR THE SHEET IN LIEU OF DRAWING "mm" TO EVERY NUMBER.

```

DATE: $$$DATETIME
FILE: $$$pathname

```

\*\*\* SAFETY FIRST \*\*\*

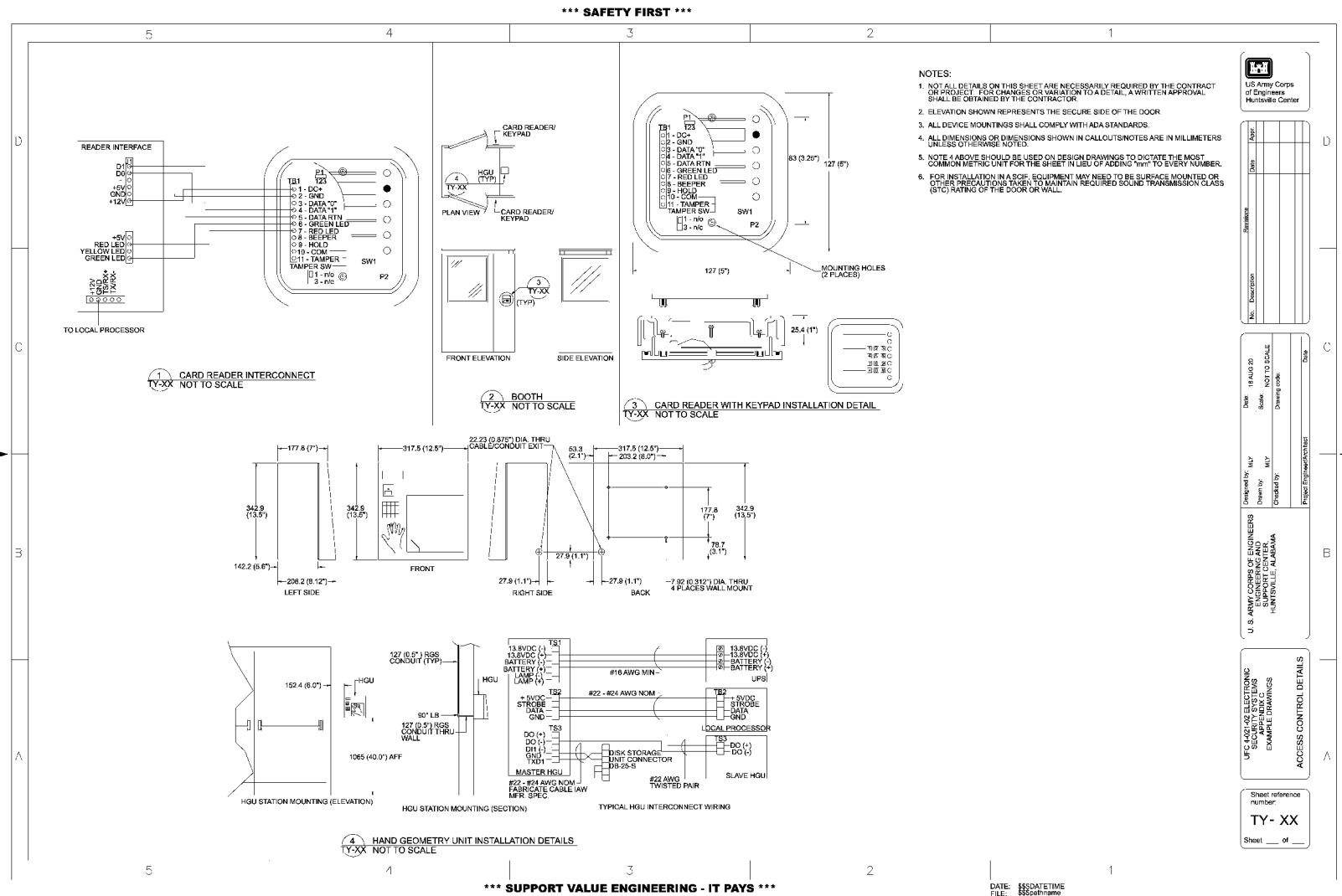


DRAFT SUBMITTAL

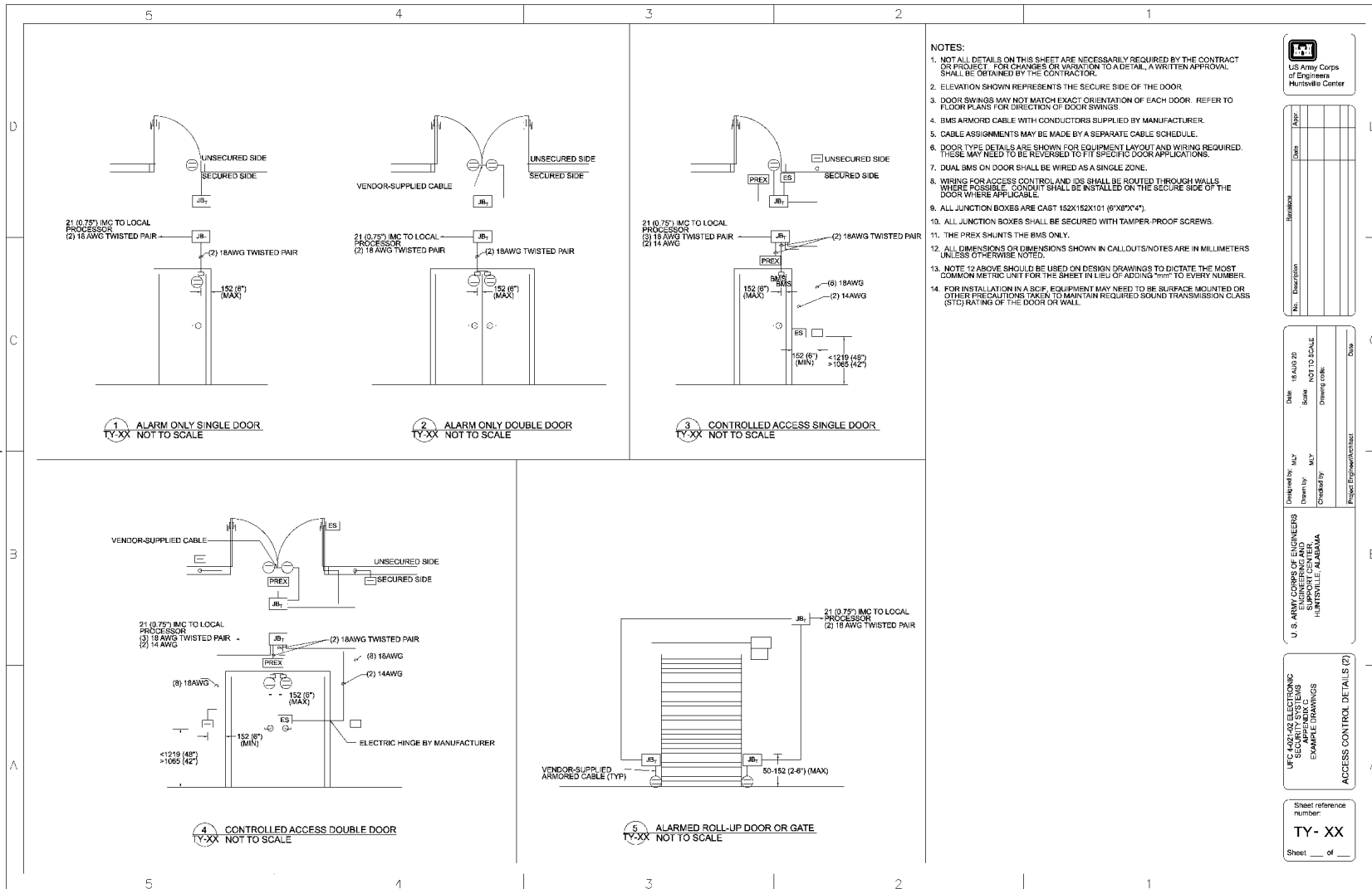
\*\*\* SUPPORT VALUE ENGINEERING - IT PAYS \*\*\*

DATE: 6/20/2025  
FILE: 6/20/2025

# C-1.4 Access Control Details.



\*\*\* SAFETY FIRST \*\*\*



- NOTES:
1. NOT ALL DETAILS ON THIS SHEET ARE NECESSARILY REQUIRED BY THE CONTRACT OR PROJECT. FOR CHANGES OR VARIATION TO A DETAIL, A WRITTEN APPROVAL SHALL BE OBTAINED BY THE CONTRACTOR.
  2. ELEVATION SHOWN REPRESENTS THE SECURED SIDE OF THE DOOR.
  3. DOOR SWINGS MAY NOT MATCH EXACT ORIENTATION OF EACH DOOR. REFER TO FLOOR PLANS FOR DIRECTION OF DOOR SWINGS.
  4. BMS ARMORED CABLE WITH CONDUCTORS SUPPLIED BY MANUFACTURER.
  5. CABLE ASSIGNMENTS MAY BE MADE BY A SEPARATE CABLE SCHEDULE.
  6. DOOR TYPE DETAILS ARE SHOWN FOR EQUIPMENT LAYOUT AND WIRING REQUIRED. THESE MAY NEED TO BE REVERSED TO FIT SPECIFIC DOOR APPLICATIONS.
  7. DUAL BMS ON DOOR SHALL BE WIRED AS A SINGLE ZONE.
  8. WIRING FOR ACCESS CONTROL AND IDS SHALL BE ROUTED THROUGH WALLS WHERE POSSIBLE. CONDUIT SHALL BE INSTALLED ON THE SECURED SIDE OF THE DOOR WHERE APPLICABLE.
  9. ALL JUNCTION BOXES ARE CAST 152X152X101 (6"X6"X4").
  10. ALL JUNCTION BOXES SHALL BE SECURED WITH TAMPER PROOF SCREWS.
  11. THE PREX SHAUNTS THE BMS ONLY.
  12. ALL DIMENSIONS OR DIMENSIONS SHOWN IN CALLOUTS/NOTES ARE IN MILLIMETERS UNLESS OTHERWISE NOTED.
  13. NOTE 12 ABOVE SHOULD BE USED ON DESIGN DRAWINGS TO DICTATE THE MOST COMMON METRIC UNIT FOR THE SHEET IN LIEU OF ADDING "mm" TO EVERY NUMBER.
  14. FOR INSTALLATION IN A SCF, EQUIPMENT MAY NEED TO BE SURFACE MOUNTED OR OTHER PRECAUTIONS TAKEN TO MAINTAIN REQUIRED SOUND TRANSMISSION CLASS (STC) RATING OF THE DOOR OR WALL.



No.	Description	Revision	Date

Designed by	Drawn by	Checked by	Project Engineer/Architect

U.S. ARMY CORPS OF ENGINEERS ENGINEERING AND CONSTRUCTION CENTER HUNTSVILLE, ALABAMA
---

UFC 4-021-02 ELECTRONIC SECURITY SYSTEMS EXAMPLE DRAWINGS ACCESS CONTROL DETAILS (2)
---

Sheet reference number: <b>TY- XX</b>
---

Sheet <b> </b> of <b> </b>
----------------------------

DRAFT SUBMITTAL

\*\*\* SUPPORT VALUE ENGINEERING - IT PAYS \*\*\*

DATE:   
FILE:

## APPENDIX D GLOSSARY

### D-1 ACRONYMS AND ABBREVIATIONS.

AA&E	Arms, Ammunition, and Explosives
ABA	Architectural Barriers Act
ACS	Access Control System
ANSI	American National Standards Institute
AO	Accrediting Official
APL	Approved Products List
AR	Army Regulation
Bio	Biometric
CAC	Common Access Card
CAD	Computer Aided Design
CCDE	Command and Control Display Equipment
CHUID	Card Holder Unique Identifier
CIIC	Controlled Inventory Item Code
CNSSI	Committee on National Security Systems Instruction
DAFI	Department of the Air Force Instruction
dB	Decibel
DC	Direct Current
DESR	Defense Explosives Safety Regulation
DFPE	Designated Fire Protection Engineer
DoD	Department of Defense
DoDI	Department of Defense Instruction
DoDM	Department of Defense Manual
DOR	Designer of Record

DPDT	Double Pole Double Throw
DPS	Door Position Switch
DTM	Data Transmission Media
EMI	Electromagnetic Interference
ESS	Electronic Security System
ET	Endurance Testing
FAR	False Alarm Rate
FAR	Federal Acquisition Regulation
FDB	Field Distribution Box
FIPS	Federal Information Processing Standards
FOUO	For Official Use Only
FOV	Field of View
FPAT	Functional Pre-Acceptance Test
fps	Frames Per Second
FSAT	Functional System Acceptance Test
GSA	General Services Administration
HD	High Definition
HDMI	High-Definition Multimedia Interface
HSS	High Security Switch
Hz	Hertz
ICIDS	Integrated Commercial Intrusion Detection System
IDB	Interior Distribution Box
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IEL	Integrated Electronic Lock

IP	Internet Protocol
IR	Infrared
IT	Information Technology
LED	Light Emitting Diode
m	Meter
Mbps	Megabits Per Second
MCESS	Marine Corps Electronic Security System
MCO	Marine Corps Order
MILCON	Military Construction
MJPEG	Motion Joint Photographic Experts Group
MP	Megapixel
NAR	Nuisance Alarm Rate
NEC	National Electrical Code
NEMA	National Electrical Manufacturer's Association
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
NVR	Network Video Recorder
O&M	Operations and Maintenance
ONVIF	Open Network Video Interface Forum
OPNAV	Office of the Chief of Naval Operations
PAT	Pre-Acceptance Test
PC	Personal Computer
PCU	Premise Control Unit
PIN	Personal Identification Number
PIR	Passive Infrared

PIT	Platform Information Technology System
PIV	Personal Identity Verification
Pixels	Picture Elements
PKI	Public Key Infrastructure
POC	Point of Contact
PoE	Power over Ethernet
PTZ	Pan/Tilt/Zoom
REX	Request-to-Exit
RFP	Request For Proposal
SAPCO	Special Access Program Central Office
SAPF	Special Access Program Facility
SAT	System Acceptance Testing
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SHDSL	Single-Pair High-Speed Digital Subscriber Line
SRM	Sustainment, Restoration, and Modernization
TCP	Transmission Control Protocol
UL	Underwriters Laboratory
UPS	Uninterruptible Power Supply
USACE	U.S. Army Corps of Engineers
VAC	Volts Alternating Current
VMS	Video Management System
VoIP	Voice Over Internet Protocol
VSS	Video Surveillance System

## D-2 DEFINITION OF TERMS.

**Access Control System (ACS):** An automated system that interfaces with locking mechanisms that momentarily permit access (for example, by unlocking doors or gates) after verifying entry credentials (for example, using a card reader). Other DoD documents may refer to the ACS as an automated access control system, electronic entry control system, automated access control system (AACS), electronic access control system, physical access control system (PACS), and electronic entry control.

**Anti-Passback:** A functional characteristic employed within ACS that is used to eliminate/mitigate the risk of someone giving their credential (passing it back) to another person after that credential is used to access a secure area.

**Authorization to Operate (ATO):** The official management decision given by a senior organizational official to authorize operation of an information system and explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation, based on the implementation of an agreed-upon set of security controls.

**Balanced Magnetic Switch (BMS): A legacy term superseded by the current term High Security Switch (HSS).** A door position switch using a switch held in a balanced or center position by interacting magnetic fields when not in an alarm condition.

**Base Level Information Infrastructure:** Information technology (IT) infrastructure that exists on DoD proprietary or leased property.

**Biometric (Bio):** A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris image samples are all examples of biometrics.

**Card Reader:** A device that communicates with a card or "smart card" using either radio frequency (RF) signals via a circuit chip or wires via a contact pad on the card. The readers consist of various types, including contactless, contact, or a hybrid with the option of a combination of a keypad or biometric reader.

**Central Monitoring Station:** The space that serves as a central monitoring and assessment facility for the ACS, video, and IDS systems. The key components of a central monitoring station include consoles, monitors, and printers. Normally, the central monitoring station is staffed 24 hours a day, seven days a week by trained personnel. Other names for the central monitoring station include security operations center (SOC), security command center and security control center (SCC), dispatch center, data transmission center (DTC), and alarm control center (ACC).

**Common Access Card (CAC):** The CAC, a "smart" card about the size of a credit card, is the standard identification for active-duty military personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel. It is also the principal card used to enable physical access to buildings and controlled spaces, and provides access to defense computer networks and systems.

**Controlled Access Area (CAA):** The complete building or facility area under direct physical control within which unauthorized persons are denied unrestricted access and are either escorted by authorized personnel or are under continuous physical or electronic surveillance.

**Data Transmission Media (DTM):** The system that allows electronic security systems (ESS) data transmission and communication between system nodes and also back to the central monitoring station. The DTM is the security communications system and can consist of fiber, dedicated conductors, wireless networks, leased T-1 lines, or virtual private networks. DTM includes both base level information infrastructure (BLII: on-base) and defense information infrastructure (DII: inter-base).

**Defense Information Infrastructure:** The information technology (IT) infrastructure that is not on DoD proprietary or leased property and requires transmission of information across property boundary lines, for example, inter-base communications.

**Electronic Security System (ESS):** The integrated electronic system that encompasses interior and exterior intrusion detection systems (IDS), video surveillance systems (VSS) for assessment of alarm conditions, access control systems (ACS), data transmission media (DTM), and alarm reporting systems for monitoring, control, and display.

**Electromagnetic Interference (EMI):** A naturally occurring phenomenon when the electromagnetic field of one device disrupts, impedes, or degrades the electromagnetic field of another device by coming into proximity with it. With ESS, devices are susceptible to EMI because electromagnetic fields are a byproduct of passing electricity through a wire. Data lines that have not been properly shielded are susceptible to EMI. A good example of an ESS application is using shielded wiring from a field card reader back to the local ACS panel.

**False Acceptance Rate (FAR):** The rate or percentage at which a false credential is inaccurately accepted as being valid by an ACS. A sample FAR for a product could be 0.1%.

**False Alarm:** An alarm when there is no alarm stimulus.

**False Rejection Rate (FRR):** The rate or percentage at which an ACS product or system rejects an authorized credential holder.

**Federal Information Processing Standard (FIPS):** A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology (IT) to achieve a common level of quality or some level of interoperability.

**Field Distribution Box (FDB):** A field distribution box (FDB) serves as a critical node for sensor processing, data transmission, and electrical power along a site perimeter.

**Frame Rate Per Second (fps):** When referring to a video image, this term refers to how often the visual still image is updated.

**Identity Assurance:** A category that conveys the degree of confidence that a person's claimed identity is their real identity, as defined in [NIST SP 800-63-3] in terms of three levels: IAL 1 (Some confidence), IAL 2 (High confidence), IAL 3 (Very high confidence).

**Intrusion Detection System (IDS):** A system consisting of interior and exterior sensors, surveillance devices, and associated communication subsystems that collectively detect an intrusion of a specified site, facility, or perimeter and annunciate an alarm.

**Local Area Network (LAN):** A geographically limited data communication system for a specific user group consisting of a group of interconnected computers sharing applications, data, and peripherals.

**Nuisance Alarm:** An alarm resulting from the detection of an appropriate alarm stimulus, or failure to use established entry control procedures, but which does not represent an attempt to intrude into the protected area. Examples of nuisance alarms would be improper opening of a monitored exit door or activation of an exterior intrusion detection system by a DoD maintenance crew. Animal activation of detection systems is a potential cause of nuisance alarms. Another example would be a wind-generated alarm of a fence monitoring system caused by flexing of the fence. Numerous nuisance alarms can cause complacency.

**Premise Control Unit (PCU):** A PCU is an electronic device that continuously monitors the alarm status of local intrusion detection sensors and duress devices and transmits alarm conditions to a remote monitoring station. The PCU allows authorized personnel to place the alarm zone in an “armed” or “disarmed” state via a local keypad, credential reader, or biometric device. The term “PCU” is generally synonymous with the terms “ACS local processor”, “access control panel”, “IDS local processor,” and “intrusion panel.”

**Personal Identification Number (PIN):** An identification string used as a password to authenticate identity and gain access to a location or computer resource. Although there are alphanumeric product options, most hardware entry devices make use of a numeric keypad. Many computer resource programs require an alphanumeric string.

**Personal Identity Verification (PIV) Card:** A physical artifact (for example, identity card, “smart” card) issued to an individual that contains a PIV card application that stores identity credentials (for example, photograph, cryptographic keys, digitized fingerprint representation) so the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

**Physical Protection System/Physical Security System:** A system to prevent unauthorized physical access to a protection and/or security system, such as fences, walls, locks, sensors, and surveillance.

**Probability of Detection (Pd):** A measure of an intrusion detection sensor's performance in detecting an intruder within its detection zone.

**Proprietary Security Network:** A completely self-contained dedicated local area network (LAN) with security system software installed and run on a host server (computer). Proprietary security networks are dedicated to the ESS, with no outside (Internet, LAN, or WAN) connections.

**Regional Dispatch Center (RDC):** A centralized security command center for multiple bases and facilities within a geographic region. This location is typically staffed 24 hours a day by staff trained to assess and initiate responses for ESS alarms. The RDC requires interface and communication systems to different bases and facilities. The RDC concept is a trend of economically consolidating different base ESS at one centralized location to save money and infrastructure rather than having different discrete base operations centers.

**Security Equipment Integration Working Group (SEIWG):** A working group responsible for a standard (SEIWG-012) pertaining to information encoded on an access control card. This standard is generally referred to as "SEIWG," although there are other SEIWG specifications as well.

**Sensitive Compartmented Information (SCI):** Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the Director of National Intelligence.

**Sensitive Compartmented Information Facility (SCIF):** A facility capable of storing or processing Sensitive Compartmented Information (SCI) material. Requirements for these facilities are defined in *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, IC Tech Spec – for ICD/ICS 705*.

**Special Access Program (SAP):** A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those typically required for information at the same classification level.

**Stand-alone System:** A system that is not connected to any other network and does not transmit, receive, route, or exchange information outside of the system's authorization boundary.

**Time Domain Reflectometry (TDR):** Process of sending an electronic signal down a conductor or fiber (wiring or cabling) and measuring the time it takes for the signal or part of the signal to return to determine the location of a flaw or disturbance. The signal's reflection begins at the flaw or disturbance point.

**Uninterruptible Power Supply (UPS):** A power supply system that includes a rectifier, battery, and inverter to maintain power in the event of a power outage. UPS systems are specified by hours of operation to sustain power during an outage (six hours, ten hours, or 24 hours). UPS systems can be standby power systems or on-line systems. Typically, a centralized UPS is not a mandated requirement for an ESS project.

**Video Analytics:** Software that allows the user to input a specific set of rules for each scene of interest, which, if violated, generate visual cues on the monitor, thus drawing the operator's attention to suspicious objects or behaviors.

**Video Management System (VMS):** Software that allows the user to conveniently view the video from all camera and recording devices.

**Video Surveillance System (VSS):** A system that is primarily used for surveillance, collection of forensic evidence, or assessment during alarm conditions. VSS was formerly known as closed circuit television (CCTV).

**Wide Area Network (WAN):** An internetwork that uses telecommunication links to connect geographically distant networks.

**Workstation:** A computer that allows a user to interact with an IDS, ACS, or VSS with the necessary software for each.

*This Page Intentionally Left Blank*

## APPENDIX E REFERENCES

### COMMITTEE ON NATIONAL SECURITY SYSTEMS (CNSS)

<https://www.cnss.gov/CNSS/>

CNSSI 7003, *Protected Distribution Systems*

### DEPARTMENT OF HOMELAND SECURITY

Homeland Security Presidential Directive 12 (HSPD 12), *Policy for a Common Identification Standard for Federal Employees and Contractors*,  
<https://www.dhs.gov/homeland-security-presidential-directive-12>

*The Risk Management Process: An Interagency Security Committee Standard*,  
November 2016/2nd Edition, <https://www.dhs.gov/>

*The Risk Management Process for Federal Facilities*, 2018 Edition,  
<https://www.dhs.gov/>

### GENERAL SERVICES ADMINISTRATION (GSA)

FIPS 201, *Evaluation Program Approved Products List (APL), Physical Access Control System (PACS) Components*, <https://www.idmanagement.gov/fips201/>

Federal Acquisition Regulation (FAR) 52.204-25, *Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment*,  
<https://www.acquisition.gov/far/52.204-25>

Federal Specification FF-L-2740B, *Locks, Combination Electromechanical*,  
<https://fedspecs.gsa.gov/s/>

Federal Specification FF-L-2890C, *Lock Extensions (Pedestrian Door Lock Assembly Preassembled, Panic and Auxiliary Deadbolt)*

### INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

<https://www.ieee.org/>

IEEE 493, *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*

IEEE C2, *National Electrical Safety Code(R) (NESC(R))*

IEEE P519.1, *Guide for Applying Harmonic Limits on Power Systems*

IEEE P519, *IEEE Standard for Harmonic Control in Electric Power Systems*

## **NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)**

<https://www.nfpa.org/>

NFPA 70, *National Electrical Code (NEC)*

NFPA 101, *Life Safety Code*

NFPA 780, *Standard for the Installation of Lightning Protection Systems*

## **NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)**

FIPS 140, *Security Requirements for Cryptographic Modules*,  
<https://csrc.nist.gov/publications/fips>

FIPS 197, *Advanced Encryption Standard (AES)*, <https://csrc.nist.gov/publications/fips>

FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*,  
<https://csrc.nist.gov/publications/fips>

SP 800-116, *Guidelines for the Use of PIV Credentials in Facility Access*,  
<https://csrc.nist.gov/publications/sp800>

## **OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**

ICS 705-01, *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities*, <https://www.dni.gov/files/NCSC/documents/Regulations/ICS-705-1.pdf>

*Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, IC Tech Spec – for ICD/ICS 705*  
[https://www.dni.gov/files/NCSC/documents/Regulations/IC Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities v151 PDF.pdf](https://www.dni.gov/files/NCSC/documents/Regulations/IC_Technical_Specifications_for_Construction_and_Management_of_Sensitive_Compartmented_Information_Facilities_v151_PDF.pdf)

## **OPEN NETWORK VIDEO INTERFACE FORUM (ONVIF)**

ONVIF Core Specification, <https://www.onvif.org/PROFILES/SPECIFICATIONS/>

## **TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA)**

<https://tiaonline.org/>

ANSI/TIA-607, *Telecommunications Bonding and Grounding (Earthing) for Customer Premises*,

## **UNDERWRITERS LABORATORY (UL)**

<https://www.shopulstandards.com/>

UL 294, *Access Control System Units*

UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*

UL 639, *Standard for Intrusion-Detection Units*

UL 681, *Standard for Installation and Classification of Burglar and Holdup Alarm Systems*

UL 1076, *Standard for Proprietary Burglar Alarm Units and Systems*

UL 1610, *Standard for Central-Station Burglar-Alarm Units*

UL 2050, *National Industrial Security Systems*

## **UNITED STATES ACCESS BOARD**

<https://www.access-board.gov>

*Architectural Barriers Act (ABA) Accessibility Standard for Department of Defense Facilities*

*Architectural Barriers Act (ABA) Standards,*

## **UNITED STATES AIR FORCE**

DAFI 31-101, *Integrated Defense (ID)*, <https://www.e-publishing.af.mil/>

ESE-SIT-0001, *Standard Electronic Security Equipment Siting and Design Guidance for Permanent Installations*, distributed by the Electronic Systems Center (ESC) / Force Protection System Program Office (SPO), Hanscom AFB, MA 01731-2100

## **UNITED STATES ARMY**

<https://armypubs.army.mil/ProductMaps/PubForm/AR.aspx>

AR 190-11, *Physical Security of Arms, Ammunition, and Explosives*

AR 190-51, *Security of Unclassified Army Resources (Sensitive and Nonsensitive)*

AR 190-59, *Chemical Agent Security Program*

AR 380-5, *Army Information Security Program*

DA PAM 385-64, *Ammunition and Explosives Safety Standards*  
[https://armypubs.army.mil/epubs/DR\\_pubs/DR\\_a/ARN31050-PAM\\_385-64-000-WEB-1.pdf](https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN31050-PAM_385-64-000-WEB-1.pdf)

Standard Drawing 872-90-04, *FE7 Chain-Link Security Fence Details for Non-Sensored Fence*

**DEPARTMENT OF DEFENSE**

<https://www.esd.whs.mil/DD/>

DoD 5200.08-R, *Physical Security Program*

DoDI-O 2000.16, Volume 1, *DoD Antiterrorism Program Implementation: DoD Antiterrorism Standards*

DoDI 5200.08, *Security of DoD Installations and Resources and DoD Physical Security Review Board (PSRB)*

DoDM 5100.76, *Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (AA&E)*

DoDM 5200.01, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*

DoDM 5200.01, Volume 2, *DoD Information Security Program: Marking of Information*

DoDM 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*

DoDM 5205.07, Volume 3, *DoD Special Access Program (SAP) Security Manual: Physical Security*

DESR 6055.09, *DoD Explosives Safety Standards*, <https://www.denix.osd.mil/ddes/>

**UNITED STATES DEPARTMENT OF DEFENSE, UNIFIED FACILITIES CRITERIA**

<https://www.wbdg.org/dod/ufc>

UFC 1-200-01, *DoD Building Code*

UFC 3-501-01, *Electrical Engineering*

UFC 3-520-01, *Interior Electrical Systems*

UFC 3-530-01, *Interior and Exterior Lighting Systems*

UFC 3-575-01, *Lightning and Static Electricity Protection Systems*

UFC 3-600-01, *Fire Protection Engineering for Facilities*

UFC 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings*

UFC 4-010-03, *Security Engineering: Physical Security Measures for High-Risk Personnel*

UFC 4-010-05, *SCIF/SAPF Planning, Design, and Construction*

UFC 4-010-06, *Cybersecurity of Facility-Related Control Systems (FRCS)*

UFC 4-020-01, *DoD Security Engineering Facilities Planning Manual*

UFC 4-020-02FA, *Security Engineering: Concept Design*

UFC 4-020-03FA, *Security Engineering: Final Design*

UFC 4-022-01, *Security Engineering: Entry Control Facilities/Access Control Points*

UFC 4-022-03, *Security Fences and Gates*

UFC 4-024-01, *Security Engineering: Procedures for Designing Airborne Chemical, Biological, and Radiological Protection for Buildings*

UFC 4-025-01, *Security Engineering: Waterfront Security*

UFC 4-141-04, *Emergency Operations Center Planning and Design*

## **UNITED STATES MARINE CORPS**

MCO 5530.14A *Marine Corps Physical Security Program Manual*,  
[https://www.marines.mil/portals/1/Publications/MCO%205530\\_14A.pdf](https://www.marines.mil/portals/1/Publications/MCO%205530_14A.pdf)

## **UNITED STATES NAVY**

OPNAV 5530.13, *U.S. Navy Conventional Arms, Ammunition, and Explosives Physical Security Policy Manual*,  
<https://www.secnav.navy.mil/doni/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-500%20Security%20Services/5530.13D.pdf>

*This Page Intentionally Left Blank*

## APPENDIX F ADDITIONAL REFERENCES

### COMMITTEE ON NATIONAL SECURITY SYSTEMS (CNSS)

<https://www.cnss.gov/CNSS/>

CNSSAM TEMPEST/1-13, *RED/BLACK Installation Guidance* (FOUO)

### INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

<https://www.iso.org/home.html>

ISO/IEC 14443-1, *Cards and security devices for personal identification — Contactless proximity objects — Part 1: Physical characteristics*

ISO/IEC 14443-2, *Cards and security devices for personal identification — Contactless proximity objects — Part 2: Radio frequency power and signal interface*

ISO/IEC 14443-3, *Cards and security devices for personal identification — Contactless proximity objects — Part 3: Initialization and anticollision*

ISO/IEC 14443-4, *Cards and security devices for personal identification — Contactless proximity objects — Part 4: Transmission protocol*

### NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems*

### NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

NIST IR 6887 E2003, *Government Smart Card Interoperability Specification*, Version 2.1, <https://csrc.nist.gov/pubs/ir/6887/e2003/final>

SP 800-63-3, *Digital Identity Guidelines*, <https://csrc.nist.gov/publications/sp800>

SP 800-73-4, *Interfaces for Personal Identity Verification* [now SP 800-73-5, *Interfaces for Personal Identity Verification: Part 1 – PIV Card Application Namespace, Data Model and Representation*; SP 800-73-5, *Interfaces for Personal Identity Verification: Part 2 – PIV Card Application Card Command Interface*; SP 800-73-5, *Interfaces for Personal Identity Verification: Part 3 – PIV Client Application Programming Interface*], <https://csrc.nist.gov/publications/sp800>

SP 800-78-4 [now SP 800-78-5], *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, <https://csrc.nist.gov/publications/sp800>

**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**

ICS 705-02, *Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities*,  
[https://www.dni.gov/files/NCSC/documents/Regulations/ICS\\_705-2\\_Standards\\_for\\_Accreditation\\_Reciprocal\\_Use\\_of\\_SCIFs.pdf](https://www.dni.gov/files/NCSC/documents/Regulations/ICS_705-2_Standards_for_Accreditation_Reciprocal_Use_of_SCIFs.pdf)

**SECURITY EQUIPMENT INTEGRATION WORKING GROUP (SEIWG)**

<https://www.acq.osd.mil/ncbdp/nm/pseag/about/seiwg.html>

SEIWG 0101C, *Force Protection Systems Sensor Information Interchange*

SEIWG 0300, *Force Protection Systems Command and Control Information Interchange*

**SECURITY INDUSTRY ASSOCIATION & INTERNATIONAL ELECTROTECHNICAL COMMISSION**

<https://www.securityindustry.org/INDUSTRY-STANDARDS/OPEN-SUPERVISED-DEVICE-PROTOCOL/>

IEC 60839-11-5, *Open Supervised Device Protocol (OSDP) standard*

**UNDERWRITERS LABORATORY (UL)**

<https://www.shopulstandards.com/>

UL 827, *Central-Station Alarm Services*

## UNITED STATES AIR FORCE

AFMAN31-101V1, *Integrated Defense (ID) Planning*, <https://www.e-publishing.af.mil/>

DoDM5200.08\_AFMAN31-101V3, *Physical Security Program*, <https://www.e-publishing.af.mil/>

*Air Force Non-Nuclear Intrusion Detection System (IDS) Equipment Approved List*,  
Contact AFSFC/S5G at [afsfc.ibdss@us.af.mil](mailto:afsfc.ibdss@us.af.mil) with any questions concerning these items.

ESE-TP-0023, *Electronic Security Equipment (ESE) Master Installation Acceptance Test and Turnover Plan*, AFLCMC/HBU (Test Section), 3 Eglin Street, Bldg. 1612, Hanscom AFB, MA 01731-2102, Attn: Test & Turnover Plan

USAF Standard Drawings, *Assembly & Installation of Fence, IDS Sensor Platform with Vertical Outrigger*, Contact AFSFC/S5G at [afsfc.ibdss@us.af.mil](mailto:afsfc.ibdss@us.af.mil) with any questions concerning these items.

## UNITED STATES ARMY

AR 190-13, *The Army Physical Security Program*

AR 190-17, *Biological Select Agents and Toxins Security Program*

AR 380-27, *Control of Compromising Emanations*

## DEPARTMENT OF DEFENSE

DoDM 5105.21, Volume 2, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security*

DoDI 5210.65, *Security Standards for Safeguarding DoD Chemical Agents*

DoDI 5210.88, *Security Standards for Safeguarding Biological Select Agents and Toxins (BSAT)*

DoDI 8500.01, *Cybersecurity*

DoDI 8510.01, *Risk Management Framework for DoD Systems*

## UNITED STATES DEPARTMENT OF DEFENSE, UNIFIED FACILITIES CRITERIA

UFC 4-021-01, *Design and O&M: Mass Notification Systems*

UFC 4-026-01, *Design to Resist Forced Entry*

UFC 4-215-01, *Armories and Arms Rooms*

UFC 4-420-01, *Ammunition and Explosives Storage Magazines*

UFGS 01 14 00, *Work Restrictions*

UFGS 28 08 10, *Electronic Security System Acceptance Testing*

UFGS 28 10 05, *Electronic Security Systems (ESS)*

UFGS 28 20 02, *Central Monitoring Services for Electronic Security Systems*

## **UNITED STATES MARINE CORPS**

MCO 5510.18B, *US Marine Corps Information and Personnel Security Program (IPSP)*,  
<http://www.marines.mil/portals/1/Publications/MCO%205510.18B.pdf>

## **UNITED STATES NAVY**

OPNAV 3502.8, *Navy Mission Assurance Program*,  
<https://www.secnav.navy.mil/doni/Directives/03000%20Naval%20Operations%20and%20Readiness/03-500%20Training%20and%20Readiness%20Services/3502.8.pdf>

SECNAV 5510.36B, *Department of the Navy Information Security Program*,  
<https://www.secnav.navy.mil/doni/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-500%20Security%20Services/5510.36B.pdf>

OPNAV 5530.14E, *Navy Physical Security and Law Enforcement Program*,  
<https://www.secnav.navy.mil/doni/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-500%20Security%20Services/5530.14E%20W%20CH-3.PDF>

OPNAV 5530.16B, *Minimum Security Standards for Safeguarding Biological Select Agents and Toxins*,  
<https://www.secnav.navy.mil/doni/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-500%20Security%20Services/5530.16B.pdf>

## **US ARMY CORPS OF ENGINEERS (USACE)**

Engineering Regulation 1110-1-8162, *Design and Construction Policy for Electronic Security Systems*,  
<https://www.usace.army.mil/Portals/2/docs/Protection/ER%201110-1-8162,%20Design%20and%20Construction%20Policy%20for%20Electronic%20Security%20Systems.pdf>

HNC-PR-ED-2000.10, *Design Manual*, Rev. 9.  
<https://www.hnc.usace.army.mil/Missions/Engineering-Directorate/TECHINFO/>